The Obligations of Public Entities

Krzysztof Wąsowski

Abstract The author presents the structure and principles which the Polish legislature imposes on public entities in the field of cybersecurity. The analysed regulations cover government authorities, state control authorities, law enforcement authorities, courts (both common and special), local government units and their associations (including metropolitan unions), budgetary units and Budget establishments, executive agencies, budgetary institutions, the Social Insurance Institution (ZUS) and managed funds, the Agricultural Social Insurance Fund (KRUS) and the funds managed by its President, the National Health Found, public universities, and the Polish Academy of Sciences. In addition to these public finance entities, special cybersecurity obligations have been imposed on research institutes, the National Bank of Poland, Bank Gospodarstwa Krajowego (BGK), Office of Technical Inspection (UDT), the Polish Air Navigation Services Agency (PENSA), Polish Centre for Accreditation (PCA), the National Fund for Environmental Protection and Water Management (NFEP&WM) and the provincial funds, as well as municipal companies. Despite differences in the form of activity (including possession or absence of legal personality), it is commonly agreed that the analysed regulations treat public entities as public administration authorities, at least in the functional sense, as evidenced by the indication that the obligations of public entities should be carried out within the framework of public tasks.

K. Wąsowski (✉)
Akademickie Centrum Polityki Cyberbezpieczeństwa/Academic Center for Cybersecurity Policy, Akademia Sztuki Wojennej w Warszawie/War Studies University in Warsaw, Warsaw, Poland
e-mail: k.wasowski@akademia.mil.pl

K. Chałubińska-Jentkiewicz et al. (eds.), *Cybersecurity in Poland*,
https://doi.org/10.1007/978-3-030-78551-2_20

1 Range of Public Entities Subject to Cyber Security Obligations

The National Cybersecurity System attempts to cover comprehensively and complementarily all entities which use IT tools in the spheres of both public and private activities (under private law) and are significant for state security. In addition to a number of obligations exacted on entities which are not systemically linked to the public sector (such as digital service providers and operators of essential services), the legislators also impose independent, or autonomous, obligations on public entities. It should be noted that the understanding of the term "public entity" significantly exceeds the confines of the term "public administration authority" as used by legal commentators. The legislators have outlined the range of these public institutions very broadly. The provisions contained in Chapter 5 of the National Cybersecurity System Act designate not only government administration authorities, state control authorities, and legal protection authorities, but also the courts (both common and special), local government units and their associations (including metropolitan associations), budget units and local government budget enterprises, executive agencies, budget economy institutions, the Social Insurance Institution and the funds managed by it, the Agricultural Social Insurance Fund (Kasa Rolniczego Ubezpieczenia Społecznego) and the funds managed by its President, the National Health Fund, public universities, and the Polish Academy of Sciences, as well as the organisational units created by it. Apart from these public finance sector entities, special cybersecurity obligations have been imposed on research institutes, the National Bank of Poland, Bank Gospodarstwa Krajowego, the Office of Technical Inspection, the Polish Air Navigation Services Agency, the Polish Centre for Accreditation, the National Fund for Environmental Protection and Water Management, and Voivodeship Water Management Funds. Finally, the legislators included so-called municipal companies among public entities.[1]

Despite differences in the form of activity (resulting, i.a., in having or not having legal personality), there is no doubt that the analysed regulations treat public entities as public administration authorities, at least in the functional sense,[2] by indicating that the duties of public entities should be performed while performing "public tasks".[3] The functions of public tasks may be performed by any entity to which the legislators assign relevant responsibilities in a normative Act. This is because this entity does not necessarily have to be systemically linked to the structure of public administration authorities, nor does it have to be a state legal person,[4] and it may

[1] Chałubińska-Jentkiewicz et al. (2021) passim.

[2] See more Dawidowicz (1965), pp. 5–7.

[3] Por. Biernat (1994), pp. 4–11.

[4] See more—Dybowski (1990); Szachułowicz (2000), p. 18.

operate, for example, within the structures provided for in the Code of Commercial Companies and Partnerships[5] for private commercial entities.

