Role of the Minister Competent for Computerisation in the Cybersecurity System

Katarzyna Chałubińska-Jentkiewicz

Abstract A public administration authority, as a functional unit of public administration, is responsible for the implementation and quality of public services. The areas of competence of administrative authorities often refer to a specific field. This is also the case with computerisation. The processes it involves are closely related to innovation, new technologies and science. Computerisation has formed the substantive area of activities of various ministries. The minister competent for computerisation performs a range of organisational and reporting tasks and is responsible for the monitoring the implementation of the Cybersecurity Strategy of the Republic of Poland and the performance of action plans for its implementation. The minister prepares annual reports on significant incidents reported by operators of essential services and substantial incidents reported by digital service providers, being responsible for monitoring the strategic dimension of cybersecurity.

Military and civil security issues are central in the activities of public administration authorities related to cybersecurity and the fulfilment of responsibilities in this field involves both the public and the private sectors. It is the public administration authority as a functional unit that is responsible for the delivery and quality of public services. The spheres of responsibility of administrative authorities often involve a specific sector. The same applies to computerisation. Computerisation processes are closely related to innovation, new technologies, and science. Computerisation has been one of the core objectives of various Ministries. Changes to this arrangement, and consequently to the responsibility for this aspect of state and public-administration functioning, have been commensurate with the transformation of public administration itself, and the processes related to it. Therefore, the Regulation of the Council of Ministers of 18 March 2003 on the establishing of the Ministry of Science and Computerisation, and the abolition of the office of the Scientific

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

K. Chałubińska-Jentkiewicz et al. (eds.), *Cybersecurity in Poland*,
https://doi.org/10.1007/978-3-030-78551-2_17

Research Committee,[1] introduced the concept of computerisation to the Ministry of Science and Computerisation which was being formed at the time. From 2005, public administration, computerisation, internal affairs, religious denominations, and national and ethnic minorities were the domain of the Minister of Internal Affairs and Administration.[2] In accordance with the principle of the division of responsibilities between the Ministries, the objectives related to computerisation were assigned by law. Pursuant to the Act on Government Administration Departments, the legislators made distinctions by subject matter. The Minister competent for digital affairs is responsible for matters of computerisation. In accordance with Article 12a of the Act, the computerisation department deals with issues involving:

(1) the computerisation of public administration and entities performing public tasks
(2) information and communication systems and networks of public administration
(3) support for computerisation projects
(4) the fulfilment of the international obligations of the Republic of Poland in the fields of computerisation and telecommunications
(5) participation in developing the European Union's computerisation policy
(6) the development of the information society, and counteracting digital exclusion
(7) the development of services provided by electronic means
(8) the development of state policy on personal data protection
(9) telecommunications
(10) **the civil aspect of cyberspace security**
(11) the PESEL register, Register of Identity Cards, Civil Registry, and the Central Register of Issued and Cancelled Passport Documents
(12) the vehicle register, drivers' register, and parking-card holders' register
(13) the supervision over the provision of trust services within the meaning of trust-services regulations
(13a) electronic identification.

The Prime Minister determines, by way of a regulation, the detailed scope of a Minister's activities, and designates a Ministry or other government administration office to assist the Minister. The Prime Minister, in specifying the detailed scope of the Minister's activity (in the case of a Minister managing a specific department of government administration), designates the department or departments which the Minister manages, and defines the scope of the Minister's rights as the administrator of a separate part or separate parts of the state budget.

Pursuant to the Regulation of the Prime Minister of 22 September 2014 on the detailed scope of activities of the Minister for Administration and Digital Affairs,

[1]Regulation of the Council of Ministers of 18 March 2003 on the establishing of the Ministry of Science and Computerisation, and the abolition of the office of the Scientific Research Committee, Polish Journal of Laws of 2003 No. 51, item 443 (no longer in force).

[2]The Regulation of the Prime Minister of 31 October 2005 on the detailed scope of activities of the Minister for Internal Affairs and Administration.

Article 1 (1) stipulates that the scope of activities of the Minister for Administration and Digital Affairs should include matters concerning public administration and computerisation. Pursuant to Order No. 43 of the Prime Minister of 15 July 2014 on granting a charter to the Ministry of Administration and Digital Affairs, a provision was introduced which, pursuant to Article 39 (5) of the Act of 8 August 1996 on the Council of Ministers, the Ministry for Administration and Digital Affairs was duly assigned the charter, which was an annex to the Order, the aim being to support the responsible Minister of Administration and Digital Affairs on the basis of the Regulation of the Prime Minister of 22 September 2014 on the detailed scope of activities of the Minister of Administration and Digital Affairs, which involved public administration and computerisation.

Next, under the Regulation of the Council of Ministers of 7 December 2015 on the Establishment of the Ministry for Digital Affairs under Article 39 (1) of the Act of 8 August 1996 on the Council of Ministers, the creation of the Ministry of Digital Affairs was ordered by way of the reorganisation of the existing Ministry of Administration and Digital Affairs. The reorganisation involved the exclusion from the existing Ministry of Administration and Digital Affairs—responsible for the departments of public administration, computerisation, communication, and religious denominations, and national and ethnic minorities—the organisational units supporting the departments of public administration, communication, and religious denominations, as well as national and ethnic minorities and employees working for those departments. In accordance with the Regulation of the Prime Minister of 13 December 2017 on the detailed scope of activities of the Minister of Digital Affairs, the Minister manages the department of Government Administration—computerisation.[3] Consequently, he or she would be the administrator of part 27 of the State budget. The services for the Minister were to be provided by the Ministry of Digital Affairs.

Currently the Minister for Digital Affairs does not have his own organizational unit (ministry), but is supported by the Chancellery of the Prime Minister.[4]

Article 45 of the National Cybersecurity System Act defines the competences of the minister competent for computerisation, who is competent for:

(1) monitoring the implementation of the Cybersecurity Strategy of the Republic of Poland, and associated action plans;
(2) recommending the spheres of cooperation with the private sector in order to increase the cybersecurity of the Republic of Poland;
(3) preparing annual reports regarding:

[3]Regulation of the Council of Ministers of 13 December 2017 on the detailed scope of activities of the Minister of Digital Affairs, Polish Journal of Laws of 2017 item 2327.

