Tasks of Operators of Essential Services and Digital Service Providers

Katarzyna Chałubińska-Jentkiewicz

Abstract Public tasks for cyberspace security occupy an important place in the National Security System of the Republic of Poland. The responsibility for ensuring cybersecurity lies with all network users, but public administration authorities play a significant role, with one of the basic tasks being activities to ensure public security and order. In the conditions of arrangements for the implementation of public tasks for national security, with particular emphasis on the specification of public tasks in the area of critical infrastructure protection, it is important to determine the catalogue of entities performing public tasks in the field of cyberspace security. It should be noted that these entities may be public entities performing public tasks, private entities performing public tasks based on the privatisation of public task implementation, and private entities performing their own tasks that are of significant public interest, or which were once carried out as public tasks but were subject to privatisation.

The opportunities afforded by new technologies, and the resulting necessity to adapt the administrative and legal system, are key issues concerning the development of modern public management and ensuring the security of ICT networks. Public authorities have become obligated to provide electronic services to citizens, covering both the handling of citizens' affairs and other areas of public administration functioning, not excluding the decision-making process. The computerisation processes in public administration are accompanied by changes associated with the state-citizen relationship. Furthermore, it is worth noting that in the initial period of the development of computerisation, digitalisation occurred mainly in organisational units, which based their activities on processing significant amounts of data. The first IT applications were implemented in the financial and accounting departments,

K. Chałubińska-Jentkiewicz (✉)

Akademickie Centrum Polityki Cyberbezpieczeństwa/Academic Center for Cybersecurity Policy, Akademia Sztuki Wojennej w Warszawie/War Studies University in Warsaw, Warsaw, Poland

e-mail: k.jentkiewicz@akademia.mil.pl

where IT services for public institutions were provided.¹ Modern electronic technology facilitated data processing by means of the automation of certain work in public administration. Therefore, “information technology is becoming an essential tool for the efficiency of the administrative apparatus”.² Thus, it can be concluded that the current development of administrative procedures in Poland is being significantly influenced by constant and advanced technical progress. The influence of new technical measures which have emerged in public administration is necessitating modifications to basic administrative-legal relations (individual-citizen), but is also significant for inter-sectoral cooperation in the implementation of public tasks. Cyberspace is a new sphere of influence of these processes. As cyberspace develops, the threats occurring in it evolve. Cyberspace is nowadays a symbol of progress, but also of freedom and privacy, and every interference in its functioning is associated with an attack on these values. For the countries involved in developing the information society, cybersecurity is considered to be one of the most serious challenges for the national security system. It involves the security of both the entire state establishment and individual citizens. Therefore, public tasks in cybersecurity occupy an important position in the Polish National Security System. The responsibility for ensuring cybersecurity rests with all network users; however, a significant role is played by public administration authorities, one of whose primary tasks is to ensure security and public order. In terms of arrangements regarding the implementation of public tasks for national security, with particular emphasis on the definition of public tasks in the sphere of critical infrastructure protection, it is important to establish a directory of entities performing public tasks in the field of cyberspace security. Furthermore, it should be noted that these entities may be public entities performing public tasks, private entities undertaking public tasks on the basis of the privatisation of public tasks, or private entities carrying out their own tasks, which are significant for the public interest, or which used to be performed as public tasks, but were subject to privatisation. Subsequently, the issue of intersectoral cooperation is becoming increasingly important in the process of creating a uniform cybersecurity system. The European Public-Private Partnership for Resilience was launched on the basis of the document COM (2009) 149. This platform has initiated activities and increased cooperation between the public and private sectors in identifying key resources, means, functions, and core requirements for resilience, as well as the need for cooperation and mechanisms to respond to large-scale disruptions to electronic communications. National network and information security authorities should cooperate and exchange information with other regulatory authorities, in particular data protection authorities. Responsible NIS authorities should also report major incidents which might be criminal in nature to law-enforcement authorities. Competent national authorities should also regularly publish, on a dedicated website, non-classified information on current early warnings of incidents and threats, and coordinated responses. Legal obligations should not replace or prevent informal or

¹Pawłowski (2002), p. 85.

²Knosala et al. (1996), p. 126.

voluntary cooperation, including between the public and private sectors, aimed at increasing security and exchanging information and best practices. A particularly important and useful platform at the EU level to be developed is the European Public-Private Partnership for Resilience (EP3R15). Pursuant to recital 9 of the Preamble to the Directive, certain sectors of the economy are already regulated, or may in the future be regulated, by sector-specific Union legal acts which incorporate provisions on NIS security.

The Act of 5 July 2018 on the National Cybersecurity System under the provisions of the NIS Directive, introduced the concept of an essential service, which means a service which is crucial for maintaining critical social or economic activities, listed in the register of essential services. Additionally, the Act introduced the concept of a digital service, which means a service provided electronically within the meaning of the provisions of the Act of 18 July 2002 on Providing Services by Electronic Means,³ listed in Annex No. 2 to the Act. The Act on the Provision of Services by Electronic Means assumes that such a service is characterised by the fact that it is provided at a distance, without the simultaneous presence of the parties (remotely), through the transmission of data, at the individual request of the recipient of the service, transmitted and received by means of devices for electronic processing, including digital compression, and the storage of data, which is entirely transmitted or received by means of a telecommunications network within the meaning of the Act of 16 July 2004—Telecommunications Law.⁴

With regard to the digital service, the Act also determines the entity providing the digital service, which is the digital service provider, i.e. a legal person, or an organisational unit without a legal personality, with its registered office or management bodies in the Republic of Poland, or a representative with an organisational unit in the Republic of Poland, providing the digital service, with the exception of micro and small businesses, as referred to in Article 7(1)(1) and (2) of the Act of 6 March 2018—The Entrepreneurs Law.⁵

The types of digital services are defined in Annex No. 2 to the Act, including **Internet trading platform**—a service which enables consumers or entrepreneurs to conclude contracts electronically with entrepreneurs on the website of the trading platform, or on the website of the entrepreneur who is using the services provided by the Internet trading platform (e.g. Allegro, ING Usługi dla Biznesu S.A.—ALEO.COM, B2B platform automicob2b.pl); **Cloud-computing service**—a service which provides access to a scalable and flexible set of computing resources for shared use by multiple users (e.g. Cloud for Business—ergonet.pl, Amazon Web Services,

³ Act of 18 July 2002 on Providing Services by Electronic Means, consolidated text, Polish Journal of Laws of 2020, item 344, as amended.

⁴ Act of 16 July 2004—Telecommunications Law, consolidated text Polish Journal of Laws of 2019, item 2460, as amended.

⁵ Act of 6 March 2018—The Entrepreneurs Law, consolidated text Polish Journal of Laws of 2019, item 1292 hereinafter referred to as “EL”.

Google Cloud Platform, Microsoft Azure, private and hybrid⁶); and **Internet search engine**—a service which allows users to search all websites or web pages in a given language by means of a query, by providing a key word, phrase, or other element, referring to information related to the query providing access through a link.

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, specifies the procedures and determines the operating conditions for digital service providers. Pursuant to Article 4, an incident is considered to have a significant impact if at least one of the following situations has occurred: (a) the service delivered by the digital service provider has been unavailable for more than 5,000,000 user-hours, whereby the term “user-hour” refers to the number of affected users in the Union for sixty minutes; (b) the incident has led to a loss of integrity, authenticity, or confidentiality of stored, transmitted, or processed data, or related services presented or accessible via the digital service provider’s network and information systems affecting more than 100,000 users in the EU; (c) the incident has created a risk to public safety or a risk of fatalities; (d) the incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1,000,000.

⁶**Colocation** is the oldest and straightforward form of service in the cloud. It involves renting a server room, with access to electricity, air conditioning, and the Internet. Other components—hardware, security (firewalls), load management, operating systems, software and applications, are paid for by the user company. Therefore, it is a fee for lending space in a server room.

IaaS—Infrastructure as a Service—a model consisting of providing the customer with an IT infrastructure, i.e. hardware, software, and maintenance. For example, the customer purchases a specific number of servers, disk space, or a specific amount of memory and computing power. Nonetheless, this does not mean that the hardware will be physically installed on the customer’s premises. In this model, it happens that the customer is supplying the service provider with its own software, to be installed on the rented hardware.

PaaS—Platform as a Service—the sale of a ready-made, often customised, set of applications. There is no need to purchase hardware or install software. All the necessary programs are located on the provider’s servers. The client gets access to the interface (usually in the form of a standardised working environment) through a program, e.g. a web browser. In this model, services are usually available to the user from any computer connected to the Internet.

SaaS—Software as a Service—The customer receives specific, selected software functions. They use any software they need. For this reason, they are not interested in hardware or the working environment. They only have access to specific, functional tools—not necessarily connected to each other through a uniform interface. The programs run on the provider’s server. The customer is not obliged to purchase a licence for them. He or she only pays for each use of them, and access to such tools is granted on request.

CaaS—Communications as a Service—The service provider delivers a platform for a telecommunications work environment.

iPaaS—Integration Platform as a Service—A platform which provides integration between different services in the Cloud.

The tasks of a digital service provider include: (1) security of information systems and facilities; (2) incident handling; (3) business continuity management of the provider to provide a digital service; (4) monitoring, auditing, and testing; (5) the latest state of the art, including compliance with international standards as referred to in Implementing Regulation 2018/151.

