Mirosław Karpiuk*

Cybersecurity-related responsibilities of the minister competent for computerisation

Abstract

The legislator has awarded the status of being the authority competent for ensuring cybersecurity to the minister competent for computerisation in respect of digital service providers. The minister manages computerisation, a government administration department which entails cyberspace security in the civilian dimension. The range of the official's activities includes monitoring, information activities and reporting. As a competent authority for ensuring cybersecurity, the minister also no.s decisions on recognising a digital infrastructure sector entity as an operator of essential services.

Key words: cybersecurity, the minister competent for computerisation, communication and information systems

* Prof. Mirosław Karpiuk, PhD, Chair of Administrative Law and Security Studies, Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, e-mail: miroslaw.karpiuk@uwm.edu.pl, ORCID: 0000-0001-7012-8999.

The office of the minister competent for computerisation plays an important role in the sphere of cybersecurity. The minister runs the computerisation department, which includes such matters as: 1) the computerisation of public administration and entities performing public tasks; 2) communication and information systems, and networks of public administration, 3) the support for investment in computerisation; 4) the fulfilment of the international obligations of the Republic of Poland in the sphere of computerisation and telecommunications; 5) participation in the shaping of European Union's computerisation policy; 6) the development of an information society and the counteracting of digital exclusion; 7) the development of services provided by electronic means; 8) the shaping of state policy in respect of personal data protection; 9) telecommunications; 10) cyberspace security in the civilian dimension; and 11) electronic identification[1]. Cyberspace security in the civilian dimension belongs to the scope of operations pursued by the minister competent for computerisation, while in peacetime the Minister of National Defence performs tasks related to the sphere of cyberspace security in the military dimension. However, not all matters related to the sphere will belong to the competence of that minister. The Prime Minister may entrust the performance of tasks in the sphere of public sector computerisation, digital innovation, information society development and the counteracting of digital exclusion to entities obligated to transfer and provide access to public sector information which is to be used for further purposes[2]. This entrustment is to facilitate the development of a digital society and to shape citizens' digital awareness, including making them more sensitised to cyberthreats, favouring the dissemination of information about the need to run such activities with the use of information and communication systems so as to respect cybersecurity principles.

Cybersecurity is currently a sphere which should be principally protected, which is directly related to the universal presence and development of services rendered by electronic means, via information and information systems. Threats which negatively affect the systems and disrupt their operation must not only be promptly eliminated, but should also be predicted and blocked. Protective measures, preventing or neutralising cyber-attacks, must constitu-

1 Art. 12a of the Act of 4 September 1997 on Government Administration Departments (consolidated text, Journal of Laws 2021, item 1893, as amended).

2 Art. 10c(1) of the Act of 8 August 1996 on the Council of Ministers (consolidated text, Journal of Laws of 2021, item 178, as amended).

te a priority in public administration policies, in particular in the era of a digital society.

The legislator defined cybersecurity as „the ability of information systems (information and communications systems with electronic data stored therein) to resist action that compromises the availability, authenticity, integrity and confidentiality of processed data or the related services offered by those information systems"[3]. The minister competent for computerisation deals with cybersecurity in the civilian dimension, within the meaning indicated above.

In line with Art. 45 of the NCSA, the minister competent for computerisation is responsible for: 1) monitoring the implementation of the Cybersecurity Strategy of the Republic of Poland and implementing action plans for strategy implementation, 2) recommending areas for cooperation within the private sector to strengthen the cybersecurity of the Republic of Poland; 3) preparing annual reports on: a) major incidents reported by operators of essential services, affecting the continuity of the services they render in the Republic of Poland, and the continuity of essential services provided in European Union Member States; b) material incidents reported by digital service providers, including incidents affecting two or more European Union Member States, 4) conducting informational activities concerning good practices, educational programmes, campaigns and training to extend the knowledge and to raise awareness of cybersecurity, including safe use of the internet by various types of users; 5) collecting information about major incidents which affect or have been forwarded by another European Union Member State; and 6) providing access to information and good practices related to reporting major incidents by operators of essential services and material incidents by digital service providers, obtained from the Cooperation Group, including: a) the rules

3 Art. 2(4) of the National Cybersecurity System Act of 5 July 2018 (consolidated text, Journal of Laws 2020, item 1369, as amended), further referred to as the NCSA. For additional information about cybersecurity, refer to: M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies and cybersecurity*, ibidem 2019, no. 2; M. Karpiuk, *Activities of local government units in the scope of telecommunication*, ibidem, no. 1; K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2; I. Hoffman, K.B. Cseh, *E-administration, cybersecurity and municipalities – the challenges of cybersecurity no.s for the municipalities in Hungary*, ibidem 2020, no. 2; I. Hoffman, M. Karpiuk, *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, ibidem 2022, no. 1; M. Karpiuk, *Tasks of the Minister of National Defense in the area of cybersecurity*, ibidem.

of procedure for incident handling, b) the rules of procedure for risk management, c) the classification of information, risk factors and incidents. Under Art. 45 of the NCSA, the legislator has placed upon the minister competent for computerisation a set of organisational and reporting obligations[4].