[4]Regulation of the Council of Ministers of 6 October 2020 on the detailed scope of activities of the Minister of Digital Affairs, Polish Journal of Laws of 2020 item 1716.

(a) serious incidents notified by operators of essential services affecting the continuity of their essential services in the Republic of Poland and in the Member States of the European Union;
(b) significant incidents notified by digital service providers, including those involving two or more European Union Member States;

(4) conducting informational activities on good practices, educational programmes, campaigns, and training, to expand knowledge and build awareness of cybersecurity, including the safe use of the Internet by various categories of users
(5) collecting information on serious incidents which concerns, or has been provided by, another Member State of the European Union
(6) providing information and good practices related to the reporting of serious incidents by operators of essential services, and significant incidents by digital service providers, obtained from the Cooperation Group, including

(a) incident-management procedures
(b) risk-management procedures
(c) the classification of information, risks, and incidents

The Act imposes a range of organisational and reporting obligations on the Minister competent for computerisation. The Minister competent for computerisation is responsible for monitoring the implementation of the Cybersecurity Strategy of the Republic of Poland and associated action plans, and preparing annual reports on serious incidents notified by operators of essential services and significant incidents notified by digital service providers, with responsibility for the strategic monitoring cybersecurity at the national level. It is important to add that these responsibilities, according to the division between government departments, also include issues of cybersecurity in the civil dimension. Accordingly, the Minister of National Defence is responsible for the security of cyberspace in the military sphere, indicated as part of the national defence department.

The responsibilities provided for in the said provision relate to the following obligations of the Member States as defined in the Directive:

(1) **Monitoring the implementation of the Cybersecurity Strategy of the Republic of Poland, hereinafter referred to as "the Strategy", and the delivery of action plans for its introduction**

This includes supervision over the implementation of Poland's strategic cybersecurity objectives. The strategy builds on the actions undertaken previously by government administration, aimed at increasing the level of security in the cyberspace of the Republic of Poland. Following strategic assumptions, both national-development strategies and those relating to the sphere of public order and national security make their success conditional on the use of communication and information systems. Not only is digitisation a source of development and innovation, but it also creates risks associated with the growing number of online threats. Considering these new threats, the extensive architecture of communication and information systems, and the growing dependence of society and entrepreneurs on these systems, it is necessary to expand the national cybersecurity system and ensure a coherent

approach across the country. The main objective of the Strategy is to define a framework of actions aimed at achieving a high level of resilience for national communication and information systems, operators of essential services, critical infrastructure operators, digital service providers, and public administration, to incidents in cyberspace. Furthermore, the proposed strategic policies are also expected to increase the effectiveness of law-enforcement agencies and the judiciary in detecting and combating crimes and terrorist and spying activities in cyberspace. The strategic objectives include specific goals, such as gaining the ability to coordinate nationwide activities aimed at preventing, detecting, combating, and minimising the effects of incidents which compromise the security of communication and information systems central to the functioning of the state, reinforcing the ability to counteract cyber threats, improving national capabilities and expertise in the field of cybersecurity, and developing a strong international position for Poland in the field of cybersecurity.

Moreover, it is essential to achieve a capacity for nationally coordinated actions to prevent, detect, combat, and minimise the effects of security incidents on communication and information systems central to the functioning of states, and to adapt the legal environment to the requirements and challenges in the field of cybersecurity.

(2) **Recommending areas of cooperation with the private sector in order to improve the cybersecurity of the Republic of Poland.**

The need for cross-sectoral cooperation was indicated by the European Union's Cybersecurity Strategy: an open, secure, and protected cyberspace enhances private-sector readiness and engagement. This strategy stressed the fact that the vast majority of network and information systems are independently owned and operated by private entities, and that the deeper involvement of the private sector in the efforts to enhance cybersecurity is essential. The private sector should develop its own cyber resilience capabilities at the technical level, and ensure the exchange of best practices between different industries. Equally, the public sector should benefit from the instruments developed by the industry to respond to incidents, identify causes, and conduct forensic analyses. The purpose of the discussed regulation is, therefore, to create a situation in which entities operating in many critical areas (energy, transport, banking, stock exchanges, and technologies facilitating the provision of essential online services, as well as public-administration authorities) assess the cybersecurity threats they are exposed to, ensure the reliability and resilience of the network and information systems employing the appropriate risk-prevention strategies, and exchange information with the competent network and information-security authorities. The European Public-Private Partnership for Resilience was launched in accordance with document COM (2009) 149.[5] This platform has

[5]Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience,* COM (2009) 149.

initiated activities by and increased cooperation between the public and private sectors in identifying key resources, means, functions, and baseline requirements for resilience, as well as the demand for cooperation and mechanisms for responding to large-scale electronic-communications disruptions. Communication from the Commission: Joint Communication to the European Parliament and the Council—Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels, 13.9.2017. JOIN(2017) 450 final, emphasised that the effectiveness of traditional law-enforcement mechanisms has been undermined by the characteristics of the digital world, which consists mainly of privately owned infrastructures and multiple entities operating within various jurisdictions. In consequence, cooperation with the private sector, including industry and civil society, is fundamental to the public authorities' effective fight against crime. However, the role as defined above is the implementation of the aforementioned guidelines at the level of government administration.

(3) **Preparing annual reports regarding:**

   (a) serious incidents reported by operators of essential services affecting the continuity of their essential services in the Republic of Poland and the continuity of their essential services in the Member States of the European Union
   (b) significant incidents notified by digital service providers, including incidents involving two or more Member States of the European Union.

(4) **conducting informational activities on good practices, educational programmes, campaigns, and training, to increase knowledge and build awareness of cybersecurity, including the safe use of the Internet by various categories of users**
(5) **collecting information on serious incidents which involves or has been provided by another Member State of the European Union**
(6) **providing information and good practices related to the reporting of serious incidents by operators of essential services, and significant incidents by digital service providers, obtained from the Cooperation Group, including**

   (a) incident-management procedures
   (b) risk-management procedures
   (c) the classification of information, risks, and incidents.

