Mirosław Karpiuk*

The obligations of public entities within the national cybersecurity system

Abstract

The lawmakers have imposed a number of obligations on public entities within the national cybersecurity system to ensure that information systems are resilient against actions which compromise the confidentiality, integrity, accessibility, and authenticity of the data being processed in these systems, or the related services provided by such systems. These obligations include incident reporting and handling by the appropriate public entities, and designating contact persons to communicate with national cybersecurity system entities. However, they do not apply to all public bodies – only those specifically named by the lawmakers. An important spectrum of measures in this regard involves public-entity incidents, i.e. occurrences which impair, or might impair, the quality of, or disrupt the performance of, a public function by a public entity. When fulfilling their obligations, it is particularly important for public entities to handle incidents, understood as taking measures to identify, register, analyse, classify, prioritise, contain, and remedy the incidents.

Key words: cybersecurity, information system, incident, essential service

* UWM Professor Mirosław Karpiuk, Ph.D., The Department of Administrative Law and Security Sciences, the Faculty of Law and Administration, the University of Warmia and Mazury in Olsztyn, e-mail: miroslaw.karpiuk@uwm.edu.pl, ORCID: 0000-0001-7012-8999.

The obligations of public entities arising from Chapter 5 of the National Cybersecurity System Act of 5 July 2018[1] ("the NCSA") apply to 1) public-finance entities[2], 2) research institutes, 3) the National Bank of Poland, 4) a National Development Bank), 5) the Office of Technical Inspection, 6) the Polish Air Navigation Services Agency, 7) the Polish Centre for Accreditation, 8) the National Fund for Environmental Protection and Water Management and the regional funds for environmental protection and water management, 9) commercial companies and partnerships in charge of public services[3]. The reason why such a broad range of public entities falls under the regime of the NCSA is that there exists a need for a comprehensive, and, at the same time, systemic, approach to the national cybersecurity system, one going beyond the implementation of the EU Directive, which applies to operators of essential services and digital-service providers. Some public entities might be considered operators of essential services, in which case they will have the same obligations as other such entities. The Directive allows each Member State to take the measures necessary to ensure the protection of their core security interests, and to safeguard public order. The establishment of a national cybersecurity system is an attempt at providing a procedural and organisational response to the emerging cyberspace threats[4].

The above-mentioned public entities in charge of public services, which rely on information systems[5] under Article 21 of the NCSA, are required to

1 The National Cybersecurity System Act of 5 July 2018 (Journal of Laws of 2018, item 1560, as amended).

2 These public-finance entities within the national cybersecurity system include 1) public authorities, including Government-administration bodies, State inspection and safeguarding authorities, and courts and tribunals; 2) local-government units and their associations; 3) metropolitan associations; 4) budgetary entities; 5) local-government budgetary establishments; 6) executive agencies; 7) public-sector enterprises; 8) the Social Insurance Institution, including any funds under its management, and the Agricultural Social Insurance Funds, including any funds under the management of its President; 9) the National Health Fund; public tertiary institutions; 11) the Polish Academy of Sciences, including any organisational units it might establish, Article 9 of the Public Finance Act of 27 August 2009 (consolidated text, ibidem of 2019, item 869, as amended)

3 The aim of public service functions is to meet, continuously and without disruptions, collective population needs by providing publicly accessible services, Article 1 (2) of the Municipal Engineering Act of 20 December 1996 (consolidated text, ibidem, item 712, as amended).

4 K. Czaplicki, *Komentarz do art. 21*, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Czaplicki, A. Gryszczyńska, G. Szpor, LEX 2019.

5 An information system is a set of interconnected computer devices and programs designed to process, store, send, and receive data via telecommunications networks using

designate a contact person to communicate with other entities within the national cybersecurity system. Public-administration bodies may designate one contact person to communicate with organisations within the national cybersecurity system on matters involving public functions which rely on information systems, and which are performed by entities subordinate to, or supervised by, such bodies. Local-government units may designate one contact person to communicate with entities within the national cybersecurity system on matters involving public functions which rely on information systems, and which are performed by the organisational divisions of such units.

Article 21 (1) of the NCSA lays down the obligation to designate a contact person to communicate with entities within the national cybersecurity system. This applies to the entities listed in Article 4 (7–15) of the NCSA which are in charge of any public functions which rely on information systems. Notably, the provision does not stipulate the legal form in which to designate such a contact person.

