Personal Data Protection in the Context of the Act on the National Cybersecurity System

Monika Nowikowska

Abstract The dynamic development of technology has led to significant changes in the concept of cyberspace. Currently, it is primarily a virtual space in which we communicate with each other using computers, phones and tablets connected by a network. Cyberspace protection has now become one of the most frequently discussed security-related topics. At a time when information systems allow the collection of huge amounts of information, supervision over data security is one of the key challenges of each country and individual network users. This article describes the principles of personal data protection by national CSIRTs, which are responsible for handling and responding to computer security incidents.

The principles of personal data protection in cyberspace have been regulated under Polish law in several legal acts. The fundamental act which stipulates the protection of personal data, is the Constitution of the Republic of Poland of 2 April 1997.¹ The right to personal data protection is a unique legal construct intended to protect the values referred to in Article 47 of the Constitution of the Republic of Poland. The Constitution provides that everyone is entitled to the legal protection of his or her private life, family life, honour, and reputation, as well as the right to decide on their personal life.² In the relevant literature, the individual's right to the protection of his or her personal data is referred to as "information autonomy".³ The right to the protection of personal data is categorically associated with the right to privacy, recognising it as its unique form.⁴

¹The Constitution of the Republic of Poland of 2 April 1997, Polish Journal of Laws No. 78, item 483, as amended.

²Nowikowska (2018), p. 165.

³Safjan (1999), p. 9.

⁴Polok (2008), p. 26.

M. Nowikowska (✉)

Instytut Prawa/Institute of Law, Akademia Sztuki Wojennej w Warszawie/War Studies

University in Warsaw, Warsaw, Poland

e-mail: m.nowikowska@akademia.mil.pl

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (The General Data Protection Regulation) (GDPR), is also of fundamental importance in this regard.⁵ The issue of personal data is also governed by the Act of 10 May 2018 on personal data protection,⁶ which repealed several provisions of the former Act, and introduced new ones, which regulate, inter alia, the status of the President of the Personal Data Protection Office, as well as the procedure for initiating and conducting proceedings in connection with the infringement of personal data in the common courts, and the Act. The group of legislative acts regulating the principles of personal data processing in cyberspace also includes the Act on the National Cybersecurity System.

According to Article 1 of the GDPR, the EU legislators, when determining the adoption and application of uniform solutions for the processing of personal data in all EU Member States, pursue two equally important objectives: first, they protect the fundamental rights and freedoms of natural persons, and in particular the right to the protection of their personal data; and second, they ensure the free transfer of personal data between Member States.

According to the GDPR, “personal data” refers to any information concerning an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an internet identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a natural person.⁷

Polish literature sources emphasise that it is irrelevant to the principles of personal-data processing (including the determination of the scope and type of obligations incumbent on processors and personal-data controllers) that the processing of the data occurs in cyberspace.⁸ Ensuring cybersecurity is understood as ensuring the security of data and services, and, consequently, providing confidentiality, integrity, availability and authenticity. These characteristics are included in the literature as attributes of information security. Data confidentiality means the protection of communications or stored data against interception and reading by unauthorised persons. Data integrity is the confirmation that the data sent, received, or stored, are complete and unchanged. The concept of accountability is understood as ensuring that the activities of an entity can be unambiguously attributed only to that entity.

⁵Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (The General Data Protection Regulation), OJ EU 2016 L 119/1, as amended.

⁶Act of 10 May 2018 on personal-data protection, consolidated text Polish Journal of Laws of 2019, item 1781, as amended.

⁷Taczowska-Olszewska and Nowikowska (2019), p. 245.

⁸Taczowska-Olszewska (2019), p. 76.