Strategic cooperation between Member States, and the exchange of information, experience, and best practices concerning the security of network and information systems are essential to respond effectively to the challenges posed by security incidents and threats to those systems across the Union. These tasks also apply to cross-sectoral information exchange, especially in the field of educational activities and the application of good practices. These responsibilities are supported by extensive reporting. This reporting includes issues related to the duties referred to in recital 61 of the NIS Directive, according to which competent authorities should have the necessary means to perform their duties, including the power to obtain sufficient information to assess the security level of network and information

systems. The NIS Directive defines such a concept as "an incident", which means any event which has a genuinely adverse impact on the security of network and information systems; "incident handling", which means all procedures for detecting, analysing, containing, and responding to an incident; and **"risk", which means any reasonably identifiable circumstance or event which has a potentially adverse impact on the security of network and information systems**. According to the definitions provided in the Act: an "incident"—an event which has or might have an adverse effect on cybersecurity; a "critical incident"—one which results in significant damage to public security or order, international interests, economic interests, the operation of public institutions, civil rights and the freedoms or the lives and health of the people, as classified by the respective CSIRT MON, CSIRT NASK, or CSIRT GOV; a "serious incident"—an occurrence which causes or is likely to cause a significant deterioration in or disruption to the provision of an essential service; and a "significant incident"—an event which has a serious impact on the provision of a digital service within the meaning of Article 4 of 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.[6] Risk, in turn, means a combination of the probability of an undesirable event and its consequences, and risk estimation means the overall process of risk identification, analysis, and evaluation. Therefore, reporting includes gathering information on the incidents themselves, as well as providing information obtained from the Cooperation Group—within the scope of developed cybersecurity procedures, as well as the measures applied and all kinds of regulations on preventive actions related to the application of so-called good practices in incident response. The second pillar of the NIS Directive primarily involves cooperation between Member States. The NIS Directive introduces cooperation mechanisms on two levels: technical, and political-strategic. Technical cooperation is to be provided by the European CSIRT Network and the creation of mechanisms for the exchange of information on cross-border incidents between CSIRTs designated for operators of essential services and digital service providers. Cooperation at the political and strategic levels is to be implemented through the creation of a Cooperation Group which will work on the development of common strategic concepts and will receive, among other things, annual reports from the appropriate authorities. In accordance with recital 4 of the preamble to the Directive, a Cooperation Group composed of representatives of Member States, the Commission and the European Union Agency

[6]Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, OJ EU 2018 L 26/48 (hereinafter referred to as "Implementing Regulation 2018/151).

for Network and Information Security (nowadays: the European Union Agency for Cybersecurity; hereinafter referred to as "ENISA") should be established to promote and facilitate strategic cooperation between Member States on the security of network and information systems. In order for this group to be effective and accessible to all, it is essential that all Member States have at least the minimum capabilities, and strategy, to ensure a high level of security of network and information systems on their territory. Additionally, security and incident-reporting requirements should apply to operators of essential services and digital service providers for the promotion of a risk-handling culture, and to ensure that the most serious incidents are reported. Article 11 of the NIS Directive establishes a Cooperation Group composed of representatives of the Member States, the Commission, and ENISA. According to Article 11 of the NIS Directive, the Cooperation Group is to perform its tasks on the basis of biennial work programmes. The responsibilities of the Group include providing strategic guidance on the activities of the computer security incident response teams network, exchanging information and best practices, and discussing Member States' capabilities and preparedness. The Cooperation Group is also obliged to submit, every year and a half, a report evaluating the experience gained in its strategic cooperation. It is also responsible for discussing, at the request of a Member State, specific draft national measures by that Member State concerning the identification of operators of essential services in a particular sector. According to Article 14(7) of the NIS Directive, competent authorities, acting jointly within the framework of the Cooperation Group, may develop and adopt guidelines on the circumstances in which operators of essential services are required to report incidents, including guidelines on parameters to determine the significance of the impact of an incident. The Cooperation Group should be presided over by a representative of the Member State holding the Presidency of the Council of the European Union. The Chairperson should be assisted in the performance of his or her duties by a representative of the Member State holding the previous Presidency of the Council of the European Union, and a representative of the Member State which will hold the next Presidency. The Chairperson may indicate the duties in respect of which he or she will need such support. In the event that the Member State holding the Presidency of the Council decides not to preside over the Group, a two-thirds majority of the members of the group shall elect a replacement Chairperson.

The responsibilities of the Cooperation Group as defined in the Directive are:

(a) providing strategic guidance on the activities of the CSIRTs network;
(b) exchanging best practice on information exchange related to incident reporting
(c) exchanging best practice between Member States, and, in collaboration with ENISA, assisting Member States in capacity building with a view to ensuring the security of network and information systems
(d) discussing Member States' capabilities and preparedness, and, on a voluntary basis, assessing national strategies for network and information system security and the effectiveness of CSIRT, and identifying best practice
(e) exchanging information and best practices on awareness raising and training
(f) exchanging information and best practices on research and development relating to the security of network and information systems

(g) where relevant, exchanging experiences on matters relating to the security of network and information systems with the relevant Union institutions, bodies, offices, and agencies
(h) discussing the standards and specifications with representatives from the relevant European standardisation organisations
(i) collecting information on best practice for risks and incidents
(j) examining the summary reports on an annual basis
(k) discussing the work undertaken with regard to exercises on network and information-systems security, education programmes and training, including the work performed by ENISA
(l) with the assistance of ENISA, exchanging best practice with regard to the identification of the operators of essential services by the Member States, including in relation to cross-border dependencies, regarding risks and incidents
(m) discussing the rules on incident reporting.