Government administration authorities in the political system are subject, respectively by hierarchy, to the Council of Ministers, which conducts the internal and external policies of the Republic of Poland,[6] and governs all matters of state policy not reserved for other state and local government authorities.[7] The Council of Ministers has also been given a clear mandate to lead the government administration.[8]

In addition, the Constitution of the Republic of Poland includes the following state authorities as state control and legal protection authorities: the Supreme Audit Office,[9] the Ombudsman,[10] and the National Broadcasting Council.[11] These are autonomous state authorities, with their independence from both the executive and the legislative authorities already guaranteed at system level. The cybersecurity system has also been extended to the courts and tribunals,[12] whose autonomy from other state authorities derives from the principles of tri-partition and the balance of power.[13]

Local government is an emanation of the de-centralised state system,[14] and performs all public tasks not reserved for others by the legislators.[15] Local government units also have the constitutional right to associate[16] and establish municipal associations.

Budgetary units are organisational entities in the public finance sector, with no legal personality, and whose expenditures are financed directly from the budget, while they transfer the collected revenues to the account of the state budget revenue, or the budget of a local government unit, respectively.[17] A local government budget entity, in turn, is a separate, autonomous, unit within the structure of a specific territorial government unit, and within its activities in the field of broadly understood municipal management, performing tasks of a public-utility type.[18] The cyber

[5]The Commercial Companies Code of 15 September 2000, consolidated text of 2019, item 505, as amended.

[6]See Article 146 (1) of the Constitution of the Republic of Poland.

[7]See Article 146 (2) of the Constitution of the Republic of Poland.

[8]See Article 146 (3) of the Constitution of the Republic of Poland.

[9]See Articles 202–207 of the Constitution of the Republic of Poland.

[10]See Articles 208–212 of the Constitution of the Republic of Poland.

[11]See Articles 214–215 of the Constitution of the Republic of Poland.

[12]See Articles 173–201 See Article 10 of the Constitution of the Republic of Poland.

[13]See Article 10 of the Constitution of the Republic of Poland.

[14]See Article 15 (1) of the Constitution of the Republic of Poland.

[15]See Article 10 of the Constitution of the Republic of Poland.

[16]See Article 172 (1) of the Constitution of the Republic of Poland.

[17]According to the requirements of Article 11 (1) of the Act on Public Finances of 27 August 2009, consolidated text Polish Journal of Laws of 2019, item 869, as amended.

[18]See more—Banasiński and Jaroszyński (2017), p. 28.

security system also includes executive agencies, which are referred to as new public management institutions,[19] the aim of which is to implement the transition from the bureaucratic model of public management to the so-called managerial model.[20] Cybersecurity obligations are also imposed on budgetary-economy institutions, i.e. the public finance sector units created in order to perform public tasks, with their typical features including the implementation of the public tasks entrusted to them for remuneration, and covering their operational costs and liabilities from the revenues obtained.[21]

The Social Insurance Institution (Zakład Ubezpieczeń Społecznych—ZUS) is a state organisational unit with legal personality. The scope, tasks, and responsibilities of ZUS are defined by law.[22] ZUS is managed by its President, who performs his or her functions with the help of the management board—a collegial authority. The control function is performed by the Supervisory Board, appointed by the Prime Minister, with the reservation that individual members of the Board should be appointed by the appropriate public administration authorities and organisations of employers, employees and pensioners.[23] The legislators have differentiated the Head Office from the field organisational units within the structure of ZUS. The main task of this public undertaking is to implement the social security regulations.[24] As part of its public tasks, ZUS is also obligated to maintain a contact point for the exchange of data within the System for Electronic Exchange of Social Security Information.[25]

The Agricultural Social Insurance Fund (Kasa Rolniczego Ubezpieczenia Społecznego—KRUS) is a state organisational unit, with a status not clearly defined by law. The legislators have given KRUS the basic task of administering social insurance for farmers.[26] The fund is managed by its President, who has the status of a central government administration authority, and reports to the Minister competent for rural development.[27]

[19]See Zieliński (2014).