Both public-administration bodies in charge of public functions which rely on information systems, as performed by any units subordinate to, or supervised by, such bodies [Article 21 (2) of the NCSA], and local-government units in charge of public functions which rely on information systems, as performed by their respective organisational units [Article 21 (3) of the NCSA], may designate one contact person to communicate with entities within the national cybersecurity system. Accordingly, the lawmakers have imposed the obligation of designating only one contact person, even if the nature of, and the workload involved in, functions which rely on information systems would require a whole group of such persons.

A public-administration body may designate a contact person using whatever legal form available. No specific legal transaction is required to effect this designation.

Article 21 (3) of the NCSA stipulates that a local-government unit[6] may designate one contact person, but it does not specify which body is required

an end device specific to the given type of telecommunications network – i.e. an information and communications technology system, including any electronic data processed therein – Article 2 (14) of the NCSA.

6 Local government is defined as a legal entity with a decentralised form, separate from the State, and constituted by the residents of a specific territory, and a legally separate entity fulfilling public functions in its own name and at its own responsibility, M. Karpiuk, *Samorząd terytorialny a państwo. Prawne instrumenty nadzoru nad samorządem gminnym*, Lublin 2008, p. 58.

to effect the legal transaction involved. In its existing wording, the provision raises doubts as to whether this responsibility lies with a legislative, or an executive, body in charge of ongoing policy implementation.

Commune Councils have authority in all matters associated with their activities unless the applicable law stipulates otherwise[7]. Article 1 (1) of the Communal Government Act (the CGA) states that Commune Councils have implied authority in all matters associated with their activities, unless the applicable law stipulates otherwise[8]. This provision includes a general clause under which Commune Councils are entrusted with all local public matters associated with their activities, unless the applicable law stipulates otherwise. In accordance with Article 18 (1) of the CGA, Commune Councils are implied to be the responsible entities when it is not clear from the CGA or other Acts which communal authority has the responsibility to resolve a specific matter. Consequently, where a legal regulation grants authority to communal bodies, such authority is due to the Commune Council. This implied authority of Commune Councils does not apply, however, if a legal regulation assigns a specific matter to other authorities, including the executive body of the Commune, or to any auxiliary entities[9]. The Commune Council's authority "in all matters associated with its activities" should be understood through the lens of Article 15 (1) of the CGA, i.e. as activities involving local law-making and supervision. Generally, this does not preclude non-authoritative activities, e.g. ones which are intentional in nature, provided that they remain within the statutory remit of the Commune[10].

District Boards implement the resolutions of District Councils, and District functions, as defined by law[11]. Article 32 (1) DGA implies that in addition to implementing the resolutions of District Councils, the authority of District Boards extends to all District functions as defined by law. This wording suggests that it is implied that District Boards have the authority to

7 Article 18 (1) of the Communal Government Act of 8 March 1990 (consolidated text, Journal of Laws of 2019, item 506, as amended) ("The CGA").

8 Judgment of the Regional Administrative Court of 6 March 2018, II SA/Bd 882/17, LEX no. 2412223.

9 K. Wlaźlak, *Komentarz do art. 18*, [in:] *Ustawa o samorządzie gminnym. Komentarz*, red. P. Chmielnicki, LEX 2013.

10 Judgment of the Regional Administrative Court of 13 February 2018, II SA/Op 600/17, LEX no. 2446979.

11 Article 32 (1) of the District Government Act of 5 June 1998 (consolidated text, Journal of Laws of 2019, item 511, as amended) ("the DGA").

fulfil District functions in matters in which District Councils have restricted authority[12].

Regional Boards may fulfil functions within the remit of Regional Governments, unless they are restricted to Regional Parliaments and Regional Government's organisational units[13]. In Article 41 (1) of the RGA the lawmakers have established the rule of Regional Boards' implied authority[14].

Apart from the obligation to designate a contact person to communicate with entities within the national cybersecurity system, the lawmakers have introduced the obligation to report and handle public-entity incidents (public-entity incidents are events which impair, or might impair, the quality of, or disrupt the performance of, a public function by a public entity, as referred to in Article 4 (7–15) of the NCSA – Article 2 (9) of the NCSA). This obligation is laid down in Article 22 of the NCSA. Under this regulation public entities, as referred to in Article 4 (7–15) of the NCSA, serving public functions which rely on information systems are required to 1) ensure public-entity incident management; 2) report public-entity incidents, immediately but not later than 24 hours after detection, to the appropriate CSIRT MON (the Polish Ministry of Defence's Computer Security Incident Response Team), CSIRT NASK (NASK – the National Research Institute's Computer Security Incident Response Team) or CSIRT GOV (the Internal Security Agency's Computer Security Incident Response Team); 3) handle public-entity incidents and critical incidents in cooperation with the appropriate CSIRT MON, CSIRT NASK, OR CSIRT GOV, including to provide all necessary data, personal data included; 4) provide the persons for whom public functions are performed with access to the knowledge required to understand cybersecurity threats and apply effective protection measures against them, in particular by publishing information on this subject on their websites; 5) provide the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV with the details of the contact person to communicate with entities within the national cybersecurity system, as designated by the