In performing his or her duties, the Chairperson should be guided by the principles of inclusiveness, commitment, respect for diversity, and the pursuit of consensus. In accordance with Article 11(2) of the NIS Directive, the Cooperation Group may, where appropriate, invite representatives of influential stakeholders to participate in its meetings. In order to ensure that acceding countries meet the requirements specified in the NIS Directive from the date of their accession, representatives of these countries should be invited to participate in the meetings of the Cooperation Group from the date of signing the Treaty of Accession to the EU. The decision to invite representatives of important stakeholders or experts to participate in a meeting, or part of a meeting, of the Group, should be taken by the Chairperson, unless a simple majority of members oppose the participation in the meeting or part of it by the representative or expert concerned. In order to facilitate its activities, the Cooperation Group should be able to create subgroups. The meetings of the Group are convened by the Chairperson, either on his or her own initiative or at the request of a simple majority of its members. The Chairperson shall present a provisional agenda for meetings during his or her term of office, taking into consideration the work programme of the Group. In general, the Group's discussions should not be publicly accessible, as making them open to the public could have a negative impact on building mutual trust between members, since they often address public security issues. However, after consultation with the Chairperson, the Group may decide to make public its deliberations on specific issues, and to facilitate making appropriate documentation publicly available. Requests to the Group for access to the documents relating to its activities shall be considered by the Commission in accordance with Regulation (EC) No. 1049/2001 of the European Parliament and of the Council. The Group's discussions are not public. In consultation with the Chairperson, the Group might decide to make public its deliberations on certain issues. Documents distributed to members of the Group, representatives of third parties, and experts, shall not be made available to the public unless access is granted or otherwise provided for by the Commission.

Pursuant to Article 46 of the Act, the Minister competent for computerisation shall ensure the development or maintenance of a communication and information system to support:

(1) cooperation between entities within the national cybersecurity system
(2) the generating and presenting of recommendations for actions to increase the level of cybersecurity
(3) the reporting and handling of incidents
(4) risk estimation at the national level
(5) alerts regarding cybersecurity threats.

According to the EU strategy, national NIS authorities should cooperate on and exchange information with other regulatory authorities, in particular data-protection authorities, and regularly publish on dedicated websites unclassified information on current early warnings about incidents and threats and the coordinated responses. Integrated computerisation involves a comprehensive, managerial, and organisational approach to building the state's information and communication system by public administration, which is expected to lead to developing information and communication governance in the state. The creation, development, and maintenance of a state information and communication system supports all the crucial procedures related to cybersecurity.

The establishment of the appropriate organisational areas at all levels, from independent institutions to departmental and local government activities, and building, providing, and maintaining a basic set of electronic services facilitating incident handling all require an effective combination of various public-administration activities. For administrative processes which involve different sectors, cross-sectoral projects seem essential. This is important, considering the required functionality of such a system, including aspects of information exchange, educational issues, real threats, alerting actions, and risk estimation. A communication and information system is one in which data is sent, received, stored, and processed by means of telecommunications networks. A service provided by electronic means does not include a transmission within the internal network of a given entrepreneur[7]—the intranet. Pursuant to Article 2(3) of the Act on Providing Services by Electronic Means, a communication and information system is a set of cooperating IT devices and software, ensuring processing and storage, as well as sending and receiving data through telecommunications networks by means of a terminal device appropriate for a given type of telecommunications network within the meaning of the Act of

[7]Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, OJ EU 2018 L 26/189.

16 July 2004—Telecommunications Law.[8] The communication between IT devices is based on the TCP/IP protocol used. The most important here is the IP protocol, which is responsible for assigning a logical IP address to each computer which is connected to the TCP/IP network.[9] The construction of the state communication and information system should be carried out in close cooperation with all the entities which are part of the national cybersecurity system. The legislators have defined the system's functionalities, which include cooperation between entities within the national cybersecurity system, the generation and transmission of recommendations for actions to increase the level of cybersecurity, incident reporting and handling, risk assessment at the national level, and warnings about cyber hazards.

The CSIRT MON, CSIRT NASK, and CSIRT GOV, sectoral cybersecurity teams, and the President of the Office of Electronic Communications may use the communication and information system under an agreement concluded with the Minister competent for computerisation.

The entities involved in the process of managing cybersecurity require enhanced security of communication systems and IT support. The Government Communications Network (GCN) was established in order to ensure the protection of information against unauthorised disclosure during telephone and video-conferencing conversations and data transmission, in particular against the loss of confidentiality, availability, and integrity.

However, the dynamic development of ICT networks, and their increasing use for data transmission, as well as for command and management, naturally made it necessary to guarantee security for the operation of the networks themselves, and for the information transmitted therein.

Therefore, the above provision ensures cooperation between the President of the Office of Electronic Communications (OEC) and other bodies—Computer Security Incident Response Teams—whose main task is to ensure the implementation and coordination of the processes of preventing, detecting, and responding to computer incidents involving communication and information systems and networks, as well as cooperation in the sphere of preventing cyber attacks. The CSIRT GOV Computer Security Incident Response Team is managed by the Head of the Internal Security Agency, and operates as a national-level CSIRT Team responsible for coordinating the process of responding to computer incidents occurring in the fields indicated in Article 26(7) of the Act of 5 July 2018 on the National Cybersecurity System. Among its fundamental tasks are recognising, preventing, and detecting threats which are detrimental to security, and important from the point of view of the continuous functioning of the state's communication and information systems of public administration authorities, and of the system of ICT networks covered by a standard list of objects, installations, devices and services categorised as critical infrastructure, as well as of the communication and information systems of owners

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

[9]Gołaczyński (2009), p. 34.

and the holders of facilities, installations, and devices of critical infrastructure referred to in Article 5b(7)(1) of the Act of 26 April 2007 on Crisis Management. CSIRT GOV and CSIRT MON, whose main task is to ensure the implementation and coordination of the processes of preventing, detecting and responding to computer incidents in the Ministry for National Defence's communication and information systems and networks, as well as CSIRT NASK, whose tasks include the monitoring of cybersecurity threats and incidents at the national level, are permitted to implement their tasks using the communication and information system operated by the Ministry for Information Technology. This usage is based on an agreement.

The legislators have decided that the basic terms and conditions for the use of communication and information systems to serve cybersecurity, and the scope of such use, will be agreed between the parties to the agreement. It should be assumed that there is also going to be an administrative agreement. The main goal of the entities concluding the agreement is the implementation of designated public tasks within the communication and information system, and the conditions and scope of this use are defined in the agreement. This form of public-administration activity is similar to civil-law contracts, which have the effect of administrative agreements primarily concerning the sphere of public law. As a rule, the mandatory provisions of this agreement have not been defined by the legislators. Nevertheless, taking into consideration the essence and purpose of the agreement on the conditions and scope of the use of the communication and information system, the agreement should specify, in particular, the parties to the agreement, its duration, whether the agreement has been concluded for a definite period of time, the subject matter of the agreement, the provisions concerning supervision over the use of the system, and the provisions concerning the form of amending or terminating the agreement.