[20]See Marchewka-Bartkowiak (2011).

[21]See Article 23 (1) of the Act on Public Finances of 27 August 2009.

[22]See Chapter 7 of the Social Insurance System Act of 13 October 1998, consolidated text, Polish Journal of Laws of 2019, item 300, as amended.

[23]See Article 75 of the Social Insurance System Act.

[24]See Article 68 (1) (1) of the Social Insurance System Act.

[25]See Article 68a(1) of the Social Security System Act, in conjunction with Regulation (EC) No 987/2009 of the European Parliament and of the Council of 16 September 2009 laying down the procedure for implementing Regulation (EC) No. 883/2004 on the coordination of social security systems (OJ EU 2009 L 284/1, as amended).

[26]See Article 2 (1) of the Agricultural Social Insurance Fund of 20 December 1990, consolidated text, Polish Journal of Laws of 2019, item 299, as amended.

[27]See Article 2 (2) of the Agricultural Social Insurance Fund.

The National Health Fund (Narodowy Fundusz Zdrowia—NFZ) is a state organisational unit with legal personality.[28] A National Contact Point for cross-border healthcare has also been established at the Headquarters of the Fund.[29]

Public universities which were established by a state authority are also covered by the regulations in respect of the cybersecurity system.[30] Research institutes have also been included in this system. They are defined in the Act as state development units, independent in legal, organisational, economic, and financial terms, which conduct research and development work aimed at the implementation and practical application of its results.[31] The Polish Academy of Sciences (Polska Akademia Nauk—PAN), in turn, is a "state scientific institution",[32] with legal personality.[33]

The National Bank of Poland (NBP) is the central bank of the country, which has the exclusive right to issue money, and to establish and implement monetary policy.[34] This entity has legal personality.[35] In contrast, Bank Gospodarstwa Krajowego is the state bank,[36] which means that it is not a state enterprise, nor is it a state organisational unit or a public finance sector entity, nor is it subject to registration in the National Court Register. The basic objective of BGK is to support the economic policy of the Council of Ministers, governmental social and economic programmes, including guarantee and suretyship programmes, and local government and regional development programmes.[37]

The Office of Technical Inspection (Urząd Dozoru Technicznego—UDT) is a state entity with legal personality, which is not responsible for the liabilities of the Treasury, and the Treasury is not responsible for the obligations of UDT. The Polish Air Navigation Services Agency is a state entity with legal personality,[38] and its statutory tasks include ensuring safe, continuous, smooth-running, and effective air

[28]See Article 96(1) of the Act on Health Care Services Financed from Public Funds of 27 August 2004, consolidated text, Polish Journal of Laws of 2019, item 1373, as amended.

[29]See Article 97a of the Act on Public Health Care Services.

[30]See Article 14 of the Higher Education and Science Law of 20 July 2018, Polish Journal of Laws of 2018, item 1668, as amended.

[31]See Article 1 (1) of the Act on Research Institutes of 30 April 2010, consolidated text, Polish Journal of Laws of 2019, item 1350, as amended.

[32]See Article 1(1) of the Act on the Polish Academy of Sciences of 30 April 2010, consolidated text, Polish Journal of Laws of 2019, item 1183, as amended.

[33]See Article 3 (1) of the Act on the Polish Academy of Sciences.

[34]See Article 227 (1) of the Constitution of the Republic of Poland.

[35]See Article 2 (2) of the Act on the National Bank of Poland of 29 August 1997, consolidated text, Polish Journal of Laws of 2019, item 1810, as amended.

[36]Within the meaning of Article 14 et seq. of Banking Law of 29 August 1997, consolidated text, Polish Journal of Laws of 2018, item 2187, as amended.

[37]See Article 4 of the Bank Gospodarstwa Krajowego Act of 14 March 2003, consolidated text, Polish Journal of Laws of 2018, item 1543, as amended.