12 Judgment of the Regional Administrative Court of 6 March 2014, III SA/Lu 691/13, LEX no. 1522917.

13 Article 41 (1) of the Regional Government Act of 5 June 1998 (consolidated text, Journal of Laws of 2019, item 512, as amended), ("the RGA") Any Regional Government functions which are not restricted to Regional Parliaments and Regional Government's organisational units may be performed by Regional Boards; Judgment of the Regional Administrative Court of 19 July 2010, II SA/Bk 380/10, LEX no. 688947.

14 A. Szewc, *Komentarz do art. 41*, [in:] A. Szewc, *Ustawa o samorządzie województwa. Komentarz*, LEX 2008.

respective entity – encompassing first and last name, telephone number, and email address – within 14 days of the designation of such a person, as well as to report any changes in these details within 14 days.

In accordance with Article 2 (2) of the NCSA, CSIRT MON is the national-level Computer Security Incident Response Team headed by the Minister of National Defence. In line with Article 2 (3) of the NCSA, CSIRT NASK is the national-level Computer Security Incident Response Team headed by NASK – the National Research Institute. CSIRT GOV is the national-level Computer Security Incident Response Team under the Head of the Internal Security Agency, as stipulated in Article 2 (1) of the NCSA.

Pursuant to Article 2 (5) of the NCSA, an "incident" should be understood as an occurrence which adversely affects, or might adversely affect, cybersecurity (i.e. impairs the resilience of information systems against actions which compromise the confidentiality, integrity, accessibility, and authenticity of the data being processed in such systems, or of related services provided by such systems). Under Article 2 (9) a public-entity incident is one which impairs, or might impair, the quality of, or disrupt the performance of, a public function by a public entity, as referred to in Article 4 (7–15) of the NCSA.

Public-entity incident management represents an internal matter for the respective public entity once the incident has occurred. In such an event, the public entity has an obligation to handle the incident, i.e. to take measures to identify, register, analyse, classify, prioritise, contain, and remedy the incident. The lawmakers used the term "ensure" to oblige public entities to deploy sufficient human and financial resources to handle public-entity incidents comprehensively[15]. In accordance with Article 2 (18) of the NCSA, incident management should be understood as handling incidents, identifying links between incidents, eliminating their causes, and drawing post-incident conclusions. The notion encompasses "incident handling", which, in line with Article 2 (10) of the NCSA, should be understood as taking measures to identify, register, analyse, classify, prioritise, contain, and remedy incidents.

Under Article 26 (2) of the NCSA, CSIRT MON, CSIRT NASK, and CSIRT GOV may provide support in handling incidents, where reasonable, at the request of operators of essential services, digital-service providers, public entities as referred to in Article 4 (7––15) of the NCSA, sectoral cybersecurity

15 K. Czaplicki, *Komentarz do art. 22*, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa...*, red. idem, A. Gryszczyńska, G. Szpor.

teams, or owners, independent possessors or dependent possessors of structures, facilities, installations, devices, equipment or services which are part of a critical infrastructure. CSIRT MON, CSIRT NASK and CSIRT GOV may provide support only at the request of one of the aforementioned entities, and they may take no action on their own initiative. Notably, such support is optional, and they have no obligation to provide it.

The lawmakers have used the categorical term "ensure" in relation to incident management by the appropriate entity. Hence, once such a public-entity incident has occurred, the appropriate entity is obliged to use available resources to ensure that the incident is handled, links between incidents are identified, their causes are eliminated and post-incident conclusions are drawn. While exemptions from this obligation are not allowed, there is a legal possibility to secure support in incident handling (provided that the entity named by the appropriate Act can lend such support).

Similarly, public entities are required to "report" incidents, and they must do so without delay, within a maximum of 24 hours from detection (not their occurrence). Such prompt action is important in that it allows a quick response to prevent a range of consequences. For expediency, incidents are reported electronically, and, where this is impossible, using other available means of communication. Information on the incident must reach the addressee as soon as possible.