1. Security of systems and facilities, as referred to in Article 16(1)(a) of the NIS Directive, means the security of network and information systems and their physical environment, and includes the following elements:
 - (a) The systematic management of network and information systems—mapping information systems and establishing a set of appropriate policies for information security management, including risk analysis, human resources, operational security, security architecture, data security, system lifecycle management, and, where appropriate, encryption and management
 - (b) Physical and environmental security—the availability of a set of measures to protect the security of digital service providers’ networks, and information systems, against damage, using a holistic risk-based approach to threats, which takes into account, for example, system failures, human errors, malicious actions, and natural phenomena
 - (c) Security of supplies—establishing and maintaining the appropriate policies to guarantee the availability, and, where appropriate, the traceability, of critical supplies used to provide services
 - (d) Controls on access to network and information systems—the availability of a set of measures intended to ensure that physical access and logical access to network and information systems, including the administrative security of network and information systems, are authorised and restricted based on business and security requirements.
2. With regard to incident management, referred to in Article 16(1)(b) of the NIS Directive, measures taken by the digital service provider shall include:
 - (a) maintaining and testing detection processes and procedures to ensure timely and appropriate intelligence on unusual events;
 - (b) processes and policies for reporting incidents and identifying shortcomings and weaknesses in its IT systems;
 - (c) reacting in accordance with established procedures and reporting on the results of the measures taken;
 - (d) assessing the significance of a given incident, documenting the intelligence gained from incident analysis, and gathering relevant information which can provide evidence and support the process of continuous improvement.
3. Business continuity management, defined in Article 16(1)(c) of the NIS Directive—the ability of an organisation to maintain, or, where necessary, restore, its services at predetermined acceptable levels after a disruption, which includes:
 - (a) establishing and applying contingency plans based on business impact analyses, to ensure the continuity of services delivered by digital service providers, which is assessed and tested at regular intervals, for example through practice;

- (b) post-disaster recovery capabilities, which are evaluated and tested at regular intervals, for example through practice.
4. Monitoring, auditing and testing referred to in Article 16(1)(d) of the NIS Directive shall include the establishment and maintenance of policies involving:
 - (a) conducting planned sequences of observations or measurements to assess whether network and information systems are operating as intended;
 - (b) inspections and verifications to determine whether a standard or a set of guidelines is being applied, whether the records are accurate, and whether efficiency and effectiveness targets are being fulfilled;
 - (c) a process aimed at revealing flaws in the security mechanisms of network and information systems which serve to protect data and maintain functionality as intended. This type of process includes technical processes and personnel involved in the operation flow.
 5. International standards pursuant to Article 16(1)(e) of the NIS Directive—standards adopted by the international standardisation body referred to in Article 2(1) (a) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council. According to Article 19 of the NIS Directive, European or recognised international standards and specifications relevant to the security of network and information systems, including existing national standards, may also be implemented.
 6. Digital service providers shall ensure that the appropriate documentation is made available to the competent authority for the purposes of verifying compliance with the safeguards set out in 1, 2, 3, 4 and 5.

In the field of its responsibilities, the digital service provider:

- (1) undertakes activities which allow the detection, recording, analysis, and classification of incidents;
- (2) provides, to the extent necessary, access to information for the appropriate CSIRT MON, CSIRT NASK, or CSIRT GOV about incidents classified as critical by the respective CSIRT MON, CSIRT NASK, or CSIRT GOV;
- (3) qualifies the incident as significant;
- (4) reports a significant incident immediately, no later than 24 hours after detection, to the appropriate CSIRT MON, CSIRT NASK, or CSIRT GOV;
- (5) ensures the handling of a significant incident and critical incident in cooperation with the respective CSIRT MON, CSIRT NASK, or CSIRT GOV, furnishing the necessary information, including personal data;
- (6) removes vulnerabilities;
- (7) communicates to the operator of essential services which supplies the essential service through that digital service provider information about any incident affecting the continuity of the essential service of that operator.

The NIS Directive introduces a definition of the concept of “operators of essential services”, according to which it is a public or private entity, belonging to one of the

types referred to in Annex II of the Directive, fulfilling the criteria stipulated in Article 5(2) of the Directive, i.e.:

- (a) the entity provides a service which is fundamental to maintaining critical social or economic activity
- (b) the provision of this service depends on network and information systems and
- (c) the incident would have a significantly disruptive effect on the provision of this service.

The concept of services is defined in Article 57 of the TFEU,⁷ and means “benefits normally provided for remuneration, to the extent that they are not covered by the provisions on the free movement of goods, capital and persons”. The definition of services contained in primary law is negative. Services include, in particular, (a) industrial activities; (b) commercial activities; (c) craftspeople’s activities; (d) performing independent professions.

The operator of an essential service is an entity referred to in Annex No. 1 to the Act, which has an organisational unit on the territory of the Republic of Poland, in respect to which the competent authority for cybersecurity issues has issued a decision granting the status of an operator of essential services. Sectors, subsectors, and types of entity are defined in Annex No. 1 to the Act. In these circumstances, the so-called essential services have been assigned in the field relevant to cybersecurity. According to recital 19 of the Directive, Member States should be responsible for determining which entities meet the definition of an operator of essential services. To ensure a coherent approach, the definition of the operator of essential services should be applied consistently by all Member States. The NIS Directive provides for the assessment of operators in specific sectors and subsectors; the preparation of an inventory of essential services; the consideration of a common list of cross-sectoral factors to determine whether a possible incident could have a significantly disruptive effect; a consultation process involving the relevant Member States in the case of operators providing services in more than one Member State; and support from the cooperation group in the identification of operators. The operators of essential services shall guarantee an increase in the level of security of the services provided through the introduction of the effective management of the cybersecurity system, and the protection of the entities providing services in the field of cybersecurity.

The concept of service should not include services to which the Treaty’s provisions on the exchange of goods, and the movement of capital and persons, do not apply. The service will therefore include all activities performed for remuneration which serve or accompany the exchange of goods and the free movement of capital and persons, including the services of so-called online intermediaries, which provide Internet-access services as well as hosting services or services by providers of platforms storing data from users and data-encryption services. The Polish regulation indicates the necessity for the service provider to have a key organisational unit

⁷The Treaty on the Functioning of the European Union of 26 October 2012, OJ EU 2012 L 326/47.

located on the territory of Poland. The Civil Code⁸ indicates in Article 41, in relation to legal persons, and correspondingly in Article 33¹ in relation to organisational units without a legal personality to which the Act grants legal capacity, that the registered office is the place where their governing body is located. Each Member State shall establish a list of services, and, where an operator provides a service which is essential for maintaining critical social or economic activities, in two or more Member States, those Member States shall consult each other. This consultation occurs before the identification decision is taken (Article 5(4) of the NIS Directive).

In accordance with recital 20 of the Preamble to the Directive, in the process of identifying operators of essential services, Member States should assess, at least for each subsector referred to in this Directive, which services must be considered essential for the maintenance of critical social and economic activities, and whether entities within sectors and subsectors, and the providers of those services, meet the criteria for identifying operators. While evaluating whether an entity provides a service which is critical to maintaining vital social or economic activity, it is sufficient to examine whether the entity provides a service which is included in the list of essential services. Furthermore, it must be demonstrated that the provision of the essential service depends on network and information systems. Additionally, when assessing whether an incident could have a significantly disruptive effect on the provision of a service, Member States should take into consideration a number of cross-sectoral, and, where appropriate, sectoral factors.

Pursuant to Article 6 of the Directive, Member States shall take into account at least the following cross-sectoral factors when determining the significance of the disruptive effect: (a) the number of users dependent on the service provided by the entity; (b) the dependence of the other sectors specified in Annex II on the service provided by the entity; (c) the impact which incidents—in terms of their scale and duration—could have on economic and social activity or public security; (d) the market share of this entity; (e) the geographical coverage related to the area which could be affected by the incident; (f) the importance of the entity in maintaining a sufficient level of service, taking into account the availability of alternative means of providing this service. In order to determine whether an incident would have a significantly disruptive effect, Member States are required to take into consideration sectoral factors, where appropriate. These guidelines were taken into consideration in the secondary legislation to the Act. In accordance with the Regulation of the Council of Ministers of 31 October 2018 on serious incidents thresholds, the parameters to be taken into account to determine whether the impact of the incident is significant include the number of users affected by the disruption of the essential service; the timing of the impact of the incident on the essential service provided; the geographical coverage of the area affected by the incident, and other factors specific to the subsector; also whether the incident caused at least one of the following circumstances:

⁸The Civil Code, consolidated text of the Polish Journal of Laws of 2020, item 1740, as amended, hereinafter referred to as CC.

- (a) the death of a person,
- (b) serious damage to health,
- (c) other than serious damage to the health of more than one person, and
- (d) financial losses exceeding PLN 250,000.

For the identification of operators of essential services, holding an organisational unit in a Member State involves the need to operate efficiently and effectively through stable structures. The legal form of such structures, whether a branch or a subsidiary with legal personality, is not a determining factor in this respect (recital 21).

The process for identifying operators of essential services is specified in Article 5 of the Directive. Member States were required to identify, for each sector and subsector referred to in Annex II, by 9 November 2018 at the latest, the operators of essential services with an organisational unit on its territory.

The Polish legislators follow the definition from the NIS Directive, and therefore the operator of essential services is an entity which meets all the following conditions:

- (1) will be one of the entities listed in the Annex to the Act,
- (2) will provide the essential service listed in the inventory of essential services,
- (3) the provision of this service will depend on information systems,
- (4) the incident would have a significantly disruptive effect on its performance.

Consequently, the operator of essential services is a party to the rights and obligations under the Act, regardless of whether it has entrusted to another entity activities related to the provision of the essential service. Therefore, all issues of responsibility sharing between the various entities should be regulated internally by these bodies. An important element in the decision, as evidence of the will of the administrative authority, is the decisive resolution of the matter covered by the motion initiating the proceedings. It should be explained that a case may only be settled (within the meaning of Article 104(1) and (2) of the Code of Administrative Procedure—CAP) by a public administration authority if the facts have been duly established. For this reason, in Article 7 of CAP, the legislators assigned to the necessity of establishing the objective truth the status of the principle of administrative proceedings. Therefore, it is the duty of the authority to conduct the submission of evidence in such a way as to result in the creation of actual grounds for adopting the legal basis for the settlement. Undoubtedly, a defective establishment (or failure to establish) of facts relevant to the case prevents the authority from issuing an appropriate decision. Otherwise, an administrative decision—in accordance with Article 104 of CAP—resolves the case on its merits within the limits of the demand specified by the parties. The decision in administrative proceedings, on the other hand, consists of applying the applicable law to the established facts of an administrative case. Therefore, the public administration authority pursues the objective of the administrative procedure, which is to implement the applicable legal standard for administrative and legal relations, when these relations require such a measure. According to this objective of the administrative procedure, also the essence of the administrative decision can be distinguishing between the factual

basis and the legal basis of the administrative decision. The factual basis is the findings of facts made by a public administration authority, while the legal basis is those legislative provisions which the authority has accepted as binding in a given case, and applied in its ruling.⁹ Establishing the actual implementation of the conditions indicated above enables an administrative decision to be made in the context of establishing the status of the operator of essential services.