[38]See Article 1 (2) of the Act on the Polish Air Navigation Services Agency of 8 December 2006, consolidated text, Polish Journal of Laws of 2017, item 1967, as amended.

navigation in Polish airspace.[39] The Polish Accreditation Centre is a national accreditation authority which is a state legal entity.[40] The National Fund for Environmental Protection and Water Management, and the provincial funds for environmental protection and water management, are environmental protection institutions.[41] The National Fund is a state institution with legal personality,[42] while voivodeship funds have the status of local government units with legal personalities,[43] but they are not local government organisational units.[44]

This general review of the legal status of individual entities charged with taking certain actions within the framework of the functioning of the cybersecurity system shows that their systemic nature is quite diverse. The principle of the functional approach to public entities is clearly apparent, and is closely related to the public tasks implemented by these entities.

2 Obligation to Report and Handle an Incident in a Public Entity

An obligation placed on a public entity becomes enforceable only when the task imposed on that entity is carried out using an information system. The concept of an information system has been legally defined by reference to the concept of an information and communication system,[45] supplemented by the fact that it also involves processing data in an electronic form in that system. If a certain public entity does not perform public tasks at all, it will not be subject to this obligation. Such a situation is difficult to imagine in the current legal regime, and would require the intervention of the legislators, who would prohibit a public entity indicated in this provision from the fulfilment of public tasks in general, or would order such an entity not to fulfil its tasks using the information system, which nowadays seems unlikely.[46] Ensuring "incident management" includes, at the same time, an obligation to ensure access to know-how, and a procedure to inform certain entities of the

[39]See Article 3 (1) of the Act on the Polish Air Navigation Services Agency.

[40]See Article 38 (2) of the Act on Conformity Assessment and Market Supervision of 13 April 2016, Polish Journal of Laws of 2019, item 544, as amended.

[41]See Article 386 (3) of the Environmental Protection Law of 27 April 2001, consolidated text of 2019, item 1396, as amended.

[42]See Article 400 (1) of the Environmental Protection Law.

[43]See Article 400 (2) of the Environmental Protection Law.

[44]See Article 400 (3) of the Environmental Protection Law.

[45]Within the meaning of Article 3 point 3 of the Act on the Computerisation of the Activities of Entities Performing Public Tasks of 17 February 2005, consolidated text, Polish Journal of Laws of 2019, item 700, as amended.

[46]Por. Wąsowski (2019), pp. 188–189.

designation of the responsible person. It is worth pointing out that the catalogue of these duties is of closed nature (*numerus clausus*).

Incident management as a term is understood by the legislators not only as "dealing with" such incidents, but also detecting links between them, removing their causes, and developing the appropriate proposals addressed at, inter alia, detecting them more effectively, and taking action to prevent such events in the future. An obligation characterised in this way provides a legal basis for any action, both managerial and organisational-technical, which it should carry out, not only within its "own" capacities, but also with "external" assistance—of a public entity in this respect.

Notwithstanding the obligation to undertake incident management, a public entity must immediately report a detected "in-house" incident to the competent Computer Security Incident Response Team (CSIRT). The determination of competence is reduced to the scope of subject-matter competence based on a catalogue of incident types (also in terms of the sector in which the incident has been detected). In this case, the legislators did not specify any exact rules for the observance of competence ex-officio by the applicable CSIRT. The rules for the assessment and observance of competence as laid down in the Code of Administrative Procedure do not apply. A notification to the competent CSIRT should be made without undue (culpable) delay, no later than 24 hours after the detection of such an incident. It is worth noting that the legislators have not specified in detail the technology of such an electronic form. It will be reasonable to assume that the notification should be made by e-mail, while the public authority is obliged to provide the e-mail address of the competent CSIRT.[47] Where it is not possible to communicate the information by electronic means, any other way of passing on the notification is acceptable. However, it is worth assuming that in each of the possible ways chosen by the informant there should be a guarantee that the information (notification) reaches the addressee. Only then will it be possible to consider the act of notification as having been carried out.

