Magdalena Kędzior

WSPiA University of Rzeszow

Personal data security – challenges, current state and outlook[1]

ABSTRACT

Due to the rapid development of the information society recent years have brought new technological challenges and related threats to the security of personal data. The answer to these phenomena was the legal regulation of the means, rules and institutions that guard the security of personal data.

The purpose of this paper is to analyze the current legal framework applicable at national level in Poland, to assess legislative changes at the European level, and to take position on their adequacy. The study is limited to the issues of securing personal data laid down in Chapter V of the Polish Act of 29 August 1997 on the Protection of Personal Data and to the relevant provisions of the 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, included in section II (articles 32–34). The paper uses mainly the method of legal-dogmatic analysis and the comparative method.

Keywords: data security, guarantees of personal data security, General Regulation on Personal Data

1. Introduction

The process of creating a legal framework for the protection of personal data is dynamic, which is clearly illustrated by the already completed

[1] Pursuant to the applicable legislation as of June 1, 2017.

legislative work on the new EU Regulation on the protection of natural persons with regard to the processing of personal data[2] and on the new Polish Act on the Protection of Personal Data.[3] Intensive legislative work is a response to the present day requirements. A rapid technological development in the past decades has brought new challenges in the field of personal data protection both in the public and private sectors. The scale of data exchange and data collection has grown tremendously. It is assumed that technology has completely changed both the economy and social life. New threats to the privacy of individuals have emerged such as profiling, the violation of personal rights, e.g. image or identity theft and phishing, harassment, defamation or cyber terrorism (Brzozowska, 2012, p. 95; Ciechomska, 2017, p. 37). It should be taken under consideration that challenges related to the development of new technologies and possible interference with the right to privacy – such as profiling, geolocation or cloud data processing – allow highly undesirable manipulation in the event of improper data protection.

2. Protection of personal data as an instrument to counteract breaches of privacy

Data protection is legally guaranteed at both national and transnational levels. The Constitution of the Republic of Poland in Art. 47 grants citizens the right to privacy, and Art. 51 guarantees every person the right to the protection of information concerning that person. At European level Articles 7 and 8 of the Charter of Fundamental Rights of the European Union recognize respect for private life and the protection of personal data as related fundamental rights. The Polish definition of personal data, based on the assumptions of Directive 95/46, is extremely broad because, in the light of Art. 6 of the Act on the Protection of Personal Data, personal data shall be deemed to contain all information relating to an identified or

[2] 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 (General Data Protection Regulation). Official Journal of the European Union, L 119, 4 May 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC, 5.05.2017.

[3] https://mc.gov.pl/aktualnosci/projekt-ustawy-o-ochronie-danych-osobowych, 6.05.2017.

identifiable natural person. These include, in particular, information that allows direct identification such as: name, address, PESEL identification number or DNA code, as well as information that indirectly determines the person's identity: in particular one or several specific factors determining his or her physical, physiological, mental, economic, cultural or social features (Article 6 (2) of the Act on the Protection of Personal Data).[4] Other information such as psychophysical characteristics, state of health, likes, interests, participation in social life (events, events, use of a physician named by name, acquired qualities, skills, etc.) may also be included. The subject of personal data is every human being from birth to death (Hoc and Szewc, 2014, p. 4). According to the judgment of the Provincial Administrative Court in Warsaw of 9 July 2014 also a video monitoring system, due to the fact that it allows identification of persons, is a collection of personal data and subject to the provisions of the Act on the Protection of Personal Data.[5]

Similarly, giving a phone number and an e-mail address is giving personal information within the meaning of Art. 6 Paragraph 1–3 of the Act on the Protection of Personal Data because these data allow to identify a specific person quickly.[6] In other words, the data subject does not need to be indicated explicitly, it is enough to ensure traceability. This was ruled by the Supreme Administrative Court in Warsaw in the judgment dated of 19 May 2011, which stated that if the IP number indirectly allows the identification of a particular individual, it should be regarded as personal data within the meaning of Art. 6 Paragraph 1 and 2 of the Act on the Protection of Personal Data of 1997. A different interpretation would be contrary to the constitutional norms contained in Art. 30 and 47 of the Constitution of the Republic of Poland.[7]

[4] Such a broad legal definition of personal data makes the status of personal data potentially available to any information relating to an individual. Personal information may take different forms. In addition to traditional data, these may include photos, videos, recorded voices, so-called biometric data, etc. regardless of the manner and extent of their acquisition and disclosure (Barta/Litwiński, Ustawa o ochronie danych osobowych, Komentarz, 3. Ed., Warszawa 2015, art. 6, p. 77, subpara. 5).