One of the minister's tasks is to monitor the implementation of the Cybersecurity Strategy of the Republic of Poland. As laid down in Art. 68 of the NCSA, the strategy is adopted by the Council of Ministers by way of a resolution. Therefore, it is not a source of generally applicable law, but an internal legal regulation. Given the above, the strategy does not have any external implications, and cannot constitute any grounds for imposing specified obligations on entities outside the organisational structure of the authority which has no.d such a legal act. Accordingly, the Cybersecurity Strategy of the Republic of Poland has a limited legal effect.

Resolutions no.d by the Council of Ministers are internal regulations. They must be observed only by organisational units subordinate to the authority which no.s such legal acts[5]. Unlike the system being the source of generally applicable laws, internal legal acts form an open-ended system[6].

The main objectives of the strategy are to improve the levels of resilience to cyber threats, to increase the level of information protection in the public, military and private sectors, and to promote knowledge and good practices helping citizens to better protect their information. Specific objectives include: 1) developing the national cybersecurity system, 2) increasing the level of resilience of information systems operated by both the public administration and the private sector, and providing the capability to effectively prevent, and respond to, incidents; 5) boosting national potential in the sphere of security in cyberspace; 4) raising awareness and social competences in the sphere of cybersecurity; 5) building a strong international position of the Republic of Poland in the sphere of cybersecurity.

The draft strategy is prepared by the minister competent for computerisation in cooperation with the Government Plenipotentiary for Cybersecurity along with other ministers and other relevant senior officers of central agencies. The

4 K. Chałubińska-Jentkiewicz, *Komentarz do art. 45* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, p. 281.

5 Art. 93(1) of the Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws 1997, no. 78, item 483, as amended).

6 Judgement of the Supreme Administrative Court of 10 August 2005, OSK 1826/04, LEX no. 1574295.

representative of the President of the Republic of Poland may also take part in the works on preparing the draft. The above powers have been set out in Art. 70 of the NCSA. The cooperation is to facilitate the preparation of the draft strategy, corresponding to the threats which are emerging, or which might occur, in the future in cyberspace.

The Government Plenipotentiary for Cybersecurity is responsible for coordinating actions and for the implementation of Government policies for assuring cybersecurity of the Republic of Poland, thus the engagement of this official in the development of the strategy seems necessary. The participation of ministers and relevant senior officers of central agencies might in turn be justified by their diverse roles and tasks, the performance of which is necessary to develop and effectively implement the strategy. Furthermore, the participation of these entities in the development of the strategy is indispensable due to the need to ensure the security and protection against cybersecurity threats to information systems operated not only by entities classified as operators of essential services, but also the information systems of public entities (who are not operators of essential services) performing public tasks via the systems, in order to prevent incidents which may result in reduced quality or disrupt the performance of a public task[7].

The minister competent for computerisation provides relevant information obtained from the Cooperation Group, which has been established to support and facilitate strategic cooperation and the exchange of information between Member States, as well as to increase trust and confidence, with a view to reaching a high common level of security of networks and information systems in the European Union[8]. The position of the Chair of the Cooperation Group is filled by a representative of the Member State holding the Presidency of the Council of the European Union. In the performance of his or her tasks, the Chair is supported by the representative of a Member State which held the previous presidency of the Council of the European Union, and the representative of a state which will hold the next presidency[9].

7 I. Szulc, *Komentarz do art. 70* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, ed. A. Besiekierska, Warszawa 2019.

8 Art. 11(1) of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Official Journal of the European Union 2016, L 194, p. 1).