The handling of an incident and a critical occurrence in a public entity has been entrusted to a public entity cooperating with the competent CSIRT. The entity obliged to provide a service has been indicated as a public entity, and the cooperating entity as the competent CSIRT, which should support the public entity in carrying out such an obligation. The legislators have also included an obligation imposed on a public entity, carried out during incident handling, to provide essential data, including personal details. All data (other than personal) which might be (even indirectly) related to the detection and response to incidents should be treated as essential.

Public entities are also responsible for the implementation of the material and technical task of providing the beneficiaries of public tasks with access to know-how and useful information on cybersecurity. This obligation is manifestly described in more detail when the necessary information on cybersecurity is published. Similarly

[47]See Article 22 (5) of the National Cybersecurity System Act of 5 July 2018, Polish Journal of Laws of 2018, item 1560, as amended.

to other cybersecurity tasks imposed on public entities, the legislators have not provided for direct legal sanctions.[48]

3 Formal Requirements for Reporting an Incident in a Public Entity

The reporting of incidents is conditional on numerous formal and informational requirements. The informational obligations involve the transfer of data of a subjective nature (data on the public entity, the reporting person, and the person authorised to provide explanations) and of an objective nature (containing information on what caused the incident, its essential features, the effects it had or might have had, and about the preventive actions taken or planned).

The obligation to include data on the public entity in the notification is defined at the basic level (name, number in the relevant register, registered office, and address). It is worth pointing out that in situations in which a public entity is not subject to the obligation of registration (e.g. public administration authorities), it will not be able to indicate the register number.

The person submitting the notification should, in principle, be the responsible person designated by the public entity. However, the legislators do not grant such a person specific exclusivity to undertake such duties. When reporting an incident, the time and speed with which the competent CSIRT is informed of such an event is of crucial importance. Therefore, the obligation to make a report in emergency situations may be fulfilled by persons other than the one responsible. Also, the informant should indicate his or her name, telephone number, and e-mail address.

A person entitled to submit explanations is another party whose data should be disclosed in the notification. The scope of the disclosure of the information about such a person is the same as that of the person submitting the notification. The mere mention of such a person in the notification means that he or she has given a specific authorisation to clarify the submitted information. No additional document is required to confirm such an authorisation. Nor is there any formal limitation on the person who reports to be shown as entitled to submit explanations at the same time.

Details of the public task should be included in the description of the incident, which should be linked to an indication of the legal basis for carrying out such a task. The estimate of the number of people affected by the incident need not be clearly defined. In a situation in which it would be impossible to determine a precise figure, an estimate of the number of people who were affected by such an incident should be given. Correct timing is important and should be presented in the most precise way possible. In a virtual reality, the requirement to define the geographical area affected might concern the entire region, although, where possible, a precisely defined area

[48] Wąsowski (2019), pp. 190–192.

should be identified. The most important element in the description, by general consent, is the identification of the causes of the incident, its course, and the effects of its impact on the information systems of the public entity. This description should indicate all the relevant facts which had a direct and indirect impact on the occurrence, course, and consequences of the incident. The cause and source of the incident are important, so the standard-setter acknowledges such an obligation, both as part of the description of the impact of the incident on the public task being carried out and as a stand-alone criterion in the incident report.

It is also important to describe any preventive measures which were taken after the incident had occurred, in order to prevent the recurrence of such an event. The description of such activities should be disclosed in the most transparent way possible. The notification shall also include a listing and description of all corrective actions taken after the incident occurred. Notwithstanding the required factual information, the notification shall include any information which might contribute to the identification of the incident, its assessment, and the taking of corrective and preventive action. The legislators have also introduced an obligation to supplement the information in the notification as an ongoing and permanent duty. The addendum shall be communicated without delay, at the same time, and in the same way, as the original notification.

Any restrictions on the transmission of information contained in the notification would involve information classified as legally protected secrets. In particular, a company secret has the status of such a clause. It is worth mentioning at this point that in addition to company secrets, current legislation regulates almost 70 types of legally protected secrets.[49] Such limitations may only be ignored if the disclosure is necessary to carry out the tasks of the competent CRSIT MON, CSIRT NASK, or CSIRT GOV, and, in addition, if the scope of the information disclosed is incomplete or limited to what is essential. Such legally protected information may also be disclosed at the request of the competent CSIRT, and its disclosure shall be subject to the same restrictions as if it had been transmitted by a public entity on its own initiative. In the notification, the protected legal information disclosed shall be classified, and shall be separated and secured in such a way that it cannot be disclosed to unauthorised persons.