[5] II SA/Wa 2393/13 judgment of the Provincial Administrative Court in Warsaw of 9 July 2014.

[6] II SA/Kr 682/13 judgment of the Provincial Administrative Court in Cracow of 11 October 2013.

[7] SK 1079/10 judgment of the Supreme Administrative Court in Warsaw of 19 May 2011.

Pieces of information that characterize a person but do not allow identification are not considered to be personal data. Anonymous information is not regarded as personal information (Jarzęcka-Siwik and Skwarka, 2012, p. 798). Sensitive data require a special protection from the point of view of the right to privacy. In accordance with the provisions of the Act on the Protection of Personal Data these include information that reveals racial or ethnic origin, political views, religious or philosophical beliefs, religious affiliation, party or trade union membership, and health information, genetic code, addictions, or sexual life. This group of data is subject to more intensive protection, inter alia due to the fact that Art. 49 of the Act on the Protection of Personal Data provides for stricter criminal liability for their illegal processing. Another category of sensitive data is data on convictions, punishments and penalty notices, as well as information on judgments given in court or administrative proceedings.

In the era of technological development and modern economy, data security is therefore designed to protect the privacy of natural persons, on the one hand, and on the other hand to increase the confidence of consumers and entrepreneurs in the information society. The European Commission's priority is to ensure that personal data are effectively protected, regardless of the technology used to process the data (Szpor, 2013, p. 56). Finally, the complexity of the issues related to the protection of personal data and the conflict of interests arising in this context should be emphasized. While companies in the computer technology and telecommunications industries, in an effort to maintain good customer relationships, have begun to take measures aimed at encrypting mobile services to prevent unauthorized access to data, it is still an ongoing problem that a large amount of easily accessible data on citizens are collected and their content is surveilled by government agencies or eGovernment services.[8]

[8] Institute for Human Rights and Busienss, Top 10 List of Business and Human Rights Issues for 2015, http://www.ihrb.org/top10/2015.html (20.05.2017).

3. Obligation to protect personal data under the Act of 29 August 1997 on the Protection of Personal Data

According to the definition given by Drozd, data security is a set of legal norms which consist of obligations to protect personal data against unauthorized processing (Drozd, 2008, 14). Among the obligations of securing personal data there are technical and organizational measures, some authors also distinguish physical measures (Barta and Litwiński, 2015, p. 380). In this context, it is crucial to identify the entity responsible for securing the processing of personal data. It can be assumed that the scope of obligations concerning the personal data protection has gradually expanded. According to the assumptions of the Act on the Protection of Personal Data (Article 31) data processing security is essentially in the hands of a data controller who processes or outsources data processing on a contractual basis. Barta and Litwiński note that since 2004 there has been a provision in Polish legislation that equates the responsibility for the processing of data of the processor and the controller, but such an approach conflicts with the fundamental responsibility of the controller for complying with the provisions of the Act on the Protection of Personal Data (Barta and Litwiński, 2015, p. 331-332). In this respect, it can be assumed that the division of responsibilities of the processor and the controller for the security of data processing is unclear. According to the content of Art. 31 Paragraph 4 the responsibility for complying with the provisions of the Act rests with the data controller and the data processor is liable for processing the data contrary to the contract of entrustment. Certain data protection responsibilities may also be assigned to a data protection administrator, although in principle he performs control functions and not the managerial ones (Drozd, 2008, p. 26).

It should be emphasized that the legislator, in Art. 52 of the Act on the Protection of Personal Data, provided for fines, restriction of liberty or deprivation of liberty for the violation of the obligation to properly secure the data. It is assumed that such an offense can be committed by any person who manages, i.e., administers personal data in the course

of processing the data.[9] The Act does not define the concept of data administrator. It is therefore assumed that this is anyone managing the data, although it does not have to be a data controller. The administrator's status is governed by the internal regulations of the data controller and these regulations assign data protection responsibilities to specific individuals. It is assumed that only after analyzing such acts as security policy, organizational regulations, contracts of employment, scope of activity, it is possible to determine who, in case of a given employer, is the data administrator responsible for the protection of personal data.