9 Art. 2(1) of Commission Implementing Decision (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Art. 11(5) of the Directive (EU) 2016/1148 of the European Parliament

As laid down in Art. 46 of the NCSA, the minister competent for computerisation is obligated to ensure the development and maintenance of an information and communication system[10] supporting: 1) the cooperation between entities forming part of the national cybersecurity system; 2) generating and handing over recommendations about activities aimed at increasing the level of cybersecurity; 3) reporting and handling incidents; 4) performing risk assessments at the national level, and 5) warning about cybersecurity threats. CSIRT MON, CSIRT NASK, CSIRT GOV, sectoral cybersecurity teams, and the President of the Office of Electronic Communications may use the information and communication system on the basis of an agreement with the minister competent for computerisation, under which the scope and conditions for using the system are defined. The information and communication system referred to in Article 46 of the NCSA is very important from the perspective of cybersecurity, and it plays a vital role in this sphere. For instance, it facilitates cooperation between the entities forming part of the national cybersecurity system, and provides warnings against cyberthreats.

The minister competent for computerisation not only ensures the development or the maintenance of the communication and information system through which the national cybersecurity system is supported, but is also obliged to have such a system established.

The group of entities authorised to use the information and communication system referred to in Art. 46 of the NCSA includes Computer Security Incident Response Teams operating at the national level, and managed by the Head of the Internal Security Agency, the Minister of National Defence or the Research and Academic Computer Network – National Research Institute (NASK), as well as sectoral cybersecurity teams and the President of the Office of Electronic Communications.

It should be stressed that CSIRT MON, CSIRT NASK and CSIRT GOV teams cooperate with the minister competent for computerisation, ensuring a coherent and complete risk management system at the national level, performing tasks aimed at counteracting supra-sectoral and cross-border

and of the Council concerning measures for a high common level of security of network and information systems across the Union (Official Journal of the European Union 2017, L 28, p. 73).

10 An information and communication system is a set of cooperating IT hardware and software, providing the possibility to process and store, as well as send and receive, data via ICT networks with the use of a terminal device suitable for a given network type – Art. 3(3) of the Act on the Computerisation of the Operations of the Entities Performing Public Tasks (consolidated text, Journal of Laws 2021, item 2070, as amended).

cybersecurity threats, and facilitating the coordination of incident handling, once they are notified. The above sphere of cooperation has been set out in Art. 26 of the NCSA.

Sectoral cybersecurity teams are primarily responsible for: 1) receiving notifications of major incidents and supporting incident-handling activities; 2) supporting operators of essential services in the performance of specified obligations, 3) analysing major incidents, searching for links between incidents and preparing conclusions to be derived from incident handling actions, and 5) cooperating with relevant CSIRT MON, CSIRT NASK and CSIRT GOV teams in the scope of coordinating actions aimed at handling major incidents. These powers are specified in Article 44 of the NCSA.

Telecommunications operators are obliged to immediately inform the President of the Office of Electronic Communications about any breaches of security or the integrity of networks or services which have had a significant impact on the functioning of such networks or services, and about preventive and corrective actions. The President of the Office of Electronic Communications forwards the information to a CSIRT with jurisdiction over the notifying telecommunications operator if it refers to events which can be categorised as incidents[11].

Pursuant to Art. 48 of the NCSA, the minister competent for computerisation manages the single point of contact whose tasks include: 1) receiving notifications of major incidents or material incidents affecting two or more European Union Member States from single points of contact designated in other European Union Member States, and forwarding the notifications to CSIRT MON, CSIRT NASK, CSIRT GOV or sectoral cybersecurity teams, 2) forwarding, at the request of a competent CSIRT MON, CSIRT NASK or CSIRT GOV, notifications of major or material incidents affecting two or more European Union Member States to single points of contact designated in other European Union Member States; 3) ensuring the representation of the Republic of Poland in the Cooperation Group; 4) ensuring cooperation with the European Commission in the sphere of cybersecurity; 5) coordinating

11 Art. 175a of the Act of 6 July 2004 – Telecommunications Law (consolidated text, Journal of Laws 2021, item 576, as amended). The provision imposes a burdensome obligation on telecommunications operators, as they must notify the President of the Office of Electronic Communications each time they identify a breach which has had a significant impact on the functioning of networks or services, A. Krasuski, *Komentarz do art. 175a* [in:] idem, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2015.

collaboration between competent authorities for cybersecurity and public authorities in the Republic of Poland and the respective authorities of other European Union Member States; and 6) ensuring the exchange of information for the purpose of the Cooperation Group and the CSIRTs Network[12].

As laid down in Art. 47 of the NCSA, the minister competent for computerisation may perform tasks in the sphere of cybersecurity through competent units which are subordinate to, or supervised by, the said ministry. The tasks entrusted to these units are financed in the form of a special-purpose subsidy from state budget funds to be distributed by the minister competent for computerisation. In other words, the minister competent for computerisation finances the entrusted tasks in the sphere of cybersecurity by way of special-purpose subsidies.