The status of the operator of essential services should be determined by means of a decision. The legislators have not specified that it is this particular form; however, it should be assumed that if the legal situation of a particular entity is determined, it is an administrative decision. An administrative decision is considered to be a declaration of will of an administrative body which has legal effects in the sphere of the administrative-legal relationship (the formation, modification or expiry of that relationship).¹⁰ If a standard of substantive administrative law requires concretisation, the form of administrative decision is considered to be the form of such concretisation. This applies also in this case. For the operator to be recognised in its field of operation, an administrative decision must be issued. Hence, the decision is an act of authority, issued by an authorised body.¹¹ Article 104(2) of CAP provides that decisions shall resolve the case as to its substance in whole or in part; or otherwise the case will be closed at a given level. This interpretation of the form of operation of the public administration body derives from Article 2 of the Constitution of the Republic of Poland, which states that the Republic of Poland is a democratic legal state which follows the principles of social justice. According to the court, “From the principle of a democratic state of law, the judicial doctrine and jurisprudence derives two principles of paramount importance for the formation of the rights of the individual in relation to public administration, and thus for the interpretation of the law: the principle of the right to a trial and the principle of the right to a court. The essence of the principle of the right to a trial is to grant an individual the right to defend his or her legal interests in proceedings governed by procedural law. The principle of the right to a trial is of fundamental importance for the interpretation of the substantive law provisions on the form of settlement, towards the adoption of the principle of settling an individual’s affairs in the form of an administrative decision when the substantive administrative law provision does not assume another form of settlement on an *expressis verbis* basis. The Code of Administrative Procedure does not contain a legal definition of the term “administrative decision”. However, it is assumed by legal commentators and in judicial decisions that, in accordance with the provisions of Article 1(1) of the CAP, it follows that an administrative decision is a sovereign manifestation of the will of a

⁹Judgment of the Court of Appeal in Katowice of 5 April 2013. File No. III APa 55/12 LEX No. 1313277.

¹⁰Judgment of the Supreme Administrative Court of 25 April 2012, File No. I OSK 654/11 LEX No. 1264894.

¹¹Cf. judgment of the Supreme Court of 3 April 2000, I CKN 582/98, LEX No. 50843, Borkowski (1996), p. 439.

public-administration authority, issued in proceedings pending before that authority in an individual administrative case, and constitutes its decision. Administrative decisions are the basic form of action of public administration authorities, and are therefore the primary object of appeal in administrative court proceedings. A complaint to the administrative court is available both against administrative decisions issued under the Code of Administrative Procedure and against decisions issued under another procedure regulating jurisdictional proceedings, i.e., against decisions in cases in which, pursuant to Article 3 of CAP, jurisdictional proceedings have been excluded from the scope of the Code of Administrative Procedure (exclusions of applications of the Act). The situation of the adoption of the decision in question for an administrative decision has an impact on the entity's rights to take appeal actions, which can hinder the process of determining the list of operators of essential services.

Furthermore, it shall be possible for operators in the sectors and subsectors referred to in this Directive to provide both essential and non-essential services. For the purposes of identifying operators, Member States should therefore establish a list of services which they consider to be essential (such a list is specified in Annex No. 1 to the Act).

According to Article 41 of the Act, the authorities competent for cybersecurity matters are:

- (1) for the energy sector—the Minister competent for energy issues
- (2) for the transport sector, excluding the water transport subsector—the Minister competent for transport
- (3) for the water-transport subsector—the Minister competent for the maritime economy and the Minister competent for inland navigation
- (4) for the banking sector and infrastructure of financial markets—the Polish Financial-Supervision Authority
- (5) for the healthcare sector, excluding the entities mentioned in Article 26(5)—the Minister competent for health matters
- (6) for the healthcare sector covering the entities mentioned in Article 26(5)—the Minister of National Defence
- (7) for the drinking water supply and distribution sector—the Minister competent for water management
- (8) for the digital infrastructure sector, excluding the entities referred to in Article 26(5)—the Minister competent for digital affairs.
- (9) for the digital infrastructure sector including the entities referred to in Article 26(5)—the Minister of National Defence
- (10) for digital service providers, excluding the entities mentioned in Article 26(5)—the Minister competent for digital affairs.
- (11) for digital service providers including the entities mentioned in Article 26(5)—the Minister of National Defence.
- (12) for entities subordinated to the Minister of National Defence or supervised by him, including those whose communication and information systems or networks are covered by a uniform list of objects, installations, devices, and

services included in the critical infrastructure referred to in Article 5b(7)(1) of the Act of 26 April 2007 on Crisis Management; and

- (13) Entrepreneurs of particular economic and defensive importance, in respect of whom the Minister of National Defence is the authority organising and supervising the performance of tasks for the benefit of state defence, within the meaning of Article 5(3) of the Act of 23 August 2001 on the Organisation of Tasks for State Defence Performed by Enterprises.

It should be emphasised that, according to recital 45 of the preamble, the Directive applies only to those public administrations which have been identified as operators of essential services. However, Member States remain responsible for ensuring the security of the network and information systems of public administrations outside the scope of the NIS Directive.

Where an entity provides an essential service in other Member States of the European Union, the authority competent for cybersecurity matters shall, in the course of the administrative proceedings, consult with those states through the Single Points of Contact to determine whether the entity is recognised as an operator of an essential service in those states. In accordance with Article 5(4) of the Directive, where an operator provides a service referred to in 2(a) in two or more Member States, those Member States shall consult each other. Such consultation shall take place before a decision on classification is taken. This provision is equivalent to the procedure for identifying an operator of essential services as stipulated in the Directive. For the purposes of the identification process, where an entity provides an essential service in two or more Member States, these states should engage in bilateral or multilateral discussions among themselves.

In relation to an entity which no longer meets the conditions, the competent authority for cybersecurity shall issue a judgment stating that the decision to consider an operator of essential services has expired.

The content of the provision of Article 162(1) of CAP states

a public-administration authority is obliged to determine the expiry of a decision if the following conditions are jointly met:

- (a) the decision became pointless,
- (b) the decision shall be declared void by a provision of law or the declaration of voidness is in the public interest or in the interests of a party.

An administrative decision which establishes the status of an operator of essential services is not indefinite. When the operator no longer meets the conditions, the authority issues a new decision, this time determining the expiry of the previous one. Similarly as the decision determining the status of an operator of essential services, the decision determining its expiry is subject to all CAP regulations. There is no doubt that in the event of a legal provision's ordering the decision to expire, a public administration authority is obliged to examine whether the conditions listed in this provision are being met. A ruling to grant the status of an essential service, or a decision to rescind such a decision, is immediately enforceable. The requirement of immediate enforceability is regulated in Article 108(1) and (2) of CAP. The essence

of the immediate enforceability of administrative decisions is that the decision becomes enforceable, and constitutes an enforcement order, although it is not final. According to the above-mentioned standard, the rigour of immediate enforceability can be imposed *ex-officio*, or at the request of a party, only for a decision against which an appeal is being lodged, i.e. against a non-conclusive decision. The enforcement of a non-conclusive decision is exceptional; therefore the prerequisites for making the decision immediately enforceable must not be interpreted in a broadening but in a narrowing way. In the case of a regulation concerning the administrative decision determining the status of an operator of essential services, its immediate enforceability was established by law. This solution results from the special status of the regulation of services which are important for security.

Article 7 of the National Cybersecurity System Act obliges the Minister competent for digital affairs to maintain a list of operators of essential services. This list is created taking into consideration the division into sectors, subsectors, and types of entities introduced by the Act. The entry into or removal from the list is declaratory in nature, and will be a material and technical activity, implemented on the basis of administrative decisions by the competent authorities, in terms of identifying operators of essential services in the relevant sectors. This provision also defines the procedure for access to the information and the directory of entities in which the information from the list will be made available. Recital 25 of the Preamble to the Directive indicates the obligation to establish a list containing all operators of essential services, or by adopting national measures containing objective quantitative criteria, such as the end result of the operator's activities or the number of users, which make it possible to determine which entities are covered by obligations relating to network and information system security.

The public register is an institution through which a registry authority with the characteristics of a public body manages an official dataset, controls the reported information, may modify it on its own, or request specific changes, and holds the power to refuse to publish certain information with regard to its content.¹² In the traditional definition, maintaining the register and publishing the data included in it can have certain legal effects, and this occurs when the public notification and publication of the indicated data determines the effectiveness of a legal action.¹³ The information contained in the register is received, recorded, and made available by means of a decision, which is an act of law, resulting in the registration.¹⁴ Such an approach is primarily related to the nature of the register as a regulatory instrument in the sphere of organising public administration activities. The registration system is based on the state's determination of the conditions. The registration procedure involves the possibility of verifying whether the market-share requirements imposed by law on interested parties are being fulfilled.

¹²Ganczar (2009), p. 99.

¹³Ganczar (2009), p. 100.

¹⁴Ganczar (2009), p. 632.

The regulatory model adopted in the Act assumes that the responsibilities of sectoral institutions in the field of cybersecurity will be extended, instead of establishing a single national entity for cybersecurity at the central level. Administrative, regulatory, and control responsibilities have been assigned to the Ministers responsible for the sectors listed in the NIS Directive, namely energy, transport, banking and financial institutions, healthcare, water supply, digital infrastructure, and digital service providers (Article 41). Regarding the healthcare sector, digital infrastructure, and digital service providers, the separate entities subordinated to or supervised by the Minister of National Defence were taken into consideration. Article 42 of the Act stipulated a schedule of tasks to be performed by the competent authorities. These tasks include conducting analyses, issuing administrative decisions granting the status of an operator of essential services, rescinding the status of an operator of essential services, and monitoring the application of the Act by operators of essential services, as well as digital service providers in their respective sectors.