Public entities "ensure" that incidents and critical incidents are handled. This is done in cooperation with the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV, and involves the provision of essential data, including personal details. They fulfil this obligation not on their own, but in conjunction with other, specialised, entities. Essential data are those which facilitate the appropriate measures to detect, register, analyse, classify, prioritise, contain, and remedy incidents.

Under Article 2 (6) of the NCSA a critical incident to be handled by a public entity is an occurrence which seriously compromises security or public order, and/or jeopardises international interests, economic interests, public institutions' activities, civic rights and freedoms, and/or human health and lives, as classified by the appropriate CSIRT MON, CSIRT NASK, or CSIRT GOV. Such incidents, then, encroach on the sphere of security[16]. Security –

16 For more on security, see M. Karpiuk, *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne Humanum" 2018, vol. 2, p. 67–70; M. Czuryk, *Bezpieczeństwo jako dobro*

to be protected by such handling of incidents – involves detecting and counteracting threats, and taking measures to minimise and eliminate their consequences. Critical incidents affect both security and public order[17]. Public order is an organised and harmonious system of legally guaranteed legal and social relations allowing public institutions, private entities, and social organisations, as well as the public at large, including its groups and individual members, to function unhindered.

Public entities provide individuals for whom public functions are performed with access to expert knowledge. This knowledge should help them to understand cybersecurity threats and use effective measures to protect themselves against these threats. And this means identifying the potential cause of the incident.

wspólne, „Zeszyty Naukowe KUL" 2018, vol. 3, p. 15; M. Karpiuk, *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013, p. 77–89; *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, red. W. Kitler, M. Czuryk, M. Karpiuk, Warszawa 2013, p. 11–45; M. Karpiuk, *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia Iuridica Lublinensia" 2017, vol. 4, p. 10; M. Czuryk, K. Drabik, A. Pieczywok, *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olszyn 2018, p. 7; M. Czuryk, J. Kostrubiec, *The legal status of local self-government in the field of public security*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2019, vol. 1, p. 33–47; M. Karpiuk, *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014, p. 28–34; K. Bojarski, *Współdziałanie administracji publicznej z organizacjami pozarządowymi w sferze bezpieczeństwa wewnętrznego w ujęciu administracyjno-prawnym*, Warszawa–Nisko 2017, p. 19–72; W. Lis, *Bezpieczeństwo wewnętrzne i porządek publiczny jako sfera działania administracji publicznej*, Lublin 2015, p. 29–46; D. Tyrawa, *Gwarancje bezpieczeństwa osobistego w polskim administracyjnym prawie drogowym*, Lublin 2018, p. 40–46; K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, Toruń 2019, p. 15–24; M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop, *Prawo zarządzania kryzysowego. Zarys systemu*, Olsztyn 2016, p. 13; M. Karpiuk, *Służba wojskowa żołnierzy zawodowych*, Olsztyn 2019, p. 15–17; J. Kostrubiec, *Status of a Voivodeship Governor as an Authority Responsible for the Matters of Security and Public Order*, „Barometr Regionalny" 2018, vol. 5, p. 35–40; K. Chałubińska-Jentkiewicz, M. Karpiuk, K. Zalasińska, *Prawo bezpieczeństwa kulturowego*, Siedlce 2016, p. 7.

17 For more on public order, see: M. Karpiuk, K. Prokop, P. Sobczyk, *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017, p. 14–21; K. Chałubińska-Jentkiewicz, *Moralność publiczna w polskim prawie gospodarczym i w prawie mediów*, [in:] *Klauzule porządku publicznego i moralności publicznej*, red. G. Blicharz, M. Delijewski, Warszawa 2019, p. 244–245; M. Karpiuk, N. Szczęch, *Bezpieczeństwo narodowe i międzynarodowe*, Olszyn 2017, p. 96–102, A. Pieczywok, *Profesjonalność funkcjonariuszy wybranych służb w obszarze bezpieczeństwa i porządku publicznego*, [in:] *Służba w formacjach bezpieczeństwa i porządku publicznego*, red. M. Karpiuk, A. Pieczywok, Warszawa 2016, p. 10; M. Karpiuk, *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, vol. 9, p. 11.

Public entities "provide" the personal details of the contact person to communicate with entities within the national cybersecurity system. This information makes it possible to verify the contact person and prevent communication by unauthorised individuals. Such data must be known to CSIRT MON, CSIRT NASK, or CSIRT GOV.