In accordance with Article 47 of the Act on the National Cybersecurity System, the Minister competent for computerisation may perform the tasks referred to in Article 45(1) and Article 46(1) subject to the rules specified in separate provisions by means of units responsible in this respect which are subordinated to or supervised by the Minister competent for computerisation. A significant role in the implementation of tasks related to digitalisation and computerisation processes is performed by the advisory units of the Minister competent for computerisation. Such a unit is the Council for Computerisation. Pursuant to Article 17 of the UIDP the Council for Computerisation was established, whose name under the amendment of 10 January 2014[10] was changed to the Council for Computerisation. It is a consultative and advisory authority of the Minister competent for computerisation. Opinions, minutes of meetings, and other Council documents are published in a separate part of the Public Information Bulletin on the website of the Minister competent for computerisation. The Council shall present a report on its activities for each calendar year to the Minister by 30 April of the following year. The responsibilities of the Council include:

[10]Polish Journal of Laws of 2014, item 183.

(1) suggesting and providing opinions on the draft positions of the Council of Ministers on the documents of the European Commission and the European Parliament concerning computerisation, communication, and the development of the information society, at the request of the Minister competent for computerisation, including issuing opinions on the draft of the Integrated State Computerisation Programme and other government documents, including draft development strategies and draft programmes within the meaning of the Act of 6 December 2006 on the Principles of Conducting the Development Policy concerning matters of computerisation, communication or the development of the information society;
(2) issuing opinions on draft regulations published pursuant to Article 18 of the UIDP
(3) providing opinions on other draft legal Acts and other documents submitted by the Minister competent for computerisation, communication, or information society development
(4) providing opinions on reports and other studies on the computerisation of the Minister competent for computerisation

   (a) requirements and demands concerning the development of the information society
   (b) the principles of the functioning of public registers
   (c) the principles of the implementation of communication and information systems in public administration, and the status of their implementation
   (d) the current technical solutions applicable to the computerisation of administration, network development, and broadband services
   (e) Polish terminology in the fields of computer science and communications.

The Council is composed of fifteen to twenty members. Candidates for membership of the Council may be recommended by:

(1) Ministers
(2) the General Director of the State Archives
(3) the President of the Polish Committee for Standardisation
(4) the co-Chairperson of the Joint Commission of Government and Local Government
(5) scientific entities within the meaning of the Act of 30 April 2010 on the principles of science financing (Polish Journal of Laws of 2010, No. 96, item 615, as amended), which, within the framework of their statutory activities, conduct scientific research or development work in the fields of information technology and communications
(6) Chambers of Commerce representing entrepreneurs conducting business activities in the fields of the electronic economy, communications, media, the manufacturing of IT equipment, software, or providing IT services
(7) associations registered in the National Court Register whose statutory purpose is to represent the IT environment or to support the applications of IT, the electronic economy, communications, or media.

The Minister competent for computerisation appoints the members of the Council for a biennial term of office from among the candidates recommended by the entities indicated above.

The Minister competent for computerisation may appoint and dismiss the Chairperson and Deputy Chairperson of the Council from among its members. The Chairperson of the Council manages its work and represents the Council externally. In the event of the Chairperson's absence, the Deputy Chairperson shall replace him or her. The Council is supported by the office serving the Minister competent for computerisation. Other persons may be invited to meetings of the Council by the Minister competent for computerisation or the Chairperson of the Council, if it is advisable to do so in order to fulfil the tasks of the Council. The detailed procedure of the Council shall be established by its regulations, determined at the request of the Council by the Minister competent for computerisation. However, this institution has an exclusively advisory and consultative nature. The legislators have defined precisely which institutions are supervised by this authority.

Pursuant to the announcement of the Minister for Digital Affairs of 19 June 2018 on the list of organisational units subordinate to, or supervised by, the Minister for Digital Affairs, issued pursuant to Article 33(1d) of the Act on the Council of Ministers, a register of organisational units subordinate to, or supervised by, the Minister for Digital Affairs was established, constituting an appendix to the announcement. According to the announcement, the Digital Poland Projects Centre is a subordinate unit, while the following units are supervised: the Central Computer Science Centre; the Communications Institute—National Research Institute; and the Institute of Innovative Technologies EMAG and Scientific and Academic Computer Network—National Research Institute. Apparently, the scope of the delegation includes the institutions defined above.

It should be added that by Order No. 13 of the Minister for Digital Affairs of 2 May 2016 on the appointment and responsibilities of the Plenipotentiary of the Minister for Digital Affairs for International Cooperation, the Plenipotentiary of the Minister for Digital Affairs for International Cooperation was appointed, who is responsible for:

(1) representing and acting on behalf of the Minister for Digital Affairs in the international and national arenas on international issues
(2) strategic advice to the Minister for Digital Affairs on international activities
(3) developing with the Minister for Digital Affairs of a directional policy and international cooperation strategy of the Ministry
(4) monitoring the effective implementation of the Ministry's foreign policy on behalf of the Minister for Digital Affairs. Thus, the tasks of such a person include activities beyond the European Union and the regulation of the directive.

Furthermore, Order No. 30 of the Minister for Digital Affairs of 22 October 2017 on the establishment of the Operating Centre of the Minister for Digital Affairs established the Operating Centre of the Minister for Digital Affairs, which supports the implementation of the tasks of the Minister for Digital Affairs in the field of cybersecurity, as well as crisis management and defence, in particular on the security

of the civil sphere of cyberspace of the Republic of Poland and the system for responding to ICT incidents and civil planning. The Centre can serve as a separate place of permanent duty and as an HNS point of contact within the meaning of Article 1(2)(1) of Order No. 19 of the Minister for Digital Affairs of 15 June 2016 on the Functioning of the HNS System in the computerisation department of government administration for the purposes of tasks resulting from the duties of the host country (The Official Gazette of the Ministry for Digital Affairs, item 21). The Centre is deployed, if necessary, by recommendation of the Minister, a member of the Management of the Ministry of Digital Affairs, or, depending on the nature of the threat or event, at the request of the Head of the organisational unit nominated in the Instruction of the Operations Centre, or by the appropriate Head of the organisational unit for exercises in the fields of cybersecurity, crisis management, and defence. The following are the main tasks of the Centre:

(1) Supporting the Minister in managing the National Cybersecurity Centre[11] operating within the National Research Institute—the Scientific and Academic Computer Network, a unit supervised by the Minister competent for responding to ICT incidents.
(2) Ensuring close cooperation with other entities involved in responding to ICT incidents, in particular with the Internal Security Agency, the Government Security Centre, and the Police.
(3) Supervising and coordinating the activities of units subordinate to, or supervised by, the Minister in a crisis situation, or in circumstances of extraordinary threats, if justified by the scale or effects of the situation.
(4) Forwarding to the appropriate organisational units of the Ministry proposals for the development of draft decisions, positions, guidelines, and recommendations concerning cybersecurity, crisis management, and defence matters, for the purposes of the Ministry's management and the Crisis Management Team of the Minister for Digital Affairs.
(5) Analysing the situation, coordinating and directing the activities of the Ministry in the event of an emergency situation causing disruptions to the functioning of IT systems, networks, or telecommunication services, or when such disruptions affect the essential (basic) services provided to the public or public-administration systems, registers, or publications.
(6) Monitoring the development of a crisis situation where justified by its extent or consequences.
(7) Ensuring permanent communication with the Office of Electronic Communications and the NCSC in the event of a disruption to the functioning of IT systems, networks or telecommunication services, or when such a disruption affects essential services provided to the public or public-administration systems, registers, or publications.

[11] National Cybersecurity Centre, "the NCSC".

(8) Ensuring the circulation of information in a crisis situation for the management of the Ministry and the Crisis Management Team of the Minister for Digital Affairs.
(9) Providing a place to perform emergency duty in the event of an alert level, or CRP alert level, for persons authorised to make decisions on the security of communication and information systems—in accordance with the Act on Anti-Terrorist Activities
(10) Ensuring the circulation of information for the purposes of tasks included in the list of the undertakings and procedures of the crisis management system
(11) Coordinating designated support arising from the obligations of the host state (HNS) in the Ministry, the Office of Electronic Communications, and entrepreneurs with special economic and defensive importance within the meaning of Article 6(1)(2) and Article 18(1) and (3) of the Act of 21 November 1967 on the Universal Duty to Defend the Republic of Poland (Polish Journal of Laws of 2017, item 430).

Units subordinate to, or supervised by, the Minister ensure that the Centre is staffed on the basis of individual contracts and agreements. While on duty, the Centre cooperates with the Ministry's Press Officer on media monitoring and information policy.

It should be emphasised that the Centre's tasks are related to situations concerning national and internal procedures instigated in a crisis situation, while the procedures defined in the National Cybersecurity Act refer to the common objective of the EU, i.e. to provide common procedures for responding to cyber threats in the area of the EU Single Market. It can be observed that the tasks of different institutions and entities in the private sector can overlap, but in both systems, the Minister competent for computerisation remains the common coordinator.

The roles entrusted to these units, including in cybersecurity, are financed in the form of an earmarked subsidy from the part of the state budget which is administered by the Minister competent for digital affairs. According to the Regulation of the Prime Minister of ^ October 2020 on the detailed scope of activity of the Minister for Digital Affairs, this Minister is the administrator of part 27 of the state budget. Article 127 of the Public Finance Act[12] delineates a list of tasks for which funds from an earmarked subsidy may be used. The detailed regulations concerning particular types of designated subsidy, the rules for their granting, and the settlement and legal consequences related to irregularities in these processes, are specified in the Act. Earmarked subsidies may be allocated for financing or subsidising statutorily defined tasks, implemented by entities other than local government units. The amount of each grant so planned, in accordance with Article 215(2) of the PFA, should be additionally described, with the appropriate type of subsidy in question as an earmarked subsidy. Such a subsidy may be used by the beneficiary in connection

[12]Act from Public Finance, Polish Journal of Laws of 2019, item 869, as amended, hereinafter "the PFA".

with a public task only after the conclusion of a subsidy agreement. From the very nature of an earmarked subsidy, it follows that it may be utilised by the subsidy beneficiary in connection with the implementation of a public task only for expenditures incurred after the conclusion of the subsidy agreement. In addition, it follows from Article 251(2) of the PFA that the use of the subsidy is made in particular through payment for the tasks for which the subsidy was awarded, or, if separate regulations provide for the method of awarding and settling the subsidy, the utilisation of the subsidy is achieved through the implementation of the objectives indicated in these regulations. Therefore, since the provision of the subsidy is made on the basis of an agreement, use of the subsidy can only be made by paying for the completed tasks resulting from the subsidy agreement, and thus performed after it has been signed (the Resolution of the College of the Regional Chamber of Auditors in Kraków of 14 August 2013. KI-411212/2013—the essence of an earmarked subsidy NZS 2013/5/10).

The Minister competent for computerisation, as the single point of contact (Articles 48–50), has the responsibility to receive and forward, at the request of the appropriate CSIRT, reports of serious or significant incidents involving two or more Member States of the European Union to ensure the representation of the Republic of Poland within the Cooperation Group, to exchange information for the benefit of the public authorities and for the competent authorities in Poland and abroad, and the CSIRT, and to meet its reporting obligations to the Cooperation Group and the European Commission. In recent years there has been a growing interest in cybersecurity, which has resulted in an increasing number of units and organisations' dealing with this issue. Nevertheless, in order to perform public tasks in this area more effectively, cooperation and exchange of information between administrative, military, and civil areas are indispensable. The Cybersecurity Strategy of the European Union proposes an open, secure and protected cyberspace,[13] and a network of national cybersecurity authorities. According to the EU strategy, national NIS authorities should cooperate and exchange information with other regulatory authorities, in particular data-protection authorities, and regularly publish, on a dedicated website, unclassified information on current early warnings about incidents and threats, as well as about coordinated responses. According to the European Commission, legal obligations should not replace or prevent informal or voluntary cooperation, including between the public and private sectors, to increase security and exchange information and best practices. An especially important and useful platform at the EU level which needs to be developed is the European Public-Private Partnership for Resilience.[14] All these tasks are not the complete catalogue of

[13]COM (2013) from 7 February 2013 JOIN(2013) 1 final.

