EJSM Vol. 27/2, 3/2018, ISSN: 2450-8535 | www.wnus.edu.pl/ejsm | DOI: 10.18276/ejsm.2018.27/2-08 | 65–71

THE SECURITY OF PERSONAL DATA PROTECTION IN THE POLISH INFORMATION SOCIETY – SELECTED ASPECTS

Agnieszka Budziewicz-Guźlecka

University of Szczecin, Faculty of Management and Economics of Services, POLAND
e-mail: agnieszka.budziewicz@wzieu.pl

RECEIVED 18 January 2018
ACCEPTED 2 September 2018

JEL CLASSIFICATION A14, F10, O32

KEYWORDS information society, data security, information, RODO

ABSTRACT

The European Parliament and Council Regulation (EU) 2016/679 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 will come in force from 25 May 2018. The Regulation provides for many changes that must be implemented by the Polish legislator. It also sets out new responsibilities and tasks for data administrators. The GDPR (RODO) introduces greater protection of personal data than hitherto. The aim of the article is to present the most important changes resulting from the implementation of the GDPR. Increasing the knowledge about the protection of personal data is the responsibility of every entity, entrepreneur, manager and employee. The following research methods were used in the article: method of critical analysis of literature, logical inference method, method of analysis and synthesis. First, the article addressed the essence of data and information security. Next, it focused on the protection of personal data. Finally, changes in data protection were presented in connection with the new legal solution from the point of view of a member of society as well as of the organization.

Introduction

The European Parliament and Council Regulation (EU) 2016/679 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 will come in force from 25 May 2018. The Regulation provides for many changes that must be implemented by the Polish legislator. It also sets out new responsibilities and tasks for data administrators. The GDPR (RODO) introduces

greater protection of personal data than hitherto. The aim of the article is to present the most important changes resulting from the implementation of the GDPR. The article presents the following research hypothesis – Increasing the knowledge about the protection of personal data is the responsibility of every entity, entrepreneur, manager and employee. First, the article addressed the essence of data and information security. Next, it focused on the protection of personal data. Finally, changes in data protection were presented in connection with the new legal solution from the point of view of a member of society as well as of the organization.

The essence of data and information security

The Internet is the driving force behind today's economy, creating opportunities and chances for business development worldwide. However, the importance of information security should be pointed out (Drab-Kurowska, 2013, p. 302). The importance of information security issues was already noted in 1999 by Sienkiewicz and Goban-Klas, who analyzed the scale of dangers related to the development of information technologies, telecommunications networks and digitization of life, relating to the conduct of information policy, information security management and protection of information resources strategic for the individual and the nation (Sienkiewicz, 1999).

Proper identification of threats is now the basis for determining the proper strategy not only of survival but also of the development of each organizational entity (Polończyk, 2017, p. 81). Information security is often defined as a state free of threats.

In another approach, it refers to all kinds of efforts that serve to protect the information possessed, important in the context of security, and thus affecting the smooth functioning of state structures and society. It also serves to provide information advantage by gaining new or more current data and by disinformation actions against possible opponents, which may be other entities (Madej, 2009, p. 1819). The broad definition of information security emphasizes the condition of internal and external circumstances that allow the state to have an information society that will survive and freely develop (Nowak, Nowak, 2011, p. 103). Information security is a broad concept, as it concerns not only the security of information itself in every form (including that which the entity itself is unaware of), but also the security of the systems in which it is generated, processed, stored and transmitted, the environment in which these systems operate, and the staff that uses these systems. It follows from this that information security includes the concept of security of information (data), which means protection of all forms of data exchange, storage and processing (Janczak, Nowak, 2013, p. 20). Besides, even the very concept of information is very broad and variously defined. More on this topic is written by M. Czaplewski (2012, p. 55).