4 Obligation to Designate a Person Responsible for Contacts with National Cyber Security System Operators

The general norm requires the public entities listed in the Act to appoint a person responsible for maintaining contact with the entities in the national cyber security system. The concept of "responsible person" has not been clarified by the legislators.

[49]For more information on this subject, see Polok (2006), pp. 23–25.

It can be speculated on—particularly in the light of what is known as a logical-linguistic interpretation—that this could be both a natural person and a legal person. However, it is more difficult to indicate at this level of interpretation that the term "responsible person" may also be used to describe an organisational unit without legal personality. In the light of a systemic interpretation, it appears that the legislators aimed at referring to a specific natural person, since it distinguishes the concept of a "person" from that of an "entity" (or "entities"), which has a much broader scope of meaning.[50]

An obligation imposed on the indicated public entity should be implemented by way of "appointing" a responsible person. Legal commentators in administrative law tend to avoid defining "appointing" as a legal form of administration. It is more often determined as a result of the application of some legal form of administrative authority (e.g. an administrative act or an internal management act). It can therefore be assumed that the concept of "appointing" a specific responsible person is intended to signify an effect achieved by a public entity through the use of an indeterminate form of administrative action. On the other hand, the legal form of such appointment, although not explicitly indicated in the Act, should first relate to internal forms of administrative activity, due to the context of the provision suggesting the designation of a person who is organisationally related to a public entity, and, second, take the form of a specific declaration of will by the entity. The question remains of how to express this will. At first glance, it seems that the appointment should be made unilaterally, either in an individualised form, resembling a type of official order, or in a normative form, assigning the duties of the appointed person to a function, which may be carried out in the form of regulations, guidelines, or internal orders. It seems, however, that this "appointment" may also be done in a bilateral, even contractual, format—especially if the allocated person is not an employee of a public entity. The term "person" itself, and not, e.g., "employee", shows that the legislators do not limit the circle of appointed persons to those who are organisationally related to the public entity.

The "appointed person" of the entity will, in turn, be required to "maintain contact with the entities in the national cybersecurity system." The legislators are not setting out here the framework for such an obligation. The appointed person will have to be disclosed to the competent CSIRT MON, CSIRT NASK, or CSIRT GOV in the manner specified therein, without regulating the procedure for the other entities forming the national cybersecurity system, as a kind of "contact point" for those entities.[51] With this wording it is difficult to prove any "exclusivity" for such an appointed person to maintain these contacts. In the practice of a public entity, other persons (formally "non-appointed") performing specific tasks within the entity may also maintain contact with entities in the national cybersecurity system. Regardless of the formula for "appointing" a contact person, it is worthwhile setting out in such an "appointment act", or in a kind of "appointment agreement", the rules (even

[50]Zob. Wąsowski (2019), pp. 185–192.

[51]See Article 22(1)(5) of the NCSA.

procedures) for implementing the obligation of the designated person to maintain contact with the entities in the national cybersecurity system.

Nor do the legislators specify what the responsibilities of the designated person will be. The issue of a possible transfer of responsibility from a public authority to the designated person has also not been resolved. In this respect, the lack of a clear directive by the legislators should be taken as an indication that the designation of the person responsible by a public entity does not in any way supersede the responsibility of the public entity in question for efficiently maintaining contact with all the "elements" in the national cybersecurity system. It is puzzling that there are no sanctions (in particular of a criminal-administrative nature) for failure to comply with a public entity's obligation by not appointing an appropriate contact person with the entities in the national cybersecurity system, while for operators of essential services for failure to comply with a similar duty[52] there *are* imposed specific sanctions of an administrative nature.[53]

The use of wording referring to appointing the "competent person" (using the singular instead of the plural) suggests that a public entity has the right to appoint only one person, instead of, for example, a team of responsible persons. Such a literal interpretation does not seem to be conclusive, however, as the legislators clearly limit the "circle" of designated responsible persons to "one". Thus, it should be recognised that more than one individual can be a "responsible person". Even if a strictly literal interpretation is considered binding, it should be pointed out that the provisions of this regulation do not restrict public entities to indicating a specific sequence in the assuming of the obligation to maintain contacts by the deputies (in the event of an even temporary inability to perform their duties) of the designated responsible person.