There are formal requirements to be observed when reporting public-entity incidents to the appropriate CSIRT MON, CSIRT NASK, or CSIRT GOV. In accordance with Article 23 (1) of the NCSA, a public-entity incident report should include 1) the details of the reporting entity, including its name, appropriate-register number, head office, and address; 2) the first and last names, telephone number and email address of the reporting individual; 3) the first and last names, telephone number and email address of the individual authorised to provide explanations on the reported information; 4) a description of how the public-entity incident has affected the performance of its public function, including a) which public function has been affected, b) how many people have been affected, c) the time at which the incident occurred and was detected, and how long it continued, d) the geographical range of the incident, e) the cause of the incident and how it developed, and its impacts on the information systems of the public entity affected, 5) information on the cause and source of the incident, 6) information on any preventive measures taken, 7) information on any remedial action taken, 8) any other relevant information. This information is provided to facilitate a quick and commensurate response to the threat, and to allow a preliminary determination of the nature and consequences of the incident, followed by the appropriate remedial action.

Since the information provided at the time of the incident might be incomplete, and since the public entity affected will learn more about the incident as it develops, such a public entity has the obligation to update the information given at the time of the report, and to send such updated information to the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV. This is the optimum solution to handle incidents.

It is unreasonable to require public entities to furnish all the essential information, such as the source and cause of the incident, and the preventive and remedial measures taken against it, within as short a time as 24 hours. Any information emerging thereafter should be provided immediately after being obtained. Affected entities should not wait until all the appropriate

information is available. Rather, they are required to send any fragmentary information obtained on an ongoing basis[18].

Under Article 23 (3) of the NCSA, where necessary for the appropriate CSIRT MON, CSIRT NASK, or CSIRT GOV to fulfil their functions, public entities are required to file incident reports containing information considered to be legally protected secrets, including trade secrets. If the effects of an incident are significant, the lawmakers have provided for the possibility of providing extensive information, including legally protected information, with the caveat that the public entity's report must state explicitly what information constitutes legally protected secrets, including trade secrets.

A trade secret should be understood as any technical, technological, process-related, or organisational information of a business, or any other commercially valuable information, which as a whole, or when in a specific combination or collection of its elements, is not commonly known to the individuals dealing routinely with such information, or which is not easily accessible by such individuals, provided that the entity or person authorised to use or manage such information has taken, with due diligence, measures to maintain their confidentiality[19].

Legally protected secret information is classified information, the unauthorised disclosure of which might cause harm to the Republic of Poland, or be disadvantageous to its interests, including any disclosure while such information is being developed, regardless of its form and manner of expression[20].

18 K. Czaplicki, *Komentarz do art. 23*, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa...*, red. idem, A. Gryszczyńska, G. Szpor.

19 Article 11 (2) of the Unfair Competition Act of 16 April 1993 (consolidated text, Journal of Laws of 2019, item 1010, as amended).

20 The definition of classified information is provided in Article 1 (1) of the Classified Information Protection Act of 5 August 2010 (consolidated text, Journal of Laws of 2019, item 742, as amended) ("the CIA"). In order for a piece of information to be considered classified, and as such subject to disclosure restrictions, it is sufficient to determine whether the substantial prerequisite defined in Article 1 (1) of the CIA is met; Judgment of the Supreme Administrative Court of 9 October 2017, I OSK 1822/16, LEX no. 2461535. Accordingly, in order to recognise a piece of information as classified, it is enough that a substantial component is involved, i.e. an attribute which would make the unauthorised disclosure of the piece of information a cause of harm to the Republic of Poland, or of a disadvantage to its interests, including any disclosure while such information is being developed, regardless of its form and manner of expression (Article 1 (1) of the CIA.); Judgment of the Supreme Administrative Court of 8 March 2017, I OSK 1777/15, LEX No. 2338895.

A piece of information is classified due to its contents. Marking it as classified serves only as guidance for the recipient to ensure that it is properly protected against unauthorised disclosure or destruction. Disclosure is considered to be unlawful when a piece of information which has the attribute of secrecy is released outside legally authorised circles, or when it is deprived of such an attribute in violation of the secrecy obligation[21].

Should the appropriate CSIRT MON, CSIRT NASK, or CSIRT GOV conclude that the information provided in the report is incomplete, pursuant to Article 23 (4) of the NCSA it may request the public entity to supplement the report with the missing information, including legally protected secrets, to the extent necessary to perform the functions referred to in the Act.