When defining information security, a number of aspects are pointed out, above all confidentiality, authenticity, availability, integrity, accountability and reliability. Whitman and Mottord also point to privacy as one of the aspects that need protection due to the relationship with a given person (Whitman, Mottord, 2008). Personal information is information assets that have their own sensitivity, which is defined as the measure of importance assigned to the information by its author or trustee in order to indicate the need to protect it (Białas, 2007, p. 37).

Information security is the preservation of confidentiality, integrity and availability of information. According to the definitions in ISO/IEC 27000: 2014, confidentiality is the property meaning that information is not shared or disclosed to unauthorized persons, objects or processes; integrity is a property that ensures the accuracy and completeness of assets, and availability is the property of being available and usable at the request of an authorized entity (PN-ISO/IEC 27000: 2014).

Personal data protection

The European Union lacked transparency and certainty about the application of the law in this area. There was a need to create provisions guaranteeing an equivalent level of protection of personal data throughout the Union. If we add to this the question of the free flow of work, people or information (including personal data) that takes place in the EU, the need to regulate the protection of personal data has become evident.

In the Polish legal system, this issue is regulated by the Act of 29 August 1997 on the protection of personal data (Journal of Laws of 2016, item 922).

From 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council (EU) 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 the repeal of Directive 95/46 / EC will come in force. (Journal of Laws 119, 4 May 2016). The Member States have the task in the abovementioned time to adapt their national provisions[1] to this legal act.

The intention of the representatives of the European Union was to modernize the regulations on the protection of personal data, which has been in force since 1995 and which in the era of progressing digitalization have less and less practical application. At the same time, the new law was created to be "technologically neutral", meaning up to date regardless of the development of technology or the emergence of new telecommunications products. This is due to the current dynamic development of the technique of information transmission technology.

This neutrality (or universality, as this attribute can be called) means that the EU regulation does not contain any specific guidelines on how to protect personal data. Because it is not enough that these guidelines would have to be different for each industry, it could soon be necessary to adapt them again to changing conditions.

Changes in data protection due to a new legal solution

Basic changes related to data protection are presented in Figure 1.

The obligation to apply the provisions on the protection of personal data will be required already at the design or page creation stage[2]. Apart from that, all entities will be able to collect personal data that is necessary for processing of an order, use of the website, service or application. This means that entities will not have the right to require any information that is not directly related to a given process.

Information obligation means that entities now are required to inform individuals that their personal data is being processed. In the newsletter communication, it will be necessary to provide full information about the very fact of data processing, the purpose of the processing and the data of the administrator, as well as about the recipients' rights. The companies will also be obliged to inform about the safeguards applied to personal data.

---

[1] The laws related to information security in Poland include Act of 25 February 2016 on the re-use of public sector information Dz.U. 2016, item 352; Act of 6 September 2001 on access to public information, Dz.U. 2016, item 1764; Act of 30 August 2002 on proceedings before administrative courts. Dz.U. 2012, poz. 270; Act of 17 February 2005 on computerization of the activities of entities performing public tasks. Dz.U. 2014, poz. 1114 – amended in the scope of cooperation with the ePUAP system and interpretation of some activities in the re-use of public sector information published in Dz.U. 2016. item 352 and Dz.U. 2016, item1579; Act of 7 November 2014 on facilitating the performance of business activities Dz.U. 2014, item 1662; The Act of 18 July 2002 on the provision of electronic services, Dz.U. 2013, item 1422 Dz.U.2015, item 1844, Dz.U. 2016, item 147 and Dz.U. 2016, item 615; The Act of 16 July 2004 Telecommunications Law, Dz.U. 2016, item 1489.

[2] This also applies to sites that are in beta phase, or not yet published.