Thus, the information/security attributes indicated in the Act fulfil a twofold function—i.e. they determine the standard of security in cyberspace, and simultaneously constitute a criterion for assessing the level of cybersecurity. The absence of any of the attributes indicated in the Act, or any infringement of the required standard of protection of confidentiality, integrity, availability, and authenticity, means the occurrence of an incident which, within the meaning of the Act, is an event which has or might have an adverse effect on Cybersecurity.⁹

Pursuant to the adoption on 6 July 2016 by the European Parliament and the Council of the European Union of Directive 2016/1148,¹⁰ all Member States were required to adopt a national strategy for the security of network and information systems. The preamble of the NIS Directive emphasises that IT networks, systems, and services perform an important role in society. Their reliability and security are crucial for economic and social activities, in particular for the functioning of the internal market. The scale, frequency, and impact of security incidents are increasing, and are posing a serious threat to the functioning of network and information systems. These systems can also become the object of deliberate harmful actions aimed at damaging or disrupting their operation. Moreover, these types of incident can hinder business activity, cause significant financial losses, undermine user confidence, and result in serious losses to the Union's economy.

In numerous cases there is a risk of personal data's being compromised as a result of incidents. In such a context, cybersecurity authorities and the President of the Personal Data Protection Office should cooperate and exchange information on all relevant issues in order to address any personal-data breaches resulting from such incidents.¹¹ Furthermore, the exchange of information on risks and incidents within the CSIRT cooperation group and network can involve the processing of personal data.

Such processing should generally be in accordance with the GDPR. However, it should be noted, in accordance with Article 2(2)(d) of the GDPR, that the processing of personal data in matters relating to national security is not governed by this Regulation. The Regulation does not apply to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, and prosecution of prohibited acts, or the enforcement of penalties, including protection against and the prevention of threats to public security.¹²

The principles of sharing information and processing personal data in the national cybersecurity system are regulated in detail in Chapter 7 of the Act on the National Cybersecurity System. In terms of information sharing, the legislators have introduced the principle that information about vulnerabilities, cybersecurity incidents

⁹Sieńczyło-Chlabicz et al. (2019), p. 145 et seq.

¹⁰Directive (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, OJ EU 2016 L 194/1.

¹¹Szostek (2017), p. 257 et seq.

¹²Nowikowska (2019), p. 163.

and threats, as well as the level of risk of an incident, for reasons of state security, and for the protection of the legally protected confidentiality of the providers of essential services and digital-services suppliers, are excluded from the scope of the Act on Access to Public Information. The relevant CSIRT MON, CSIRT NASK, or CSIRT GOV may, following consultation with the notifying providers of essential services, publish on the website of the Public Information Bulletin of the Minister of National Defence, the Scientific and Academic Computer Network—the State Research Institute, or the Internal Security Agency information concerning serious incidents, when it is necessary to prevent the occurrence of the incident or ensure dealing with it. A similar solution was adopted for reports of significant incidents from digital service providers. In the latter case, CSIRT MON, CSIRT NASK or CSIRT GOV may request the Cybersecurity Authority to oblige the digital service provider to make that information public when this is necessary to prevent the incident, or to effect dealing with the incident, as well as when, for any other reason, disclosure of the incident is in the public interest.

The divulging of such information must not violate the regulations on the protection of classified information, or of other legally protected secrets, or the regulations on personal data protection. Following the May 2018 entry into force of Regulation 2016/679, the NCSA legislators took into account the requirements of the GDPR for entities included in the national cybersecurity system, particularly with regard to the processing of data by CSIRTs, and by sectoral cybersecurity teams in connection with the support and coordination of incident handling. In order to perform tasks such as the monitoring of cybersecurity threats and incidents at the national level, the risk assessment of an identified threat, or issuing communications about identified cyber threats, CSIRT MON, CSIRT NASK, CSIRT GOV, and sectoral cybersecurity teams, may process data obtained in connection with cybersecurity incidents and threats, including sensitive personal data, within the scope, and for the implementation, of these tasks. These entities may process personal data obtained in connection with cyber incidents and threats

- (1) concerning users of information systems and telecommunications terminal equipment
- (2) concerning telecommunications equipment intended to be connected directly or indirectly to network terminals
- (3) collected by providers of essential services and digital service providers, for the purposes of the provision of services
- (4) collected by public entities in the implementation of public tasks, concerning the entities reporting the incident.