Classified information must be appropriately marked as such. In accordance with Article 5 of the CIA, classified information must be marked as "Top Secret" if their unauthorised disclosure might cause significant damage to the Republic of Poland by 1) jeopardising the independence, sovereignty, or territorial integrity of the Republic of Poland; 2) jeopardising the internal security or constitutional order of the Republic of Poland; 3) jeopardising the alliances or international position of the Republic of Poland; 4) weakening the defence preparedness of the Republic of Poland; 5) causing, or potentially causing, the identification of officers, soldiers, or active intelligence or counterintelligence personnel, where such identification can put their operational safety at risk, or lead to the identification of their sources; 6) putting or potentially putting at risk the lives of health of officers, soldiers, or active intelligence or counterintelligence personnel, or their sources; 7) putting or potentially putting at risk the health or lives of crown witnesses, or their closest relatives, and people granted with State protection and assistance. Classified information must be marked as "secret" if their unauthorised disclosure might cause significant harm to the Republic of Poland by 1) preventing the fulfilment of functions associated with defending the sovereignty or constitutional order of the Republic of Poland; 2) damaging the relations between the Republic of Poland and other States and international organisations; 3) disrupting the State's defence preparations or the functioning of the Armed Forces of the Republic of Poland; 4) hindering intelligence operations conducted to ensure State security and the pursuing of criminals by the appropriate authorities and institutions; 5) significantly

21 I. Stankowska, *Komentarz do art. 1*, [in:] eadem, *Ustawa o ochronie informacji niejawnych. Komentarz*, LEX 2014.

disrupting the functioning of law-enforcement agencies and the judicial authorities; 6) causing substantial harm to the economic interests of the Republic of Poland. Information is marked as "confidential" if its unauthorised disclosure might cause harm to the Republic of Poland by 1) hindering foreign policy implementation by the Republic of Poland; 2) hindering the implementation of defence projects, or compromising the combat capability of the Armed Forces of the Republic of Poland; 3) disrupting public order or putting the safety of citizens at risk; 4) obstructing the operations of services and institutions in charge of safeguarding the security or vital interests of the Republic of Poland; 5) obstructing the operations of services and institutions in charge of protecting public order and citizens' safety, and pursuing criminals, including tax criminals, and of the judicial authorities; 6) putting at risk the stability of the financial system of the Republic of Poland; 7) exerting an adverse impact on the functioning of the national economy. Classified information is marked as "restricted" where they have not been assigned a higher degree of secrecy, and their unauthorised disclosure could adversely affect the operations of public authorities or other organisational units related to national defence, foreign policy, national security, the protection of civic rights and freedoms, the economic interests of the Republic of Poland, and the functioning of the judiciary[22].

Pursuant to Article 24 of the NCSA, public entities serving public functions which rely on information systems may provide the appropriate CSIRT

22 In order for a specific piece of information to be considered legally protected classified information, it is not necessary to mark such information in one of the ways provided for in the CIA; Judgment of the Supreme Administrative Court of 25 April 2019, I OSK 2344/18, LEX No. 2677192. Classified information is subject to protection regardless of whether it has been marked as secret by anyone authorised to do so; Judgment of the Supreme Administrative Court of 8 March 2017, I OSK 1777/15, LEX No. 2338895. For more about the protection of classified information, see M. Karpiuk, *Odmowa wydania poświadczenia bezpieczeństwa przez polskie służby ochrony państwa*, „Secretum" 2015, vol. 2, p. 137–147; K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015, p. 442–449; M. Bożek, M. Czuryk, M. Karpiuk, J. Kostrubiec, *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014, p. 66–75; M. Karpiuk, *Miejsce bezpieczeństwa osobowego w systemie ochrony informacji niejawnych*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2018, vol. 1, p. 85–99; M. Czuryk, *Właściwość Rady Ministrów oraz Prezesa Rady Ministrów w zakresie obronności, bezpieczeństwa i porządku publicznego*, Olszyn 2017, p. 109–137; M. Karpiuk, K. Chałubińska-Jentkiewicz, *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015, p. 151–173; M. Czuryk, *Informacja w administracji publicznej. Zarys problematyki*, Warszawa 2015, p. 161–177; K. Chałubińska-Jentkiewicz, M. Karpiuk, *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015, p. 33–40.