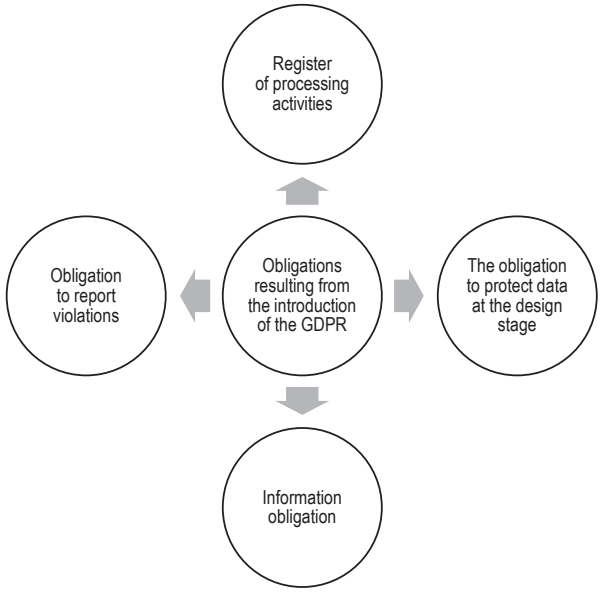

Figure 1. Basic changes related to data protection

Source: own study.

Under the new regulation, in the event of cybercrime or another breach of personal data protection, entities will be obliged as soon as possible, but not later than within 72 hours of becoming aware of a breach of security, to inform the appropriate data protection authority. The result is that entities will have to admit to violating regulations introduced for personal data.

One of the most important changes introduced by the GDPR is the register of processing activities; this document includes the purposes for which personal data are processed and information about persons who are the administrators of such data. The document is supposed to bring about transparency because it will precisely define: what data it is, the way in which data is protected, who administers the data and has access to it. There is no requirement as to the form of the document (it can even be a plain text document or an .xlsx file). It is important that the above information is clearly derived from the document. Each of the persons, whose data is processed, can report to the organization asking for information about what his/her data is processed, and thus has the right to change or delete it. Then such a document may turn out to be crucial.

The project provides for the establishment of an independent body dealing with matters of personal data protection – the President of the Office for Personal Data Protection (PUODO). He will replace the Inspector General for Personal Data Protection. The advisory body for the President of the Office will be the Council for the Protection of Personal Data established by him.

Changes in data protection due to a new legal solution from the organization's point of view

All entities operating on the market will be required to implement a completely new system ensuring compliance with data protection principles and covering technical and organizational as well as legal issues. The application

of, among others, privacy protection principles will be required at the very beginning of the design phase of specific technological solutions as well as taking into account how data processing may affect customer privacy, especially in cases involving customer profiling or monitoring of geolocation data collected in public places. The general scheme for implementing the data security system is shown in Figure 2.

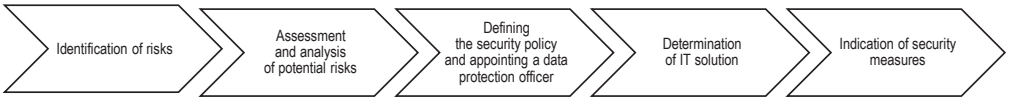

Figure 2. Basic elements related to the introduction of data security

Source: own study.

The implementation of data security in an entity must begin with an assessment and analysis of the risks that exist or may occur in an entity. Only conducting of such an analysis will allow determining what type of IT solution can meet the requirements. When making this selection, entities will be required, at the request of the institutions and offices supervising the performance of the GDPR, to demonstrate that the solution has been selected in terms of compliance with the data processing principles. The next step is to check the security policy and IT system management instructions and update them. Meanwhile, entrepreneurs will have to indicate security measures and procedures for secure data processing, including actions that must be taken in the event of a specific threat, for example, the so-called data leak.

Changes in data protection due to a new legal solution from the point of view of a member of society

The new rights of persons whose data will be processed are presented in Figure 3.

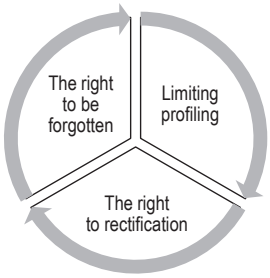

Figure 3. New rights resulting from the GDPR Regulation

Source: own study.

The right to be forgotten was actually in force, but it was not used, due to the imprecise wording. The GDRP introduces the right to be forgotten as an explicitly written provision for every person whose data is processed.