For the purposes of performing the tasks specified in the Act on the National Cybersecurity System, CSIRT MON, CSIRT NASK, CSIRT GOV, and other sectoral cybersecurity teams, may transfer data to each other to the extent necessary to perform these tasks, and to cooperate with the President of the Personal Data Protection Office. The data are deleted or anonymised as soon as it is determined that they are not essential for the performance of the assignment, or within 5 years from the end of the incident to which they relate. Insofar as the processing of data is

unrelated to national security, the Act provides for restrictions on the scope of certain obligations and rights for the controller or processor of personal data. Such restrictions include, but are not limited to, the data subject's right of access, the right of rectification, the right to limit the processing in the event when the accuracy of the data is challenged, and, in the event of an objection, the notification of the data subject about the recipients informed of the rectification or deletion of the personal data, where the exercise of this right would prevent CSIRT from accomplishing its tasks.

To summarise the above, it can be stated that the main task of CSIRTs is not to collect and process personal data—this is a secondary activity emanating from other tasks. In the course of monitoring cybersecurity incidents and threats or analytical activities, CSIRTs might encounter data which are generally non-personal data, but, as a result of the appropriate correlation of the information, might *become* such data, and be used to identify the perpetrator of an incident. Personal data which might be generated during the handling of an incident can include network-traffic content, data provided during the incident report, databases obtained as part of computer forensics, as well as logs and event logs. Due to the specificity of CSIRT, it is not possible to create an exhaustive list of the processed data. The explanatory memorandum of the Act emphasises that CSIRTs have no interest in personal data per se, but can be part of other data processing activities, especially with regard to a broad understanding of what personal data is. In such a case, intervention seems justified and proportionate.¹³

References

- Nowikowska M (2018) Ochrona danych osobowych w dokumentach kontrolnych. In: Taczkowska-Olszewska J, Nowikowska M, Brzostek A (eds) *Reforma ochrony danych osobowych. Cel, narzędzia, skutki*. Poznań
- Nowikowska M (2019) Zasady udostępniania informacji i przetwarzania danych osobowych. In: Taczkowska-Olszewska J, Chałubińska-Jentkiewicz K, Nowikowska M (eds) *Retencja, migracja i przepływ danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*. Warsaw
- Polok M (2008) *Bezpieczeństwo danych osobowych*. Warsaw
- Safjan M (1999) Ochrona danych osobowych – granice autonomii i informacji. In: Wyrzykowski M (ed) *Ochrona danych osobowych*. Warsaw

¹³Nowikowska (2019), p. 165.

- Sieńczyło-Chlabicz J, Zawadzka Z, Nowikowska M (2019) Prawo prasowe, Warsaw
- Szostek I (2017) Prawo do informacji publicznej a ochrona danych osobowych w polskim systemie prawnym. In: Kitler W, Taczowska-Olszewska J (eds) Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne, Warsaw
- Taczowska-Olszewska J (2019) Dane osobowe w cyberprzestrzeni. In: Taczowska-Olszewska J, Chałubińska-Jentkiewicz K, Nowikowska M (eds) Retencja, migracja i przepływ danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa, Warsaw
- Taczowska-Olszewska J, Nowikowska M (2019) Prawo do informacji publicznej, Informacje niejawne. Ochrona danych osobowych, Warsaw

Monika Nowikowska PhD, adjunct at the Department of Cybersecurity Law and New Technologies of the Institute of Law of the War Studies University. Author of several dozen scientific publications in the field of intellectual property law and the media. He also specializes in issues related to security, such as audit, protection of classified information and personal data. Internal auditor, legal advisor.

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

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