As public entities, public administration authorities are treated specially in terms of appointing the responsible person. First, they may only appoint "one" responsible person. Second, that person will be required to cooperate ("maintain contact") with the entities in the national cyber-security system to a specific extent, namely with regard to "*public tasks dependent on information systems"*. In today's complexity of individual public tasks (understood as tasks imposed by the standards of the universally applicable law, aimed at the realisation of the common good), it is difficult to imagine a total separation between the operation of a public administration authority and the use of even the least-complicated information systems. It is clear, therefore, that it should be recognised that, within the practice of public administration authorities, all public tasks performed by these authorities will be related to the use of information systems and, in this sense, will depend on their use.

It appears that the specificity of a "single responsible person" does not involve the performance of public tasks dependent on information systems, but the appointment of a common responsible person for a given public administration authority and the units subordinate to or supervised by it. At the same time it could be assumed that the

[52]See Article 73 (1) of the NCSA.

[53]See Article 9 (1) of the NCSA.

wording presented by the legislators was not so much about one (in the literal sense—the only) person for the public administration authority and its related entities, but about the possibility of appointing even several persons (similarly to other public entities), with these persons, within the scope of their responsibilities, also having entities related by ties of subordination or supervision to the given public administration authority. The relations of supremacy—subordination and supervision—have been described quite extensively in the literature on the subject.[54] The essence of superiority lies in the competence of a public administration authority vis-à-vis a subordinate entity which authorises the superior to have a binding influence on the activities undertaken by the subordinate entity, and on the personnel of such an entity. Speaking in simple terms, supervision means the authority (resulting from the provisions of generally applicable law) which allows the supervisor to control the supervised entity, and, in the modes specified by law, to influence the decisions of the supervised entity.

A similar system of appointing "one" person, as in the case of public administration authorities, has been applied to local government units. Local government units currently include communes, districts, and self-government voivodships. These units have been given legal personality by the legislators, which is certainly different from the situation with public administration authorities, which in principle do not have such a personality. The problem is that acting on behalf of local government units are their bodies (both constituting and executive), which also perform the function of public administration authorities (this group, sometimes also referred to as "state" authorities, is divided into government administration authorities, and, i.a., local government administration authorities, including local government authorities). In this context, the introduction of the differentiation of responsibilities in the analysed provision between public administration authorities (paragraph 2) and local government units (paragraph 3) loses its significance.

Within the framework of the cooperation of public entities with the competent CSIRT, the legislators have also introduced a specific informational procedure for transferring the data of the responsible person appointed on the basis of the National Cybersecurity System Act. Formal requirements shall include the name of the responsible person, his or her telephone number, and e-mail address. Failure to indicate one of the three formal elements results in failure to comply with this requirement. The legislators do not, however, attribute clear consequences in the form of statutory sanctions for such deficiencies. The obligation to provide the basic data of the responsible person shall be fulfilled within 14 days of the appointment of that person. The same applies to the time limit for the passing on of information on changes to such data. With today's technological progress and the need to quickly (in principle immediately) respond to incidents, such an extensive time frame seems to be too wide.

[54]See more—Cieślak (2014), pp. 75–85.

5 Obligation to Provide Information to the Competent CSIRT

This provision sets the legal basis for allowing public entities carrying out public tasks, which depend on information systems, to communicate to the competent CSIRT information about other incidents, cyber-security threats relating to risk assessment, vulnerabilities, and the technologies used. This possibility has also been attributed to the operators of essential services. This task is complementary to the informational obligations imposed on public entities in the field of cybersecurity; it aims at the broadest possible prevention involving early detection and analysis of any phenomena which might affect the functioning of the cybersecurity system.