Article 17 gives the person, to whom the data relates the right to request immediate deletion of his personal data, including in a situation where:

- personal data are no longer necessary for the purposes, for which they were collected or otherwise processed,
- the person to whom the data relates has withdrawn the consent on which the processing is based and there is no other legal ground for processing,
- the person to whom the data relates objects to the processing and there are no overriding, legitimate grounds for processing,
- personal data were processed unlawfully,
- personal data has been collected in connection with offering services of the information society.

Limitation of profiling[3] are the rules that lead to profiling constraints, including the obligation to obtain consent for profiling before the start of data collection, a strict obligation to inform about profiling, and the need to accept a lack of consent for profiling.

The right to rectify is a provision in the GDPR, which gives every person the opportunity to view their personal data. Everyone will be able to not only see at any time what personal data are processed by entities but also will be able to correct it, that is, withdraw, change or limit to a smaller amount of data.

Conclusions

When comparing the costs and benefits of efficiency, security, accessibility and management of the IT infrastructure, a decision should be made on optimally selected measures that will be part of the personal data processing system. It should be decided whether it will be created within its own premises and technical resources, or whether external entities should be used (Kołodziej 2017). Solutions related to the electronic flow of documents must be observed in order to assess the risk and continuously increase the level of security. This means that the fee for these services will not be one-off, but fixed – and incurred periodically.

Ensuring an adequate level of security of personal data processing that guarantees data consistency and limiting the possibility of losing certain data, as well as deletion, modification or confidentiality is directly related to the implemented security policy, including organizational and program security, which inevitably involves incurring financial outlay by all entities operating on the market.

References

Białas, A. (2007). *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*. Warszawa: WNT.

Czaplewski, M. (2012). Informacja – jej podstawowe koncepcje i komponenty. *Zeszyty Naukowe Uniwersytetu Szczecińskiego*, *746. Ekonomiczne Problemy Usług*, *101*, 55–68.

Drab-Kurowska, A. (2013). The role of social media in economy. *Zeszyty Naukowe Uniwersytetu Szczecińskiego*, *763. Ekonomiczne Problemy Usług*, 297–304.

Janczak, J., Nowak, A. (2013). Bezpieczeństwo informacyjne. Wybrane problemy. Warszawa: Wydawnictwo AON.

Kołodziej, M. (2017). Własna serwerownia, kolokacja czy hosting? *ABIExpert*, *3* (4), 33–35.

[3] Profiling is drawing conclusions about the features of a person whose personal data is collected and processed based on the other features of the same person.

Madej, M. (2009). Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego. In: M. Madej, M. Terlikowski (eds.), *Bezpieczeństwo teleinformatyczne państwa* (pp. 17–40). Warszawa: Wydawnictwo PISM.

Mottord, H.J., Whitman, M.E. (2008). *Management of Information Security*. Boston: Thomson,.

Nowak, E., Nowak, M. (2011). *Zarys teorii bezpieczeństwa narodowego*. Warszawa: Difin.

Polończyk, A (2017). Zagrożenia bezpieczeństwa informacyjnego na przykładzie Krajowej Mapy Zagrożeń Bezpieczeństwa. In: H. Batorowska, E. Musiał (eds.), *Bezpieczeństwo informacyjne w dyskursie naukowym*. Kraków Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie. Instytut Bezpieczeństwa i Edukacji Obywatelskiej. Katedra Kultury Informacyjnej i Zarządzania Informacją.

PN-ISO/IEC 27000:2014 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia.

Sienkiewicz, P., Goban-Klas, T. (1999). *Społeczeństwo informacyjne. Szanse – zagrożenia – wyzwania*. Kraków: Wydawnictwo Fundacji Postępu Telekomunikacji.

Cite this article as: Budziewicz-Guźlecka, A. (2018). The security of personal data protection in the Polish information society – selected aspects. *European Journal of Service Management*, *3* (27/2), 65–71. DOI: 10.18276/ejsm.2018.27/2-08.