[14]The European Public-Private Partnership for Resilience was initiated under document COM (2009) 149. The platform launched activities and increased cooperation between the public and private sectors in identifying critical resources, means, functions, and baseline requirements, for resilience, as well as the need for cooperation and mechanisms for responding to large-scale disruptions affecting electronic communications.

requirements related to the protection of national security in the digital age. This is because the process of threat emergence is ongoing; therefore, the list of needs is constantly growing. These demands must be met by an appropriate, innovative selection of regulatory instruments, and without questioning these traditional measures. Digital democracy is a form of government operation which requires public authorities and public administration authorities to counteract all tendencies which have a negative impact on national security. Government administration and local government authorities are able to provide more efficient and more effective assistance in crisis situations related to ICT infrastructure if they receive the professional support of third-sector organisations. As the Strategy emphasises, the effectiveness of governmental organisations (the Polish Armed Forces, the Police, Guards, and Inspectorates) depends largely on proper specialist support from non-governmental organisations, which can provide as much assistance in various areas of national security as government administration units. In order for such cooperation to be real, it is necessary to provide information on potential threats, incidents, and rules adopted in individual Member States. This necessity is indicated in recital 43 of the Directive, according to which, due to the global nature of the problems related to the security of network and information systems, there is a need to strengthen international cooperation in order to improve security standards and information exchange, and also to promote a common holistic approach to security issues. For the purposes of achieving the above goals, a system of so-called points of contact was designed. According to Article 8 of the Directive, each Member State shall designate a national single point of contact for the security of network and information systems (known as "the single point of contact"). Member States may designate an existing body for this purpose. In Poland, such an authority is the Minister competent for digital affairs. Should a Member State designate only one competent authority, that competent authority is also the single point of contact. Pursuant to Article 8(2) of the Directive, the single point of contact shall have a connecting function to ensure cross-border cooperation between Member States' authorities and with the appropriate authorities in other Member States, as well as with the Cooperation Group and the CSIRT network. Member States are obligated to provide the competent authorities and single points of contact with sufficient resources to enable them to accomplish their tasks effectively and efficiently with a view to achieving the objectives of the Directive. Member States shall ensure that the designated representatives in the Cooperation Group are working together effectively, efficiently, and securely. The competent authorities and the single point of contact are required to, where appropriate, and in accordance with national law, consult and cooperate with the applicable national law-enforcement authorities and national data-protection bodies. Member States are obliged to notify the European Commission, without delay, of the designation of the competent authority and the single point of contact, their tasks, and any subsequent modifications thereto, and to make public the designation of the competent authority and the single point of contact. The European Commission shall publish the list of designated single points of contact.

The main responsibilities of points of contact:

(1) Receiving from the single points of contact in other Member States of the European Union reports of a major incident, or a significant incident, involving two or more Member States of the European Union, and forwarding these reports to CSIRT MON, CSIRT NASK, CSIRT GOV, or sectoral cybersecurity teams, i.e., obtaining and communicating information about an emergency situation from other points of contact in the EU, if the situation there is more extensive, i.e. involves more than one country; it should be noted that, according to recital 32 of the Directive, the competent authorities, or computer security incident response teams, (CSIRT's), should receive incident reports. The single points of contact should not receive any incident reports directly, unless they also operate as a competent authority or a CSIRT. However, the competent authority or CSIRT should be able to instruct the single point of contact to forward incident reports to single points of contact in other Member States affected by the incident.
(2) providing to the single points of contact in other Member States of the European Union, at the request of the appropriate CSIRT MON, CSIRT NASK, or CSIRT GOV, a report of a major incident or a significant incident involving two or more Member States of the European Union—i.e. acquiring and sharing information about such an incident with the other points of contact affected by the incident.
(3) Ensuring representation of the Republic of Poland in the Cooperation Group—i.e. serving a representative function.
(4) Assuring cybersecurity cooperation with the European Commission—i.e. implementing a policy of cooperation with the EU in the sphere of cybersecurity.
(5) Coordinating cooperation between the competent authorities for cybersecurity and public authorities in the Republic of Poland and the appropriate authorities in the Member States of the European Union—i.e. coordinating state cooperation with other EU countries with regard to cybersecurity;
(6) Securing the exchange of information for the Cooperation Group and the CSIRT Network—i.e., implementing the informational aspects of cooperation.

Under recital 35 of the Preamble of the NIS Directive, the Cooperation Group should function as a tool for the exchange of best practices, for discussions on Member States' capabilities and preparedness, and, on a voluntary basis, for assisting its members in evaluating national network and information system security strategies, and capacity building. Furthermore, for the purposes of promoting advanced network and information system security, the Cooperation Group should, where appropriate, cooperate with the relevant EU institutions, authorities, offices, and agencies to exchange knowledge and best practices, and also to advise on the aspects of network and information system security which could affect their work, while respecting the existing arrangements for the exchange of proprietary information. When cooperating with law-enforcement authorities on issues concerning the security of network and information systems which could affect its work, the

Cooperation Group should take into consideration existing information channels and established networks.

In order to carry out the tasks of the Cooperation Group, the single points of contact must provide it with specific information. Information policy is fundamental to the activities related to ensuring cybersecurity.

Another essential element at this stage of civilisational advancement is the right of citizens to obtain, collect, modify, and make available critical information of a public nature. It should be noted that access to information is becoming much easier. Also relevant is the legislation which defines the scopes of available information and separates information of an undisclosed nature.[15] Nowadays, in administrative-law research, information is understood as a new and distinctive element in the tasks of the state, and a form of procedure in times of conflict.[16] Information as a value can also be protected in the context of content relevant for national security.

The Commission's rules on security regarding the protection of EU classified information, established in Commission Decisions (EU, Euratom) 2015/443 (3) and (EU, Euratom) 2015/444 (4), shall apply to any such information received or processed by or from the Cooperation Group. Information processed by the Group which is covered by the obligation of professional secrecy must be duly protected. Members of the Group, as well as representatives of third parties and experts, are bound by the confidentiality obligation referred to in this article. The Chairperson shall ensure that third-party representatives and experts are informed of their confidentiality requirements. However, the Polish legislators have decided that any data which could become information related to national security or public order may not be provided to the Cooperation Group.