Data from the list of operators of essential services, to the extent necessary to implement their statutory tasks, shall be made available by the Minister competent for digital affairs, on request. The data are retained by units such as the police, the courts, prosecutor's offices, or other services for preventive purposes, for the detection of criminal activities. The following authorities are entitled to use the data under this provision: competent authorities in the field of cybersecurity, the courts, prosecutor's offices, the police, the Border Guard, the Military Police, the Military Counter-Intelligence Service, the Internal Security Agency, the Central Anti-Corruption Bureau the National Revenue Administration, the Government Security Centre and the State Protection Service. Such data should be used primarily as a source of information and evidence in criminal cases. Nonetheless, the institutions listed here have the right to use the data in the performance of their statutory tasks, also for preventive purposes. Public institutions very often benefit from such legal possibilities. Within the activities of the institutions indicated here, so-called operational and investigative activities can be distinguished.

Operational and investigative activities are non-contentious. This limits judicial control over their course—"the practice of the investigating service has been shaped as complementary or executive activities in relation to procedural activities and the tasks of preparatory proceedings".¹⁵

The tasks of operators of essential services include the systematic assessment and management of the risk of an incident.

Conducting systematic assessment and the management of incident risk. The first obligation of the operator of essential services concerns the creation and implementation of a security management system in the information (ICT) system, and follows from Article 14 of the Directive, according to which Member States shall ensure that operators of essential services undertake appropriate and proportionate technical and organisational measures to manage the risks to which their network and information

¹⁵See Szaff (1957), p. 38.

systems are exposed. Taking into consideration the state of the art, these measures must ensure a level of security of network and information systems commensurate with the existing risks. Member States shall ensure that operators of essential services adopt the appropriate measures to prevent and minimise the impact of security incidents on the network and information systems used to provide such essential services, with a view to ensuring the continuity of those services. According to Article 4(9) of the NIS Directive, ‘risk’ means any reasonably identifiable circumstance or event which has a potentially adverse impact on the security of network and information systems. Management is primarily involved in organising safety (defining safety requirements and the range of responsibilities, and assigning organisational functions). Information- and communication-security management is intended to ensure the security of information systems—here the information system (i.e. the information and communication system referred to in Article 3(3) of the Act of 17 February 2005 on the Computerisation of the Operations of Entities Performing Public Tasks together with the data processed in electronic form) of the data contained therein in a situation of many difficulties and adversities. Among numerous conditions which hinder this protection, it can be mentioned that communication and information systems are difficult to manage because they are highly complex, fast, and extremely diverse in terms of technology; communication and information systems and their environments are constantly changing; threats to the environment are difficult to fully identify; the management processes are highly diverse, interdisciplinary—there are often interrelationships which are not fully understood; multiple issues are difficult to identify, and, due to the human factor present here, also unpredictable. Risk assessment and the analysis of threats involves the identification of threats, the vulnerability analysis of systems, and the development and implementation of a comprehensive security plan (security policy). Therefore, in order to ensure the security of the data, and the information systems in which this information is processed, due to the complexity of these systems and processes, and their interdependence and variability over time, conscious and coordinated actions are required on the basis of the objectives set, i.e. to conduct a certain policy, referred to as the security policy in this document. Resource protection involves limiting the vulnerability of the system, and shielding it from threats by using protective measures. On the other hand, the monitoring and detection of threats involve all activities (e.g. notification) related to ensuring proper operations (including protections). The reaction to an incident is any action related to the response to the incident (security breach). Consequently, it must be assumed that the term “information system security” means a level of reasonable confidence that the potential losses resulting from the unauthorised (accidental or deliberate) disclosure, modification, destruction, or rendering inoperable the processing of information stored and transmitted through information and communication systems, will not be incurred. Information and communication security must be considered in their organisational, technical, and legal aspects. Thus, security is not a single act of introducing protections, but a continuous, dynamic, and very complex process which requires constant supervision and adaptation to fluctuating environmental conditions. Under such conditions it seems necessary to manage the information-security

system. The principles of risk management in the context of telecommunications security can be discussed with reference to International Standards. The general concepts of this management are specified in ISO/IEC 27001, which was developed to support the effective implementation of a risk-management approach to security. Understanding the concepts, models, processes, and terminology outlined in ISO/IEC 27001 and ISO/IEC 27002 is crucial for understanding PN-ISO/IEC 27005:2014 Information Technology—Security Techniques—Risk Management in Information Security. The International Standard is applicable to all types of organisations (e.g., companies, governmental institutions, non-profit organisations) which intend to manage the risks which can cause information-security breaches in these organisations. Polish Standard PN-ISO/IEC 27005:2014 Information Technology—Security Techniques—Risk Management in Information Security defines the principles and methodology of risk management in security management systems within the so-called essential services—in the sphere of threats from cyberspace. Risk management should be understood as activities consisting of risk estimation, risk handling, risk acceptance, risk monitoring, and risk communication. Where ISO standards are applied, 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, text with EEA relevance, must be taken into consideration.¹⁶ Risk assessment—a comprehensive process of risk identification, analysis, and assessment—is the task of a person or a team appointed by the operator of essential services. Risk analysis includes the following steps: estimating the consequences, assessing the probability of the incident, and determining the risk level. Consequence estimation consists of considering what effects on information resources or communication and information systems could be brought about by the materialisation of threats, taking into account the vulnerability of resources or systems. Incident risk assessment is to determine the frequency with which specific incidents might occur. Statistics on similar events should also be taken into consideration. This risk assessment, on the other hand, compares the designated risk levels with predefined risk-acceptance criteria, and facilitates the determination of priorities in risk management. Initial identification, i.e. risk diagnosis, is performed by the person responsible for a given resource, and who passes the identification results to the person responsible for performing the risk analysis. The whole process is coordinated by the plenipotentiary for cybersecurity of the institution. If a

¹⁶Regulation (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, text with EEA relevance, OJ EU 2012 L 316/12.

plenipotentiary is not appointed, the process is coordinated by the person designated by the operator of essential services. The list of threats and vulnerabilities may be extended as required by the operator of essential services, where the identification of risks is conducted. Such risk identification shall be carried out periodically or on an ad-hoc basis. Ad-hoc identification is performed when a threat to a system is observed, where the horizon of materialisation is shorter than the periodic identification of risks, and when a delay in identification would be significant for the system. Ad-hoc identification is also undertaken in the event of an ICT incident's resulting in a catastrophic loss of information security. Specifically, risk identification is carried out before the system is handed over for operation. Risk assessment is the process of comparing risk values with specific criteria in order to determine the significance of risk. Risk management is the coordinated management of cybersecurity in relation to the estimated risk, which includes activities leading to a change in the level of risk through applying protections, risk avoidance, risk transfer, and acceptance of risk even if its level exceeds that of residual risk. The method of risk management is to reduce the level of risk by means of a risk-control measure in the form of protections, selected commensurately with the nature of such risk. Regarding the implementation of public tasks, which is the subject of operators of essential services' activities, risk avoidance, as a rule, does not apply; neither does risk transfer. Nonetheless, the transfer of risk may be justified in the form of the insurance of the assets of the system. According to the standard, in situations in which the final risk level is less than or equal to 20% of the maximum level ($R_k \leq 9.6$) they are subject to automatic acceptance, but remain under the supervision of the risk owner for monitoring purposes. Risks for which the level is in the range of $9.6 < R_k \leq 38.4$ are subject to acceptance according to the rules established in the entity, or are re-analysed. Risks for which the level exceeds 80% of the maximum level ($R_k > 38.4$) are submitted to the entity's management for approval. Pursuant to recital 46 of the Directive, risk-management measures include actions to identify, prevent, detect, and deal with all risks of incidents and to mitigate their impact. The security of network and information systems includes the security of stored, transmitted, and processed data.

Another significant task is to implement technical and organisational measures appropriate and proportional to the estimated risk, taking into account the latest state of the art, including

- (a) the maintenance and safe operation of the information system
- (b) physical and environmental security, including access control
- (c) the security and continuity of service delivery on which the provision of the essential service depends
- (d) implementing, documenting and maintaining action plans which facilitate the continuous and uninterrupted provision of the essential service, and ensuring the confidentiality, integrity, availability, and authenticity of information
- (e) covering the information system employed to provide the essential service with a continuous monitoring system.

According to recital 53 of the preamble to the Directive, in order to avoid imposing a disproportionate financial and administrative burden on the operators

of essential services and digital service providers, the requirements should be proportionate to the risks associated with the network and information system concerned and should take into account the state of the art of such measures. An essential task in ensuring the protection of systems is the application of the appropriate safeguards, proportional to the needs and objectives, i.e. also non-excessive safeguards against the loss of security of the provision of essential services. These protections take the form of technical and organisational measures. The legislators have defined in general terms the actions to be taken by the operator of essential services. Ensuring the continuity of service provision is the principal duty. This is achieved by maintaining, documenting, and implementing plans to ensure the provision of the essential service, and the confidentiality, integrity, availability, and authenticity of information; the maintenance and secure operation of the information system; physical and environmental security, including access control, security and continuity of service delivery on which the provision of the essential service depends; and the inclusion of the information system used to provide the essential service under a continuous monitoring system. Consequently, the reduction of the risk level is performed in the process of dealing with the risk. The basic method of dealing with risk in the case of operators of essential services is to apply safeguards in the form of continuous monitoring, i.e. in the 24/7 system. The application of a security feature must take into account its impact on the other security attributes and may in itself be a risk factor. For example, the application of security measures to limit the risk of losing the confidentiality of information can increase the risk of loss of availability. Especially in the process of risk management, it is of particular importance to determine the category of safeguards. According to the security characteristics, the goal of a secure information and communication system is achieved through (1) covering the communication and information system with the process of risk management for the security of essential services provided in the communication and information system; (2) the limitation of reliability, consisting of treating other communication and information systems as potential sources of threats, and implementing safeguards in the communication and information system to control the exchange of services with these communication and information systems; (3) the introduction of multi-level protection of the communication and information system, consisting of the application of protections on as many different levels of organisation of the communication and information system protection as possible, in order to limit the occurrence of cases in which breaking a single protection results in a breach.¹⁷ Another responsibility of operators of

¹⁷Examples of protections against threats to the communication and information system resulting from cyberspace include:

Hazard category: Malicious code penetration from WAN

Building the network topology with consideration of safe and demilitarised zones (DMZ)

Network address translation

Firewalls configured according to the principle *“everything is forbidden except what is allowed”*

AV-class software at the interconnection of WAN and LAN

IDS/IPS-class systems

essential services is to collect information about cybersecurity threats. In accordance with the methodology of cyberspace risk management in government information

PROXY servers (including maintaining a blacklist of URLs and IP addresses)
 Spam detection and blocking
 Procedures for the maintenance of the protections listed in items 3–6
 Procedures for responding to detected incidents
 Hazard category: Malicious code entry from LAN
 AV-class software on workstations
 Blocking USB ports on workstations
 Supervision over unused LAN terminations
 DHCP server access authorisation
 Disabling software installation by users
 Verifying installed software on workstations
 Software upgrade procedures (patch installation)
 Hazard category: DDoS or DoS attack
 Network-traffic monitoring
 Using content delivery networks (CDN)
 Switching to static versions of the service after detecting a DDoS/DoS attack
 Agreements with Internet-access providers containing clauses transferring obligations relating to actions against an attack on the provider
 Blocking network traffic from specific IP addresses
 Procedures in the event of detecting a DDoS/DoS attack
 Hazard category: Unauthorised access to information
 Procedures for granting and withdrawing privileges in the system
 Procedures for reviewing authorisations in systems
 Applying the need-to-know principle
 Distribution of authorisation (the “eight-eyes” principle)
 Hazard category: Inappropriate use of the system by the user
 Initial training for new employees
 Periodic training for employees currently working in the company
 Implementation of applications verifying the quality of entered data
 Hazard category: Breaching access security inside the system
 Blocking the possibility for the user to install software
 Hardening of workstations (elimination of unnecessary operating-system functions and applications)
 Blocking the possibility of starting an operating system from a removable drive
 Verification whether only acceptable software is available on the workstation
 Periodic reviews of workstation logs by administrators
 Procedures for handling detected anomalies and ways of documenting such handling
 Hazard category: Data eavesdropping, data interception
 Application of zoning
 Application of equipment with reduced compromising emanations
 Room shielding
 Network cabling in closed channels, supervision of patch panels
 Using fibre-optic cables instead of galvanic connections
 Supervision over unused LAN terminations (disconnection of unused terminations on patch panels)
 Hazard category: System of operators of essential services as a source of interference in cyberspace
 Outgoing-traffic supervision
 Procedures for responding to botnet detection in an entity’s network
 Procedures for responding to spamming attempts
 Detection of illegal activities by internal users of the system

security management systems and ISO standards, the following categories of incidents in interactions between communication and information systems and cyberspace are distinguished, along with examples of vulnerabilities causing the materialisation of hazards to affect the information resource or communication and information system:¹⁸ Incident management, on the other hand, involves incident

¹⁸Hazard category: Malicious code penetration from WAN

absence or wrong placement in the system, or lack of AV software updates
 absence of or incorrect placement in network topology or incorrect firewall configuration
 absence of or incorrect placement in the network topology or improper configuration of IPS/IDS software and its sensors
 incorrect configuration of security mechanisms in WAN networks
 absence of server load monitoring
 susceptibility of users to social engineering methods in order to obtain information or enter malicious code

Hazard category: Malicious code entry from LAN

absence or wrong placement in the system, or failure to update AV software
 absence of or incorrect placement in network topology or wrong firewall configuration
 absence of or incorrect placement in the network topology or wrong configuration of IPS/IDS software and its sensors
 incorrect configuration of security mechanisms in LANs

Hazard category: DDoS or DoS attack

absence of or incorrect placement in network topology or wrong firewall configuration
 absence of or incorrect placement in the network topology or wrong configuration of IPS/IDS software and its sensors
 absence of network traffic supervision (QoS)
 absence of server load monitoring
 software error
 loss of access to WAN services (including Internet) as a result of an attack on WAN components

Hazard category: Unauthorised access to information

absence of supervision over users' rights, entitlements inadequate to tasks
 too slow implementation of changes in user authorisations
 absence of physical access control to system components

Hazard category: Inappropriate use of the system by the user

absence of proper user training in the use of the system
 absence of quality control of data entered into the system
 recovery of information from end-of-life media
 users' susceptibility to social engineering methods to obtain information or enter malicious code

Hazard category: Breaching of access security inside the system

absence of supervision over user authorisations, entitlements inadequate to the tasks (e.g. possibility of installing programs, including those used to break security)
 too slow implementation of changes in user authorisations
 absence of supervision over users' activities in the system
 absence of or wrong placement in the system, or no AV-software update
 absence or incorrect placement in network topology, or wrong firewall configuration

handling, searching for links between incidents, removing the causes of incidents, and developing conclusions resulting from incident handling. Unlike risk management, incident management will cover actual situations where a security breach has occurred.

Another responsibility of operators of essential services is to collect information about cybersecurity threats. According to the methodology of cyber risk management in government information security management systems and ISO standards, the following categories of incidents: in interaction between the communication and information system and cyberspace are distinguished, as well as examples of vulnerabilities causing the materialisation of the threat to affect the information resource or communication and information system. On the other hand, monitoring and detecting hazards are any activities (e.g. notification) related to ensuring proper operations (including protections). The reaction to an incident means all actions related to the response to the incident (security breach).

Therefore, it should be assumed that the term “information and communication security” means the level of reasonable confidence that potential losses resulting from unwanted (accidental or deliberate) disclosure, modification, destruction, or disabling of the service provided through information and communication systems will not be incurred. Information and communication security must be considered in their organisational, technical, and legal aspects. Therefore, security is not a single

absence of or incorrect placement in the network topology or wrong configuration of IPS/IDS software and its sensors

Hazard category: Data eavesdropping, data interception

absence of network-traffic supervision (QoS)

compromising emanation

absence of encryption in WAN links

eavesdropping on information in the internal network (LAN)

retrieving information from end-of-life media

Hazard category: Breaking into a communication and information system from an external WAN (security breach)

absence of system software update

absence of or incorrect placement in network topology, or wrong firewall configuration

absence of or incorrect placement in the network topology or wrong configuration of IPS/IDS software and its sensors

absence of network traffic supervision (QoS)

absence of server load monitoring

susceptibility of users to social engineering methods in order to obtain information or enter malicious code

Hazard category: Entity (office) system as a source of interference in cyberspace

absence of network traffic supervision (QoS)

absence of or wrong placement in the system, or no AV software update

absence of or incorrect placement in network topology or wrong firewall configuration

absence of or incorrect placement in the network topology or wrong configuration of IPS/IDS software and its sensors.

act of introducing protections, but a continuous, dynamic, and at the same time highly complex process, requiring constant supervision and adaptation to changing environmental conditions.

When analysing issues of telecommunications security in the context of the security of essential services, attention should be paid to the transmission of data and information through electronic media and ICT networks. Information security law is concerned with the legal protection of telecommunications systems, which incorporates certain data enabling the provision of services, the protection of the electronic services as such, and the related content and databases, as well as the network through which such services are provided. It must therefore be assumed that information security is closely linked with the concept of telecommunications security, and more specifically to information and communication technology security, which means the protection of information processed, stored, and transmitted by means of information and communication systems against unwanted (accidental or deliberate) disclosure, modification, destruction, or prevention of its processing. Computer technology and networks (ICT—Information and Communication Technologies) have become an important part of the everyday life of people, so most of the legal regulations related to telecommunications security relate to the security of communications as such, ICT security, which represents an element of telecommunications security. The obligation of the operator of essential services, which concerns the generally defined “application of measures to prevent and mitigate the impact of incidents on the security of the information system used to provide the essential service”, with particular reference to:

- (a) the application of mechanisms ensuring the confidentiality, integrity, availability, and authenticity of data processed in the information system,
- (b) ensuring that the software is updated,
- (c) protection against unauthorised modification of the information system,
- (d) immediate action when vulnerabilities or hazards of cybersecurity are identified in respect of information and communication security issues.

The term “network and information system” is defined in NIS Directive as

- (a) an electronic communications network within the meaning of Article 2(a) of Directive 2002/21/EC¹⁹;
- (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or

¹⁹“Electronic communications network” means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.

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

In light of the same act “security of network and information systems” means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;

The communication and information system in the Polish legal system was defined in the Act of 17 February 2005 on the Computerisation of the Operations of Entities Performing Public Tasks,²⁰ and according to this definition (in Article 3 (3)) it is

a set of cooperating IT devices and software, ensuring processing and storage, as well as sending and receiving, data through telecommunication networks by means of a terminal device appropriate for a given type of telecommunication network within the meaning of the Telecommunications Law—the same definition is in Article 2(3) of the PSEMA).

In accordance with Article 175d of the Telecommunications Law, the Minister competent for communications may determine by way of a regulation the minimum technical and organisational measures and methods for preventing the threats referred to in Article 175a(1) and Article 175c(1), which telecommunications undertakings are obliged to apply in order to ensure the security or integrity of networks or services, taking into consideration the guidelines of the European Commission and the European Union Agency for Cybersecurity in this respect. In the Polish legal system, the issues of information and communication security in the field of electronic communication security in relation to telecommunications and ICT networks are defined in Telecommunications Law. Pursuant to Article 3(1) of this Act, the provisions of Telecommunications Law, unless ratified international agreements binding on the Republic of Poland provide otherwise, relate to the issues of network security. It should be noted that the NCSA does not apply to the telecommunications undertakings referred to in Telecommunications Law, as far as security requirements and incident reporting are concerned, as they are subject to the above-mentioned regulations on telecommunications security. Consequently, these obligations do not overlap.

With regard to ensuring the confidentiality, integrity, availability, and authenticity of data processed in the information system, several definitions should be considered. Reference is made to the definition of ‘availability’ in Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. This document not only defines the concepts which constitute the definition of

²⁰Consolidated text, Polish Journal of Laws of 2020, item 346, as amended.

information security, but also defines ‘availability’,²¹ which means that data are available and services are fully operational.