The information procedure has not been formalised in principle. It is sufficient for such information to be provided in an electronic form (in the simplest way, by e-mail). In the event that the electronic transmission of such information is impossible or excessively difficult, the communication of information (as is the case with the notification) should take place by any available means. Written (paper) correspondence may therefore be delivered by conventional means. The legislators have also not stipulated any time limits—unlike in the case of the notification—on the information to be provided under a kind of early warning system. However, the essence of the National Cybersecurity System is that this information should also be provided immediately. The Act provides for the possibility of obtaining the status of an operator of essential services by a public entity under general principles after obtaining an appropriate administrative decision. There are no special restrictions or privileges for public entities in the procedure for becoming operators of essential services.

The legislators have limited the performance of related obligations by a public entity with the status of an operator of essential services to specific essential services which relate to the exercising of the function of an operator of that service. In activities not directly related to the essential service, the public entity is not obliged to fulfil any obligations imposed by law on the operator of essential services.[55]

6 Summary

Within the framework of the regulation contained in the National Cybersecurity System Act, the inclusion of such a large number of public entities under the regime of this regulation results from the desire to build a comprehensive and systemic approach to the national cybersecurity system,[56] rather than the implementation of

[55] See Wąsowski (2019), pp. 192–193.

[56] See Czaplicki (2019).

the NIS Directive itself.[57] The directive applies to operators of essential services and digital service providers, and the National Cybersecurity System Act goes beyond the implementation of the NIS Directive, and also defines other elements which influence national cybersecurity policy. Some public entities may be recognised as operators of essential services, and will then have obligations similar to other such entities. The NIS Directive allows each Member State to take the necessary measures to ensure the protection of the essential interests of its security, public order, and public safety. Such a directive certainly includes a broad (and not closed) definition of the circle of public entities, and assigning them legal obligations of an informational nature. It is also an attempt at a procedural and organisational response to the dangers of cyberspace.

References

Banasiński C, Jaroszyński K (2017) Ustawa o gospodarce komunalnej. Komentarz, Warsaw
Biernat S (1994) Prywatyzacja zadań publicznych, Warsaw – Cracow
Chałubińska-Jentkiewicz K, Karpiuk M, Kostrubiec J (2021) The legal status of public entities in the field of cybersecurity in Poland. Lex Localis Press, Maribor
Cieślak Z (ed) (2014) Nauka administracji, Warsaw
Czaplicki K (2019) In: Czaplicki K, Gryszczyńska A, Szpor G (eds) Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, Warsaw
Dawidowicz W (1965) Nauka prawa administracyjnego. Zarys wykładu. Tom I, Zagadnienia podstawowe, Warsaw
Dybowski T (1990) Własność Skarbu Państwa i państwowych osób prawnych w świetle art. 128 KC, Państwo i Prawo 4
Marchewka-Bartkowiak K (2011) Agencje wykonawcze, Biuro Analiz Sejmowych (18.08.2011)
Polok M (2006) Ochrona tajemnicy państwowej i tajemnicy służbowej w polskim systemie prawnym, Warsaw
Szachułowicz J (2000) Własność publiczna, Warsaw
Wąsowski K (2019) In: Kitler W, Radoniewicz F, Taczkowska-Olszewska J (eds) Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, Warsaw
Zieliński M (2014) Agencje wykonawcze UE. Europejski Przegląd Sądowy 6

Krzysztof Wąsowski PhD, advocate. Graduated from the Faculty of Law and Administration at the University of Warsaw, Poland and ARGO Top Public Management at the IESE Business School in Barcelona, Spain. Adjunct at the Department of Cybersecurity and New Technologies and an expert at the Academic Center for Cybersecurity Policy at the War Studies University in Warsaw. Partner of the law firm "WLP Legal" in Warsaw, Poland.

[57]Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of networks and information systems within the Union, OJ EU 2016 L 194/1.