On the basis of the provisions of Chapter V of the Act on the Protection of Personal Data there are several responsibilities for the data controller (processor) that aim at protecting personal data. From Art. 36 Paragraph 1 of the Act on the Protection of Personal Data follows the principle of proportionality of the data protection measures that are applied to the threats and the categories of data processed. The obligation of adequate protection is linked to the principle of proportionality. The duties of the data controller – especially ensuring security of data so that they are not made available to unauthorized persons, or removed by unauthorized persons, damaged, destroyed, altered, lost, processed in violation of the Act – are closely related to the category of tasks entrusted to him. It should be remembered that these obligations also apply to a person processing the data on the basis of a commission from the controller. These obligations relate to data processed in a traditional way and to those processed in information systems. Based on the assumptions of Art. 17 of Directive 95/46, the Act on the Protection of Personal Data stipulates that the controller and data processor respectively should implement technical and organizational measures ensuring a level of security appropriate to the risks represented by the processing of data and the nature of personal data processed. The technical and organizational measures include physical security, video surveillance, alarm systems, access control – access protection, identification cards, biometric identification – and IT security such as IDs and passwords subject to periodic changes, firewall and encryption (Krzysztofek, 2014, p. 185).

[9] As stated by the Supreme Court in the decision of 11 December 2000 the criminal liability of a subject who processes personal data is however not a data administrator are considered when his behavior – recognized as punishable by the law – results from the data processing entrusted to him. II KKN 438/00, OSNKW 2001 / 3-4 / 33.

In this context, in the Ordinance of the Ministry of the Interior and Administration of 29 April 2004 on the documentation of the processing of personal data and the technical and organizational conditions that should be met by the equipment and information systems used to process personal data, three levels of protection of personal data are generally enumerated and appropriate protection measures are assigned to them. The obligation to secure data, as Barta and Litwiński point out, is dynamic, as the controller should analyze and evaluate the changing security risks and appropriately select data protection measures (Barta and Litwiński, 2015, p. 382). Doctrine and case-law also assume that the controller is not obliged to use all possible data protection measures, but only those that are necessary, taking into account the level of risk and financial outlay.[10]

Additional requirements for data processing security named in doctrine also include other categories of obligations that complement security measures of data processing. Under Article 36 Paragraph 2 of the Act on the Protection of Personal Data it is a responsibility of the controller to maintain adequate documentation describing the way in which the data are processed and the technical and organizational measures that ensure their control. In turn, Article 39 Paragraph 1 provides for the obligation to keep records of persons authorized to process the data, and those who have been authorized to process the data are obliged to keep secrecy about the data and the means of securing the data.

Another obligation of the data controller is, in accordance with Art. 36 of the Act on the Protection of Personal Data, the obligation to designate a data protection administrator (hereinafter referred to as DPA) (*pol. ABI – administrator bezpieczeństwa informacji*). Although this obligation existed even before the entry into force on 1 January 2015 of the amendment of the Act on the Protection of Personal Data. (Formerly Article 36 (3)), it is emphasized in the doctrine that the DPA, previously provided for in the Act, did not meet the conditions of the so-called data protection officials provided for by EU law. There was no sufficient statutory basis for his independence, his scope of competence was extremely limited and he was not granted a so-called simplified registration procedure (Fajgielski, 2014, p. 2014, 39–40).

[10] The case-law assumes that no organizational and financial nature can be treated as a basis for the unlawful processing of personal data by banks. Judgment of the Supreme Administrative Court of 4 March 2002, II SA3144 / 01.

On the basis of the current provisions of the Act on the Protection of Personal Data (Articles 36a-c) DPA's subjective requirements have been determined, his position in the organizational structure of the data controller has been specified, guaranteeing him a certain degree of independence, and relatively broadly clarifying the scope of his responsibilities. These include, in particular, compliance with the provisions on the protection of personal data and the keeping of records of data files processed by the controller. The appointment of a DPA should be reported within 30 days of the appointment to the Inspector General for Personal Data (IGPD), who keeps an open record of all appointed DPAs. From a practical point of view, the provisions of Art. 36 of the Act on the Protection of Personal Data are of importance as according to these provisions IGPD may refer to a DPA, who has been entered in the registry, to control the lawfulness of the processing of personal data by the controller who appointed the DPA (Barta and Litwinski, 2015, p. 402). Where a controller appoints and registers a DPA, he or she is exempted from the obligation to register personal data files with IGPD, but this exclusion does not apply to sensitive data sets. It shall be noted that if a DPA is not appointed, the data controller performs DPA`s tasks on his own (Article 36b).