MON, CSIRT NASK, or CSIRT GOV with information on 1) other incidents; 2) cybersecurity threats (under Article 2 (17) of the NCSA a cybersecurity threat is the potential cause of an incident); 3) risk estimation (risk estimation is the process of identifying, analysing, and assessing risk); 4) vulnerabilities (under Article 2 (11) a vulnerability is the property of an information system which can be taken advantage of through a cybersecurity threat); 5) the technologies in use. Such information is reported electronically, and, where impossible, using other available means of communication. The right arising from Article 24 does not relate to public-entity incidents, but to the early warning of the appropriate CSIRTs about potential future risks. Information provided in accordance with this provision is obtained by public entities, and does not relate to them directly, or has not caused any incidents yet, but might be of interest to the appropriate CSIRTs due its nature [23].

Should the public entity referred to in Article 4 (7–15) be considered an operator of essential services, in accordance with Article 25 the provisions of Chapter 3 of the NCSA shall apply to such a public entity to the extent that it provides an essential service underlying its recognition as an operator of essential services. Consequently, the public entity is obliged to implement a security-management procedure in the information system it uses to provide the essential service. This obligation is imposed by Article 8 of the NCSA. In line with this provision, the key-service operator is required to implement a security-management procedure in the information system used to provide the essential service for the purposes of 1) systematic incident-risk estimation and management; 2) implementing suitable, risk-proportionate, technical and organisational measures based on the state of the art, including a) the maintenance and safe operation of the information system; b) physical and environmental security, including access control; c) ensuring the security and continuity of the services on which the provision of the essential service relies; d) implementing, documenting, and maintaining action plans to facilitate continuous and undisrupted provision of essential services, and to ensure the confidentiality, integrity, accessibility, and authenticity of information; e) placing the information system used to provide the essential service under continuous monitoring; 3) collecting information on cyberthreats and the incident vulnerability of the information system used to provide the essential

23 K. Czaplicki, *Komentarz do art. 24*, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa...*, red. idem, A. Gryszczyńska, G. Szpor.

service; 4) incident management; 5) implementing measures to prevent and contain the impact of incidents on the security of the information system used to provide the essential service, including a) using the mechanisms which ensure the confidentiality, integrity, accessibility, and authenticity of the data processed in the information system; b) making sure that the software is up to date; c) protecting the information system against unauthorised modifications; d) taking immediate measures once a vulnerability or threat to cybersecurity is identified; 6) applying measures to make sure that communications within the national cybersecurity system are smooth and secure.

The obligations imposed on operators of essential services include core measures and processes such as risk management and implementing physical, technical, and organisational security measures on its basis; incident management, as well as managing effective incident responses; ensuring the security of the communication channel within the national cybersecurity system. Operators of essential services should ensure the continuous and undisrupted functioning of the processes involved in the provision of essential services. Continuity management is an integral part of the holistic process of risk management, its aim being to safeguard key-stakeholder interests and their reputation-, brand- and value-creating activities[24].

The authority in charge of cybersecurity matters issues a decision on recognising an entity as an operator of essential services on condition that 1) the entity is providing an essential service; 2) the provision of such a service relies on information systems; 3) an incident would significantly disrupt the provision of the essential service by such an operator, as explicitly arising from Article 5 (2) of the NCSA. The substantive criterion for recognising an entity as an operator of essential services is based on three prerequisites: 1) the provision of an essential service; 2) the reliance of the essential-service provision on information systems; 3) the significance of the degree to which the incident would disrupt the essential-service provision by that operator. All these requirements should be met, and their fulfilment should be demonstrated in the rationale for the recognition decision[25].

24 K. Świtała, *Komentarz do art. 8*, [in:] ibidem.
25 M. Wilbrandt-Gotowicz, *Komentarz do art. 5*, [in:] ibidem.

Bibliography

Literature

Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna, red. W. Kitler, M. Czuryk, M. Karpiuk, Warszawa 2013.

Bojarski K., *Współdziałanie administracji publicznej z organizacjami pozarządowymi w sferze bezpieczeństwa wewnętrznego w ujęciu administracyjno-prawnym*, Warszawa–Nisko 2017.

Bożek M., Czuryk M., Karpiuk M., Kostrubiec J., *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014.

Chałubińska-Jentkiewicz K., *Cyberodpowiedzialność*, Toruń 2019.

Chałubińska-Jentkiewicz K., *Moralność publiczna w polskim prawie gospodarczym i w prawie mediów*, [in:] *Klauzule porządku publicznego i moralności publicznej*, red. G. Blicharz, M. Delijewski, Warszawa 2019.

Chałubińska-Jentkiewicz K., Karpiuk M., *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015.

Chałubińska-Jentkiewicz K., Karpiuk M., Zalasińska K., *Prawo bezpieczeństwa kulturowego*, Siedlce 2016.