While “data integrity” means the confirmation that data transmitted, received, or stored are complete and unchanged, “data confidentiality” means the protection of communications or stored data against interception and reading by unauthorised persons. It should be emphasised that the legal regulations strictly define the basic security conditions which a communication and information system should meet. First and foremost, it should ensure the confidentiality of data and information (data become information under certain conditions), but not limit its availability and integrity with other subsystems or documents.

The authenticity of data is a term indicating, above all, the importance of ensuring the reliability of data in terms of its origin and source, authorship, or possibly the ownership of databases.

Ensuring whether the integrity of systems is maintained—protection against unauthorised modification—means that the data in the system, and also the system itself will not be modified in an unauthorised manner. The application of software updates refers to the software which operates a given system, with the software being overall information in the form of a set of instructions, implemented interfaces, and integrated data designed to achieve the set objectives.

Entities providing essential services using information systems, including in the field of communication, introduce technologies and procedures for security management. However, in addition to individual solutions, systematic cross-border cooperation on ICT network security between sectors (the public-private sector), and between EU Member States, is becoming significant. Such a need arises from the fact that the problems of network security and the services it provides are of a global nature, which is determined by the features of the ICT network itself, and the ease of information transfer, especially after its digital-conversion process. Risk assessment and the analysis of threats, i.e. the identification of incidents, system-vulnerability analysis, and the development and implementation of a comprehensive security plan (security policy), are the basic responsibilities of the operator of essential services. Therefore, in order to ensure the security of the ICT services and systems in which these services are processed, due to the complexity of these systems and processes, and their interdependence and variability over time, it is required to conduct conscious and coordinated actions on the basis of the objectives set, i.e. to conduct a certain information policy, also referred to in this document as security policy. Security policy includes the obligation to communicate properly within the National Cybersecurity System.

²¹ Access, within the meaning of Directive 19/2002/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (AD), did not mean access provided to end-users/customers, but the provision of facilities and/or services to another undertaking, under defined conditions, for the purpose of providing electronic communications services, including access to virtual network services.

The information obligations of an operator of essential services involve the identification of the person responsible for contacts with entities forming the National Cybersecurity System, i.e.:

- (1) other operators of essential services;
- (2) digital service providers
- (3) CSIRT MON
- (4) CSIRT NASK
- (5) CSIRT GOV
- (6) sectoral cybersecurity teams
- (7) public-finance-sector entities specified in Article 9(1)-(6), (8), (9), (11) and (12) of the Act of 27 August 2009 on Public Finance
- (8) research institutes
- (9) National Bank of Poland
- (10) Bank Gospodarstwa Krajowego
- (11) Office of Technical Inspection
- (12) Polish Air Navigation Services Agency
- (13) Polish Centre for Accreditation
- (14) National Fund for Environmental Protection and Water Management, and provincial funds for environmental protection and water management
- (15) companies and partnerships performing public-utility tasks within the meaning of Article 1(2) of the Act of 20 December 1996 on Municipal Management
- (16) entities providing cybersecurity services
- (17) authorities providing services in the area of cybersecurity
- (18) The Single Point of Contact for cybersecurity issues,²²
- (19) Government Plenipotentiary for Cybersecurity Affairs,²³
- (20) The College on Cybersecurity,²⁴

The appointment of such a person is an element in security information policy, which refers to the exchange of data, and incident information in the context of a coherent and coordinated system of mutual communication. To some extent, this person acts as a spokesperson for the coordinator of cooperation with entities operating in the system.

Furthermore, providing the user of the essential service with access to the knowledge to understand cybersecurity threats, and applying effective ways of protecting against them to the extent that the essential service is provided, in particular by publishing information about them on its website, is also part of security information policy. One of the essential principles is the exchange or sharing of risk information between system stakeholders, in this case the users—recipients—of the essential service. The legislator has indicated the form of information, e.g. a message on a website. It would be good practice to prepare for the

²²Hereinafter referred to as the “Single Point of Contact”.

²³Hereinafter referred to as the “Plenipotentiary”.

²⁴Hereinafter referred to as the “College”.

service recipient a security policy for the essential service, and special alerts, operating on the basis of information on threats to the essential service, provided directly to the service recipient. This provision does not form a basis for such notifications to be made directly, but the openness of the directory of ways to access knowledge about cyber threats, and the application of effective means of protection against those threats to the extent of the essential service delivered, provides the opportunity to communicate such unsolicited information, which justifies the need to ensure security and act in the public interest. However, pursuant to Article 38 of the Act on the National Cybersecurity System, information processed under the Act shall not be made available if its disclosure would violate the protection of the public interest in relation to public security or order, and would adversely affect the conducting of preparatory proceedings for criminal offences, and their detection and prosecution.

It should be stressed, however, that the activities of the exchanging of information in accordance with recital 8 of the Preamble to the Directive should be without prejudice to the possibility for each Member State to take the measures necessary to ensure the protection of the essential interests of its security, to safeguard public policy and public security, and to facilitate the investigation, detection, and prosecution of criminal offences. According to Article 346 of TFEU, no Member State is required to supply information whose disclosure it considers contrary to the essential interests of its security. Therefore, Council Decision 2013/488/EU (5), and non-disclosure agreements or informal non-disclosure agreements, such as the TLP²⁵ confidentiality rules, apply in this context.

The operator of essential services shall also inform the authority competent for cybersecurity of the Member States of the European Union in which Member States of the European Union the entity is recognised as the operator of essential services and the date on which the provision of the essential service is terminated within 3 months of the change. The information is intended to reach the competent authority due to the nature of the service. The authorities competent for cybersecurity matters are:

- (1) for the energy sector—the Minister competent for energy issues
- (2) for the transport sector, excluding the water transport subsector—the Minister competent for transport issues
- (3) for the water transport subsector—the Minister competent for the maritime economy and the Minister competent for inland navigation
- (4) for the banking sector and the financial-market infrastructure—the Financial Supervision Authority
- (5) for the healthcare sector, excluding the entities mentioned in Article 26(5)—the Minister competent for health
- (6) for the healthcare sector including the entities mentioned in Article 26(5)—the Minister of National Defence

²⁵TLP—Traffic Light Protocol.

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

The operator of essential services shall transmit to the authority competent for cybersecurity, the relevant CSIRT MON, CSIRT NASK, CSIRT GOV, and the sectoral cybersecurity team, the data on the person referred to in paragraph 1(1), including the name, surname, telephone number, and e-mail address, within 14 days from the date of their designation, as well as information on changes to these data—within 14 days from the date of their alteration. The purpose of this provision is to identify the data of the person designated to communicate with the authorities; the authority competent for cybersecurity, CSIRT MON, CSIRT NASK, CSIRT GOV, and the sectoral cybersecurity team. The 14-day deadline appears to be relatively long, given the dynamics of the processes taking place in communication and information systems, especially in crisis situations, related to incidents threatening cybersecurity, mainly due to the obligation to maintain monitoring on a continuous basis.

The notion of **Security Operations Centres (SOC)** has been introduced into the national cybersecurity system under the government bill on amending the National Cybersecurity System Act and the Public Procurement Law (published in the Public Information Bulletin on the Government Legislation Centre's website on 7 September 2020). SOC's are to replace the existing structures responsible for the cybersecurity of operators of essential services. SOC's have an established market position as structures performing all functions related to cybersecurity surveillance and management, both within the internal organisational structure, and as part of services provided to other entities. The operators of essential services will establish SOC structures within their internal organisational units, or enter into contracts with third-party providers of SOC services. SOC's will perform risk assessment, and detect and respond to incidents. The minister competent for computerisation will maintain the list of Security Operations Centres. The assessment of risk profiles of hardware or software providers will be performed by the Board at the request of its members. The entities within the national cybersecurity system, while managing risks in their information systems, will be obligated to take into account the results of risk assessment of hardware and software providers. The entities within the national cybersecurity system will not be able to put in operation any hardware, software or services which pose a substantial threat, and will have to withdraw such hardware, software and services indicated in the assessment of a given hardware or software provider no later than within 5 years of the date of the assessment notice. The Plenipotentiary will be obliged to announce risk assessment results by means of a notice published in the Official Gazette of the Government of the Republic of Poland. With a view to preventing critical incidents, and improving the effectiveness of critical incident response, it has been recommended that new articles (Article 67a-67c) be introduced to specify the new competencies of the Plenipotentiary,

including the power to issue warnings and injunction orders. The bill introduces amendments to the provisions of the so called new Public Procurement Law. These amendments result from the introduction of risk assessment for hardware and software providers.

As intended by the legislators, electronic communications undertakings are due to become part of the “national cybersecurity system.” They will receive support in incident response. A new category of incidents, i.e. telecommunications incidents, will be introduced. Notifications of telecommunications incidents will raise the situational awareness of national-level CSIRTs and improve the coordination of incident response. A separate CSIRT Telco is to be established to provide assistance to electronic communications undertakings, and its tasks will be analogous to those of other sector-specific CSIRTs. CSIRT Telco will be managed by the minister competent for computerisation. It should be noted that the bill is to introduce regulations concerning the obligations of telecommunications operators and trust service providers in respect of ensuring cybersecurity, which is in conflict with the provisions 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 (Official Journal EU 2016 L 194/1). Under Article 1 of the Directive, the security and notification requirements shall not apply to undertakings which are subject to the requirements of Articles 13a and 13b of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Official Journal EU 2002 L 108/33, hereinafter “Framework Directive”), or to trust service providers who are subject to the requirements of Article 19 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Official Journal EU 2014 L 257/73).