The security of data processing is also indirectly guaranteed in Art. 37 and 38 of the Act on the Protection of Personal Data by the duties of a controller to allow the processing of information in the IT system and beyond only by authorized persons and to ensure control over the data flows, i.e. to ensure what personal data, when and by whom were entered, and what data, when and to whom were transferred.

4. Security of personal data in the General Data Protection Regulation of the European Parliament and of the Council (EU) 2016/679

The issue of security of personal data is covered in Section II (Articles 32 to 34) of the Regulation 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.[11]

[11] According to art. 99 sec. 2 it is envisaged that the regulation will become effective from 25 May 2018.

With regard to the scope of data security obligations, the EU legislature assumed that if the processing operation was carried out on behalf of the controller, the controller selects a processor that guarantees the implementation of appropriate technical and organizational measures and procedures. This is probably motivated by the need to ensure the lawful nature of the processing and guarantee legal protection of data subjects.

Following the so-called principle of adequacy, it was stipulated that the controller and the processor implement data protection authorities technical and organizational measures to ensure the level of security appropriate to the processing risks and the nature of the personal data to be protected, taking into account the latest technological developments and the costs of their implementation. Compliance with data protection obligations can be demonstrated, inter alia, by applying an approved Code of Conduct referred to in Art. 40 or an approved certification mechanism referred to in Art. 42 of the Regulation.

In the light of Art. 32 of the Regulation, the controller and the processor are therefore required to put in place appropriate measures to ensure the security of processing by extending the obligation provided for in Article 17 Paragraph 1 of the Directive 95/46 / EC on processors, regardless of the terms and conditions of the contract concluded with the controller. Literal interpretation of Art. 32 of the Regulation indicates that the responsibility of the controller and the data processor has been equalized.

Articles 33 and 34 of the Regulation provide for a new obligation of notification of a personal data breach, based on the obligation to give notice of personal data breaches as specified in Article 4 Paragraph 3 of the Directive 2002/58/EC on privacy and electronic communications.[12] The aim of the duty is to strengthen the rights of data subjects and enhance the supervisory powers of data protection authorities. At present, the supervisory authorities and individuals are not always informed of such breaches. (Szpor, 2013, p. 60). It should be expected that the competent national authorities will have full and accurate data on security breaches when such an obligation is introduced. Data controllers will be required to keep records of personal data breaches

[12] Official Journal of the E of 2 November 1995, L 281/31.

in order to enable the competent national authorities to analyze and evaluate, and consequently to eliminate similar cases in the future. According to Article 33 Paragraph 1 of the Regulation in case of a personal data breach, the controller shall report such a breach to the supervisory authority without undue delay and if possible no later than 72 hours after the breach is found, unless the breach is unlikely to result in the risk of a breach of freedom of natural persons. In turn, the processor warns and informs the controller immediately after the personal data breach has been established. Under Article 33 Paragraph 5, the controller shall prepare a record of any personal data breaches for the supervisory authority, including the circumstances of the breach, its effects and the remedial action taken.

Pursuant to Article 34 (1) of the Regulation, the natural persons who might be adversely affected by a personal data breach shall be informed forthwith so as to enable them to take the necessary precautions. A data breach may result in, inter alia, identity theft, damaging reputation, or identity fraud. Notification of a natural person should clearly and simply describe the nature of a personal data breach and include information on the measures taken to remedy the breach, as well as recommendations for the individual concerned.

Importantly, Article 35 of the Regulation provides for the so-called principle of data protection impact assessment. It signifies that if processing operations pose a particular risk to the rights and freedoms of data subjects, the controller or the processor shall conduct an impact assessment of the anticipated processing operations on the protection of personal data within the scope of the rights and freedoms of the data subject. The Regulation therefore provides for reacting to the changing environment in the processing of personal data and technology, in particular in case of the growing scale of data processing on the Internet. The provisions of the Regulation do not obligate to implement all possible security measures, regardless of the costs and capabilities of the controller in question, but it should be borne in mind that the lack of data protection possibilities cannot constitute grounds for abandoning the measures necessary to ensure security appropriate to the risks.