Subsidies are funds from the state budget, local government budgets or state special-purpose funds, subject to special settlement rules, allocated for the financing or co-financing of the performance of public tasks under the Act, other Acts, or international agreements[13]. Special-purpose subsidies are in particular allocated for under Art. 127(1) of the Public Finance Act:

12 The European Union legislator has established a network of national CSIRTs to contribute to the development of confidence and trust between Member States and to promote swift and effective operational cooperation. The CSIRTs Network is composed of representatives of the Member States' CSIRTs and CERT-EU. The Commission participates in the CSIRTs Network as an observer. ENISA provides the secretariat and actively supports the cooperation among the CSIRTs. The CSIRTs Network has the following tasks: 1) exchanging information on CSIRTs' services, operations and cooperation capabilities; 2) at the request of a representative of a CSIRT from a Member State potentially affected by an incident, exchanging and discussing non-commercially sensitive information related to that incident and associated risks. However, any Member State's CSIRT may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident; 3) exchanging and making available on a voluntary basis non-confidential information concerning individual incidents; 4) at the request of a representative of a Member State's CSIRT, discussing, and where possible, identifying a coordinated response to an incident that has been identified within the jurisdiction of that same Member State; 5) providing Member States with support in addressing cross-border incidents on the basis of their voluntary mutual assistance; 6) discussing, exploring and identifying further forms of operational cooperation; 7) informing the Cooperation Group of its activities; 8) discussing lessons learnt from exercises relating to the security of network and information systems; 9) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT; and 10) issuing guidelines – Art. 12 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Official Journal of the European Union 2016, L 194, p. 1)

13 Article 126 of the Public Finance Act of 27 August 2009 (consolidated text, Journal of Laws 2021, item 305, as amended), further referred to as the PFA.

1) financing or co-financing: a) public administration tasks and other tasks commissioned to local government entities by law, b) statutory tasks, including tasks in the sphere of state patronage over culture, performed by entities other than local government entities, c) ongoing tasks of local government entities, d) the tasks of executive agencies, e) tasks commissioned to non-governmental organisations, f) the costs of investment project implementation; and 2) subsidies to bank loan interests. As regards entrusted tasks in the sphere of cybersecurity, financed via special-purpose subsidies from the part of the state budget which is distributed by the minister competent for computerisation, we are dealing with statutory tasks referred to in Art. 127(1)(b) of the Public Finance Act. Special-purpose subsidies are widely applicable. However, they are always awarded for specified purposes related to the performance of public tasks. Special-purpose subsidies cover not only the financing of ongoing tasks, but also investment projects and the implementation of programmes and projects financed from European Funds[14].

Bibliography

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021.

Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2.

Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies and cybersecurity*, „Cybersecurity and Law" 2019, no. 2.

Hoffman I., Cseh K.B., *E-administration, cybersecurity and municipalities – the challenges of cybersecurity no.s for the municipalities in Hungary*, „Cybersecurity and Law" 2020, no. 2.

Hoffman I., Karpiuk M., *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, „Cybersecurity and Law" 2022, no. 1.

Karpiuk M., *Activities of local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, no. 1.

Karpiuk M., *Tasks of the Minister of National Defense in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1.

Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.

Krasuski A., *Prawo telekomunikacyjne. Komentarz*, Warszawa 2015.

Ustawa o finansach publicznych. Komentarz, ed. C. Kosikowski, Warszawa 2011.

Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, ed. A. Besiekierska, Warszawa 2019.

Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.

14 C. Kosikowski, *Komentarz do art. 127* [in:] *Ustawa o finansach publicznych. Komentarz*, ed. C. Kosikowski, Warszawa 2011.

Zadania ministra właściwego do spraw informatyzacji w zakresie cyberbezpieczeństwa

Streszczenie

Ustawodawca przyznał ministrowi właściwemu do spraw informatyzacji status organu właściwego do spraw cyberbezpieczeństwa w odniesieniu do dostawców usług cyfrowych. Kieruje on działem administracji rządowej informatyzacja, w którym mieści się też bezpieczeństwo cyberprzestrzeni w wymiarze cywilnym. Do jego zadań należy m.in.: monitorowanie, działalność informacyjna, sprawozdawczość. Jako organ właściwy do spraw cyberbezpieczeństwa wydaje też decyzje o uznaniu podmiotu z sektora infrastruktury cyfrowej za operatora usługi kluczowej.

Słowa kluczowe: cyberbezpieczeństwo, minister właściwy do spraw informatyzacji, systemy teleinformatyczne