The bill sets out the obligations of electronic communications undertakings in respect of the application, following risk assessment, of appropriate and proportionate technical and organisational measures to accurately manage the risks, which implements the provisions set out in Article 40(1) of the EECC 26. The mandatory elements of the measures, arising from Recital 94 of the EECC, have been laid down. Similarly to the provisions of the Telecommunications Law currently in force, the minister competent for computerisation will have the authority to define the minimum scope of technical and organisational measures to manage the risks posed to the security of networks and services. Each undertaking will be obliged to document risk analysis and the application of the above-mentioned security measures. Article 20b defines the information obligation of an electronic communications undertaking following the detection of a security incident. Such undertaking is responsible for incident handling, and for its classification as a telecommunications incident in line with the telecommunications incident thresholds. The undertaking concerned is obliged to notify of the incident a relevant national-level CSIRT, and to cooperate with the CSIRT. This provision implements the first sentence of Article 40(2) of the EECC. In addition, such notification should be communicated to CSIRT Telco, with

which the undertaking also cooperates on the handling of telecommunications and critical incidents. Article 20c sets out the principles of incident notification applicable to undertakings preparing action plans for particular threats. They will be obligated to send a security incident notification no later than within 24 hours of incident occurrence, based on the information held at the time. This information should be updated in the course of security incident handling. The thresholds of telecommunications incidents will be defined by means of a regulation of the minister competent for computerisation, and the notification obligation will be imposed on the basis of meeting the criteria for reaching the thresholds. Article 20d sets out the details concerning the contents of a telecommunications incident notification. Article 20e regulates the information obligations imposed on electronic communications undertakings operating on the retail market. In the event of a particular and significant threat of a security incident, such undertaking shall inform the users potentially affected by such a threat about any possible protective measures or remedies which can be taken by the users, including their costs, which is the implementation of the first sentence of Article 40(3) of the EECC. Furthermore, such undertaking will be obligated to inform the users of the security incident itself and its impact on the availability of the services provided, [26 *European Electronic Communication Code, EECC - Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, replacing Directives 2002/19/WE, 2002/20/WE, 2002/21/WE, 2002/22/WE*], if, in its opinion, the impact of the security incident is significant, which is the implementation of the provisions laid down in the second sentence of Article 40(3) of the EECC. Article 20f concerns the obligation of an electronic communications undertaking to block communication, and limit or interrupt the provision of electronic communications services at the network termination point from where such communication is sent. Such measures are possible if a threat to the security of networks or services is identified, and can only be taken to the extent necessary to prevent the threat, and only for as long as the cause of such a threat persists. The amendment to Article 32 will make it possible for the CSIRT Telco to inform the entities within the national cybersecurity system about any vulnerabilities and any measures for removing them, if such information was obtained from the entities within the system. Pursuant to the new wording of Article 34, CSIRT Telco and sector-specific CSIRTs may cooperate with law enforcement and judicial authorities, as well as with special forces in fulfilling their statutory tasks. The newly introduced Article 34a concerns the issue of cooperation between national-level CSIRTs and the President of the Office of Electronic Communications during telecommunications incidents. These provisions implement Article 41 (4) and (5) of the EECC. The proposed amendments to Article 39 allow the CSIRT Telco to process personal data in the course of fulfilling its statutory tasks. The amendment to Article 39(3)(2) is a technical modification which results from repealing the existing Telecommunications Law. Due to adding Article 39(4)(4), the minister competent for computerisation, the Director of the Government Centre for Security, the Plenipotentiary and competent authorities for cybersecurity will be entitled to process personal data obtained from electronic communications undertakings in the

course of fulfilling their statutory duties in relation to cybersecurity threats and incidents.

The current position of telecommunications undertakings in the cybersecurity system is based on national laws, but the basic solutions in this respect are a consequence of the solutions adopted in the European Union law. Any differences concerning telecommunications undertakings refer both to counteracting and combating cybersecurity threats, and to providing information about the occurrence of such threats. Thanks to entrusting relevant tasks to the President of the Office of Electronic Communications (UKE), a possibility was provided to transfer information about incidents in the telecommunications sector to competent entities within the national cybersecurity system. The structure of sector-specific regulations in respect of cybersecurity in telecommunications corresponds to the structure of obligations imposed on operators of essential services, as provided for in general cybersecurity regulations.

The “NIS 2 Directive” aims to reform the provisions on the security of network and information systems. It is to help build a high level of cybersecurity in critical public and private sectors, such as health care and its facilities (e.g. hospitals, medical laboratories), energy networks, railways, public administration, as well as infrastructure and their services, thus significantly expanding the group of entities covered by it in relation to the so-called “NIS Directives”. The general direction of regulating key sectors, in particular the telecommunications sector and the public administration sector, in the common framework of the NIS 2 Directive, will allow for the creation of a coherent cybersecurity system, both at the EU level and at the national level. Including telecommunications, or more broadly the electronic communications sector, into a uniform legal system throughout the EU is important for several key reasons: 1. Such a solution is in line with the general market development tendency resulting from the increasing use of IT technologies in telecommunications (the effect of technological convergence). Today it is telecommunications that is the provider of the Internet, which is the basis for the provision of many strategic network services, such as cloud computing. The role of software in the construction of telecommunications services and systems is also growing. Media penetration is an everyday reality. It is therefore unjustified to separate the service layer from the regulation of the telecommunications infrastructure on which these services are “embedded”. The strategy of defense against cyber attacks must be comprehensive and rely on the protection of both networks and IT systems, up to end devices. The current legal status, both in the NIS Directive and in its implementation in the Polish Act on the National Cybersecurity System, caused a state of uncertainty. The NIS Directive exempted telecommunications undertakings pursuant to Article 1 para. 2 point 1 in terms of security and incident reporting requirements, and the EU legal system provided for a separate regulation for network security and integrity. This is a paradoxical situation, because in fact the NIS Directive concerned “security”, and without the security of the network layer, the security of the service is in many cases impossible to implement. This impotence of precise delimitation shows that it is impossible to create a coherent cybersecurity system without the participation of the telecommunications sector and the sector of Internet access service providers.

Annex No. 1, Sectors and subsectors and types of entities, defines the areas to be regulated

Sector	Subsector (if any)	Type of entity
Energy	Mineral extraction	Entities conducting business activities in the field of natural gas extraction, on the basis of a concession referred to in Article 22(1) of the Act of 9 June 2011—Geological and Mining Law. ^a
		Entities conducting business activities in the field of crude oil mining, on the basis of a concession referred to in Article 22(1) of the Act of 9 June 2011—Geological and Mining Law.
		Entities conducting business activities in the field of lignite mining, on the basis of a concession referred to in Article 22(1) of the Act of 9 June 2011—Geological and Mining Law.
		Entities conducting business activities in the field of hard coal mining, on the basis of a concession referred to in Article 22(1) of the Act of 9 June 2011—Geological and Mining Law.
		Entities conducting business activities in the field of mining of other minerals, on the basis of a concession referred to in Article 22(1) of the Act of 9 June 2011—Geological and Mining Law.
	Electricity	An energy company mentioned in Article 3 (12) of the Act of 10 April 1997—Energy Law (Polish Journal of Laws of 2020, item 833, as amended ^b), holding a licence to conduct business activities in the field of electricity generation.
		An energy company referred to in Article 3 (24) of the Act of 10 April 1997—Energy Law, holding a concession to conduct business activities in the field of electricity transmission.
		An energy company referred to in Article 3 (25) of the Act of 10 April 1997—Energy Law, holding a concession to conduct business activities in the field of electricity distribution.
		An energy company referred to in Article 3 (12) of the Act of 10 April 1997—Energy Law, holding a concession to conduct business activities in the field of electricity trading.
		An energy company referred to in Article 3 (12) of the Act of 10 April 1997—Energy Law, conducting business activities in the field of electricity processing or storage.
		Entities conducting business activities in the field of system, quality, and energy infrastructure management services.

(continued)

Sector	Subsector (if any)	Type of entity
	Heat	An energy company referred to in Article 3 (12) of the Act of 10 April 1997—Energy Law, holding a concession to conduct business activities in the field of heat generation.
		An energy company referred to in Article 3 (12) of the Act of 10 April 1997—Energy Law, holding a concession to conduct business activities in the field of heat trading.
		An energy company referred to in Article 3 (12) of the Act of 10 April 1997—Energy Law, holding a concession to conduct business activities in the field of heat transmission.
		An energy company referred to in Article 3 (12) of the Act of 10 April 1997—Energy Law, holding a concession to perform business activities in the field of heat distribution.
	Crude oil	An energy company mentioned in Article 3 (12) of the Act of 10 April 1997—Energy Law, holding a concession for the performance of business activities in the field of the production of liquid fuels, mentioned in Article 32(1) of the Act of 10 April 1997—Energy Law.
		Entities conducting business activities in the field of crude-oil transmission.
		An energy company mentioned in Article 3 (12) of the Act of 10 April 1997—Energy Law, holding a concession for conducting business activities in the field of liquid-fuels transmission through a pipeline network, mentioned in Article 32(1) of the Act of 10 April 1997—Energy Law.
		An entity conducting business activities in the field of crude oil storage, including the tankless underground storage of crude oil, referred to in Article 22(1) of the Act of 9 June 2011—Geological and Mining Law.
		Entities engaged in the business of crude oil transshipment.
		An energy company referred to in Article 3 (12) of the Act of 10 April 1997—Energy Law, conducting business activities in the field of liquid fuels storage, referred to in Article 32 (1) of the Act of 10 April 1997—Energy Law, and an entity conducting activities in the field of the tankless underground storage of liquid fuels, referred to in Article 22(1) of the Act of 9 June 2011—Geological and Mining Law.
		An energy company mentioned in Article 3 (12) of the Act of 10 April 1997—Energy Law, performing business activities in the field of the transshipment of liquid fuels, mentioned in

(continued)

Sector	Subsector (if any)	Type of entity
		Article 32(1) of the Act of 10 April 1997—Energy Law.
		An energy company mentioned in Article 3 (12) of the Act of 10 April 1997—Energy Law, performing business activities in the field of liquid fuel trading, or in the field of liquid fuel trading with foreign countries, mentioned in Article 32(1) of the Act of 10 April 1997—Energy Law.
		Entities conducting business activities in the field of synthetic fuel production.
	Gas	An energy company referred to in Article 3 (12) of the Act of 10 April 1997—Energy Law, conducting activities in the field of gaseous fuel generation, referred to in Article 3(45) of Act of 10 April 1997—Energy Law.
		An energy company referred to in Article 3 (12) of the Act of 10 April 1997—Energy Law, holding a concession to conduct business activities in the field of gaseous fuel transmission.
		An energy company referred to in Article 3 (12) of the Act of 10 April 1997—Energy Law, holding a concession to conduct business activities in the field of natural gas trading with foreign countries, or to conduct business activities in the field of trade in gaseous fuels.
		An energy company mentioned in Article 3 (24) of the Act of 10 April 1997—Energy Law, being a gas transmission-system operator appointed by the President of the Energy Regulatory Office.
		An energy company mentioned in Article 3 (25) of the Act of 10 April 1997—Energy Law, being a gas distribution system operator appointed by the President of the Energy Regulatory Office.
		An energy company mentioned in Article 3 (26) of the Act of 10 April 1997—Energy Law, being a gaseous fuel storage system operator appointed by the President of the Energy Regulatory Office.
		An energy company, mentioned in Article 3 (27) of the Act of 10 April 1997—Energy Law, being a natural gas liquefaction system operator appointed by the President of the Energy Regulatory Office.
	Supply and services for the energy sector	Entities conducting business activities in the field of the supply of systems, machines, equipment, materials, raw materials, and services for the energy sector.