Czuryk M., *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, t. 3.

Czuryk M., *Informacja w administracji publicznej. Zarys problematyki*, Warszawa 2015.

Czuryk M., *Właściwość Rady Ministrów oraz Prezesa Rady Ministrów w zakresie obronności, bezpieczeństwa i porządku publicznego*, Olszyn 2017.

Czuryk M., Drabik K., Pieczywok A., *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olszyn 2018.

Czuryk M., Dunaj K., Karpiuk M., Prokop K., *Prawo zarządzania kryzysowego. Zarys systemu*, Olsztyn 2016.

Czuryk M., Kostrubiec J., *The legal status of local self-government in the field of public security*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2019, t. 1.

Karpiuk M., *Konstytucyjna właściwość Sejmu w zakresie bezpieczeństwa państwa*, „Studia Iuridica Lublinensia" 2017, t. 4.

Karpiuk M., *Miejsce bezpieczeństwa osobowego w systemie ochrony informacji niejawnych*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2018, t. 1.

Karpiuk M., *Miejsce samorządu terytorialnego w przestrzeni bezpieczeństwa narodowego*, Warszawa 2014.

Karpiuk M., *Odmowa wydania poświadczenia bezpieczeństwa przez polskie służby ochrony państwa*, „Secretum" 2015, t. 2.

Karpiuk M., *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, nr 9.

Karpiuk M., *Samorząd terytorialny a państwo. Prawne instrumenty nadzoru nad samorządem gminnym*, Lublin 2008.

Karpiuk M., *Służba wojskowa żołnierzy zawodowych*, Olsztyn 2019.

Karpiuk M., *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, t. 2.

Karpiuk M., *Zadania i kompetencje zespolonej administracji rządowej w sferze bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty materialne i formalne*, Warszawa 2013.

Karpiuk M., Chałubińska-Jentkiewicz K., *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015.

Karpiuk M., Prokop K., Sobczyk P., *Ograniczenie korzystania z wolności i praw człowieka i obywatela ze względu na bezpieczeństwo państwa i porządek publiczny*, Siedlce 2017.

Karpiuk M., Szczęch N., *Bezpieczeństwo narodowe i międzynarodowe*, Olszyn 2017.

Kostrubiec J., *Status of a Voivodeship Governor as an Authority Responsible for the Matters of Security and Public Order*, „Barometr Regionalny" 2018, t. 5.
Lis W., *Bezpieczeństwo wewnętrzne i porządek publiczny jako sfera działania administracji publicznej*, Lublin 2015.
Pieczywok A., *Profesjonalność funkcjonariuszy wybranych służb w obszarze bezpieczeństwa i porządku publicznego*, [in:] *Służba w formacjach bezpieczeństwa i porządku publicznego*, red. M. Karpiuk, A. Pieczywok, Warszawa 2016.
Stankowska I., *Ustawa o ochronie informacji niejawnych. Komentarz*, LEX 2014.
Szewc A., *Ustawa o samorządzie województwa. Komentarz*, LEX 2008.
Tyrawa D., *Gwarancje bezpieczeństwa osobistego w polskim administracyjnym prawie drogowym*, Lublin 2018.
Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, red. K. Czaplicki, A. Gryszczyńska, G. Szpor, LEX 2019.
Ustawa o samorządzie gminnym. Komentarz, red. P. Chmielnicki, LEX 2013.

Obowiązki podmiotów publicznych tworzących krajowy system cyberbezpieczeństwa

Streszczenie

Ustawodawca w ramach krajowego systemu cyberbezpieczeństwa nakłada na poszczególne podmioty wiele obowiązków związanych z zapewnieniem odporności systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Należą do nich obowiązki w zakresie zgłaszania i obsługi incydentu w podmiocie publicznym, a także obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Powyższe obowiązki zostały nałożone nie na wszystkie podmioty publiczne, a wyraźnie wskazane przez ustawodawcę. Ważne spektrum działań w tym zakresie dotyczy incydentów występujących w podmiocie publicznym, czyli incydentów, które powodują lub mogą spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego wykonywanego przez podmiot publiczny. Szczególne miejsce wśród obowiązków podmiotów publicznych zajmuje obsługa incydentów rozumiana jako czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzacja, podejmowanie działań naprawczych i ograniczenie skutków incydentu.

Słowa kluczowe: cyberbezpieczeństwo, system informacyjny, incydent, usługa kluczowa