The legislators did not make a direct reference to the Act on the Protection of Classified Information (PCI).[17] Its Article 5 describes the types of protected information. In their classification, the legislators referred to the effects which the disclosure of secret information could have on the Polish State. It has been indicated, among other things, that classified information will constitute a message whose disclosure could cause serious damage to the Republic of Poland by making it difficult to conduct operational or exploratory activities being undertaken to ensure state security, or for the prosecution of offenders by institutions or services authorised to do so; or will cause damage to the Republic of Poland by making it more difficult for the services or institutions responsible for the protection of the security or the fundamental interests of the Republic of Poland to perform their tasks; or will hinder the performance of tasks by the services or institutions, or the judicial authorities, responsible for the protection of public order, for the security of citizens, or for the prosecution of the perpetrators of crimes and fiscal offences,

[15]Gardocka (2008), p. 11.

[16]Szpor (1998), p. 24.

[17]Act of 5 August 2010 on the Protection of Classified Information, consolidated text, Polish Journal of Laws of 2019, item 742, as amended).

The aforementioned classification of confidential information has therefore been clarified by the legislators in a fairly broad manner, covering most cases which can cause damage or serious harm to the state.

Currently, classified information is governed by the following legal Acts:

(1) The Act of 5 August 2010 on the Protection of Classified Information and the secondary legislation adopted on its basis.
(2) Ratified bilateral international agreements on the mutual protection of classified information concluded with Albania, Bulgaria, Croatia, the Czech Republic, Estonia, Finland, France, Germany, Italy, Latvia, Norway, Russia, Romania, Slovakia, Spain, Sweden, Ukraine, the United Kingdom, and the United States;
(3) Agreement between the Parties to the North Atlantic Treaty for the Security of Information, done at Brussels on 6 March 1997,[18] and the Agreement Between the Parties to the North Atlantic Treaty for Cooperation Regarding Atomic Information, done at Paris on 18 June 1964.[19]

The Act on the Protection of Classified Information paved the way for the directional construction of a modern system of protection of classified information, which significantly contributed to the creation of a legal framework within which Poland's accession to the North Atlantic Alliance became possible. Over the years the Act has been in force, enormous technological progress has been accomplished, especially in the means of communication and communication and information systems, which undoubtedly has had an impact on information security, and thus on the relevance of the solutions provided in the Act and secondary legislation, especially on those issues which manifest levels far below the current technological state of the art, and are not adapted to the conditions and capabilities of modern technology. This also applies to procedures related to ensuring cybersecurity.

Regarding the information covered by the said Regulation, it can be assumed that the catalogue of information which will not be released extends beyond classified information. Meanwhile, the content of the provision does not indicate who verifies the information, and which authority makes the decision at the stage of this revision, and thus is responsible for not passing it to the Cooperation Group.

Since Member States vary widely in their level of preparedness, leading to an uneven level of consumer and business protection, and adversely affecting the overall level of security of network and information systems within the EU, it has become necessary to develop common informational procedures. Effective response to the challenges of ensuring the security of network and information systems calls for a holistic approach at the EU level, including requirements for building and planning common minimum capacities, and the exchange of information at the primary, i.e. national level. Information, which in this case is a preventive factor,

[18] Agreement between the Parties to the North Atlantic Treaty for the Security of Information, done at Brussels on 6 March 1997 Polish Journal of Laws of 2000, No. 64, item 740.

[19] Agreement Between the Parties to the North Atlantic Treaty for Cooperation Regarding Atomic Information, done at Paris on 18 June 1964 Polish Journal of Laws of 2001 No. 143, item 1594.

is a means to apply this practice. Reporting to the European Commission is essential for building a uniform, common, cybersecurity system in the EU. The Commission shall itself periodically review the functioning of this Directive and report thereon to the European Parliament and the Council. For this purpose, and with a view to further developing strategic and operational cooperation, the Commission shall take into consideration reports by the Cooperation Group and the CSIRT network on the experience gained at the strategic and operational levels. The designation by a Member State of the competent authorities, the single point of contact (their tasks and any amendments thereto, as well as information on the provisions on fines, which, in accordance with Article 21 of the Directive, should be effective, proportionate, and dissuasive) is part of a common policy to build a single cybersecurity system.

Recital 71 of the Preamble to the NIS Directive stipulates that the Commission should periodically review the Directive, in consultation with stakeholders, in particular to verify whether amendments are necessary in the light of changing social, political, technological, or market conditions. In its review, the Commission shall also assess the listings in Annexes II and III, and the consistency in the identification of the operators of essential services and the services in the sectors referred to in Annex II. The obligation to provide information contained in this provision not only arises from the need to create a coherent cybersecurity system, but is related to the provision of information by the European Commission to the European Parliament and the Council in the form of reports which assess, among other things, the consistency of the approach being taken by the Member State concerned to identify the operators of essential services. Pursuant to recital 19 of the Preamble to the Directive, in order to ensure that possible market developments are being adequately reflected, Member States should maintain under regular review a list of identified operators, and update it where necessary. Moreover, Member States should provide the Commission with the information necessary to assess to what extent this common methodology has allowed the consistent application of the definitions by Member States. The purpose of providing information concerning the tasks of CSIRT MON, CSIRT NASK, and CSIRT GOV, encompassing the main elements of incident-handling procedures, is to build a common and uniform cybersecurity system, including at the level of emergency-handling procedures, as well as the tasks of entities.

The Minister competent for digital affairs is an entity synchronising the activities of the institutions at the strategic level (at the operational level the importance of the NC Cyber and the National CSIRT should be emphasised). It is the essential element in the organisation of the cybersecurity system in Poland. It should be emphasised that the decision to appoint a special Ministry within the administration to perform cybersecurity tasks is not a permanent solution. The sphere of cybersecurity is interdisciplinary, and requires the consolidation and coordination of different elements of the state's functioning, and, within it, individual units.

References

Gardocka T (ed) (2008) Obywatelskie prawo do informacji, Warszawa
Gołaczyński J (2009) Ustawa o świadczeniu usług drogą elektroniczną, Warszawa
Szpor G (1998) Informacja w zagospodarowaniu przestrzennym, Katowice

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."