(continued)

Sector	Subsector (if any)	Type of entity
Transportation	Supervised and subordinated units	Organisational units subordinated to or supervised by the Minister competent for energy.
		Organisational units subordinated to or supervised by the Minister competent for mineral resources management.
	Air transport	An air carrier referred to in Article 3(4) of Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002. ^c
		An airport manager referred to in Article 2(7) of the Act of 3 July 2002—Aviation Law. ^d
		An entrepreneur referred to in Article 177(2) of the Act of 3 July 2002—Aviation Law, performing for air carriers and other aircraft users one or more categories of services referred to in Article 176 of that Act, and an entrepreneur referred to in Article 186b(1)(2) of the Act of 3 July 2002—Aviation Law, performing tasks related to security control for air carriers.
		An air navigation service provider referred to in Article 127(1) of the Act of 3 July 2002—Aviation Law.
	Rail transport	A railway-infrastructure administrator, within the meaning of Article 4(7) of the Act of 28 March 2003 on Rail Transport ^e excluding the administrators of only the inactive infrastructure referred to in Article 4(1b) of this Act, and the private infrastructure, referred to in Article 4 (1c), and the narrow-gauge railway infrastructure referred to in Article 4(1d) of this Act. A railway undertaking referred to in Article 4 (9) of the Act of 28 March 2003 on Rail Transport, whose activities are subject to licensing, and an operator of a service facility referred to in Article 4(52) of the Act of 28 March 2003 on Rail Transport, if the entrepreneur performing the function of an operator is also a railway undertaking.
	Water transport	A shipowner in the maritime transport of passengers and goods, according to the definition of 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 ^f with the exception of individual ships which these shipowners operate.

(continued)

Sector	Subsector (if any)	Type of entity
		A shipowner referred to in Article 5(1) (2) of the Act of 21 December 2000 on Inland Navigation. ^g
		An entity managing the port referred to in Article 2(6) of the Act of 20 December 1996 on Ports and Sea Harbours. ^h
		A manager of a port facility referred to in Article 2(11) of Regulation (EC) No. 725/2004 of the European Parliament, and of the Council, of 31 March 2004, on enhancing ship and port facility security. ⁱ
		Entities conducting activities at ports supporting maritime transport.
		The VTS (Vessel Traffic Service)—an auxiliary apparatus of the Director of the Maritime Office established in order to monitor ship traffic and transfer information, constituting a component of the National SafeSeaNet System referred to in Article 91 of the Act of 18 August 2011 on Maritime Safety. ^j
	Road transport	Authorities referred to in Article 19(2), (5) and (5a) of the Act of 21 March 1985 on Public Roads. ^k
		Entities referred to in Article 43a(1) of the Act of 21 March 1985 on Public Roads.
	Banking and financial-markets infrastructure	A credit institution referred to in Article 4 (1) (17) of the Act of 29 August 1997—Banking Law. ^l
		The National Bank referred to in Article 4(1) (1) of the Act of 29 August 1997—Banking Law.
		A branch of a foreign bank referred to in Article 4(1)(20) of the Act of 29 August 1997—Banking Law.
		A branch of a credit institution referred to in Article 4(1)(18) of the Act of 29 August 1997—Banking Law.
		Cooperative savings and credit unions within the meaning of the Act of 5 November 2009 on Cooperative Savings and Credit Unions. ^m
		An entity operating the regulated market referred to in Article 14(1) of the Act of 29 July 2005 on Trading Financial Instruments. ⁿ
		An entity referred to in Article 3(49) of the Act of 29 July 2005 on Trading Financial Instruments

(continued)

Sector	Subsector (if any)	Type of entity
		An entity referred to in Article 48(7) of the Act of 29 July 2005 on Trading Financial Instruments.
Healthcare		A healthcare entity referred to in Article 4(1) of the Act of 15 April 2011 on Healthcare Activities (Journal of Laws of 2018, item 160, 138, 650, 1128, 1375 and 1532).
		A unit subordinated to the Minister competent for health, responsible for healthcare-information systems.
		National Health Fund.
		A healthcare entity within which the hospital pharmacy department operates, within the meaning of the Act of 6 September 2001—Pharmaceutical Law ^o
		A healthcare entity within which a hospital pharmacy operates, within the meaning of the Act of 6 September 2001—Pharmaceutical Law.
		An entrepreneur conducting the activities of a pharmaceutical wholesaler, within the meaning of the Act of 6 September 2001—Pharmaceutical Law.
		An entrepreneur or an entity conducting business activities in a Member State of the European Union or a Member State of the European Free Trade Association (EFTA)—a party to the agreement on the European Economic Area which has obtained marketing authorisation for a medicinal product.
		An importer of a medicinal product/active substance within the meaning of the Act of 6 September 2001—Pharmaceutical Law.
		A manufacturer of a medicinal product/active substance within the meaning of the Act of 6 September 2001—Pharmaceutical Law.
		A parallel importer within the meaning of the Act of 6 September 2001—Pharmaceutical Law.
		A distributor of active substances within the meaning of the Act of 6 September 2001—Pharmaceutical Law.
		An entrepreneur operating as a commercial pharmacy within the meaning of the Act of 6 September 2001—Pharmaceutical Law.
The supply and distribution of drinking water		A water supply and sewage company referred to in Article 2(4) of the Act of 7 June 2001 on Collective Water Supply and Collective Sewage Disposal ^p

(continued)

Sector	Subsector (if any)	Type of entity
Digital infrastructure		An entity which provides DNS services.
		An entity operating an Internet Exchange Point (IXP), which is a network facility which allows interconnection between more than two independent autonomous systems, mainly for the purpose of facilitating Internet traffic exchange.
		An entity managing the registration of Internet domain names within a top-level domain (TLD).

^aAct of 9 June 2011—Geological and Mining Law, consolidated text Polish Journal of Laws of 2020, item 1064

^bAct of 10 April 1997—Energy Law, consolidated text Polish Journal of Laws of 2020, item 833, as amended

^cRegulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002, OJ EU 2008 L 97/72

^dAct of 3 July 2002—Aviation Law, consolidated text Polish Journal of Laws of 2020, item 1970, as amended

^eAct of 28 March 2003 on Rail Transport, consolidated text Polish Journal of Laws of 2020 No. 20, item 1043, as amended

^fRegulation (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 2004 L 129/6

^gAct of 21 December 2000 on Inland Navigation, consolidated text Polish Journal of Laws of 2020, item 1863, as amended

^hAct of 20 December 1996 on Ports and Sea Harbours, consolidated text Polish Journal of Laws of 2020, item 998, as amended

ⁱRegulation (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 2004 L 129/6

^jAct of 18 August 2011 on Maritime Safety, consolidated text Polish Journal of Laws of 2020, items 680, as amended

^kAct of 21 March 1985 on Public Roads, consolidated text Polish Journal of Laws of 2020, item 470, as amended

^lAct of 29 August 1997—Banking Law, consolidated text Polish Journal of Laws of 2020, item 1896, as amended

^mAct of 5 November 2009 on Cooperative Savings and Credit Unions, consolidated text Polish Journal of Laws of 2020, item 1643, as amended

ⁿAct of 29 July 2005 on Trading Financial Instruments, consolidated text Polish Journal of Laws of 2020, item 89, as amended

^oAct of 6 September 2001—Pharmaceutical Law, consolidated text Polish Journal of Laws of 2020, item 944, as amended

^pAct of 7 June 2001 on Collective Water Supply and Collective Sewage Disposal, consolidated text Polish Journal of Laws of 2020, item 2028

References

Borkowski J (1996) In: Adamiak B, Borkowski J (eds) Kodeks postępowania administracyjnego, Komentarz. C.H. Beck, Warsaw

- Ganczar M (2009) Informatyzacja administracji publicznej. Nowa jakość usług publicznych dla obywateli i przedsiębiorców, Warszawa
- Knosala E Matan A Zacharko L (1996) Zarys nauki administracji. Katowice
- Pawłowski A (2002) Zasoby informacyjne w administracji publicznej w Polsce. Lublin
- Szafl L (1957) O niektórych problemach dotyczących zakresu postępowania przygotowawczego, Nowe Prawo 12

Katarzyna Chałubińska-Jentkiewicz dr. hab. of legal sciences (University of Warsaw and the Jagiellonian University), legal advisor, associate professor, and head of the Department of Cybersecurity Law and New Technologies at the Institute of Law in the Faculty of National Security at the War Studies University in Warsaw. She is also a lecturer at the SWPS University and director of the Academic Center for Cybersecurity Policy. In the years 1996–2010, she worked as a lawyer in the National Broadcasting Council and with the public broadcaster TVP S.A. Between 2011 and 2017, she was deputy director of the National Audiovisual Institute (her competence centered on the field of digitization). As a scientist, she conducts research on cybersecurity, information security threats, the development of electronic media law, protection of intellectual property, and the impact of new technologies on the development of the state and the legal situation of the individual. Katarzyna Chałubińska-Jentkiewicz is the author of monographs and numerous articles, which include topics such as new technologies law, cyber responsibility, information security law, and audiovisual media: Regulatory conflict in the age of digitization, Audio visual media services; Regulation in the conditions of digital conversion; Information and computerization in public administration; Cultural Security Law and Reuse of public sector information. She is head of the Ministry of Science's research project "Polish cybersecurity system—a model of legal solutions."

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.