It should be stressed that the above provisions of the EU Regulation will apply directly to the Polish legal order (Kozik, 2017, p. 18).

5. The draft Act on the Protection of Personal Data of 28 March 2017

The draft of the new Act on the Protection of Personal Data of 28 March 2017 states that the Polish legislator has decided that the proposed new data protection Act will not repeat the provisions of the EU Regulation, but will only regulate and clarify issues not addressed at the EU level.[13] The following issues, inter alia are covered: the issue of accreditation and certification of data processors, regulation of details of proceedings concerning cases of personal data breaches and control proceedings. Also the EU regulations on the institution of the data protection officer have been detailed. In the context of data security a new legislative proposal at national level is obligating the President of the Office for Data Protection to issue non-binding good practices on data security safeguards that may be followed. The purpose of good practice recommendations is to support controllers and processors in assessing what technical and organizational measures can be implemented to adequately address the risk of data processing in a particular case. This will ensure a greater sense of legal certainty, thereby increasing the degree of compliance by administrators and processors with the provisions of Regulation 2016/679.

6. Summary

Technological progress and globalization have radically altered the way data are collected, including access to and use of data. These phenomena are accompanied by the ever-increasing danger of breaches of the right to privacy. The threat to the security of personal data can lead to social harm and economic loss. It can be prevented by rational norms aimed at the security of personal data.

The issue of securing personal data had already been regulated by the Polish legislation under the Personal Data Protection Act of 29 August 1997, which implemented Directive 45/96 EC. The Act had imposed a number of obligations on the data processors in relation with ensuring security guarantees. In this area, inter alia, the following obligations

[13] https://mc.gov.pl/aktualnosci/projekt-ustawy-o-ochronie-danych-osobowych 06.05.2017.

were introduced: an obligation of adequate protection, maintaining appropriate records, keeping records of persons authorized to process data, and finally an obligation to establish a DPA. Legal solutions, adopted as of 1 January 2015, relating to the DPA's competences and his place in the administrative structure of the controller concerned were intended to prepare the data controllers for the regulations envisaged in the EU Regulation that was being drafted at that time. They assume, inter alia, the functioning of independent Data Protection Officers, who cooperate with the data protection authority and with the data controller in the process of guaranteeing data security. A certain flaw in the national Act is that, according to the doctrine, there is an unclear separation of responsibility for improper data protection between the controller and the data processor. In view of the above, the EU Regulation on data protection analyzed herein, which stipulates that the processor is liable for data protection to the same extent as the data controller, should be assessed positively.

According to the requirements of the present day, there is a tendency in EU law – including the content of the mentioned Regulation – to strengthen the rights of citizens, including the guarantee of the security of personal data processing, by extending the controllers' information obligations regarding data security breaches. These obligations are to be exercised in order to inform the supervisory authorities as well as the data subject. The adopted legislative approach should be considered accurate from the point of view of data security and from the perspective of human rights protection. It can therefore be assumed that the reform of data protection law aims to ensure the protection of personal data in the EU, while at the same time increasing the users' ability to control their own data.

Ensuring data security as an element of protecting the privacy of individuals remains one of the challenges faced by the modern information society. It may be assumed that along with technological changes we will be faced with a further search for a balance between business or public administration interests and the protection of personal data of individuals, while the shape of the regulation on security of personal data in Poland will be mainly determined by the final scope of the new Act on protection of personal data.

Bibliography

Barta P./Litwiński P. (2015). *Ustawa o ochronie danych osobowych*. Komentarz, 3. Ed., Warszawa.

Brzozowska M. (2012). *Ochrona danych osobowych w sieci*, Presscom sp. z o. o., Wrocław.

Ciechomska M. (2017). *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych*, „Europejski Przegląd Sądowy" 2017/5.

Drozd A. (2008). *Zabezpieczanie danych osobowych*, Presscom sp. z o. o., Wrocław.

Fajgielski P. (2014). *Administrator bezpieczeństwa informacji – geneza, stan obecny i perspektywy zmian*, Dodatek do MoP 9/2014.

Hoc S., Szewc T. (2014). *Ochrona danych osobowych i informacji niejawnych*, 2. Ed., C.H. Beck, Warszawa.

Jarzęcka-Siwik E., Skwarka B. (2012). *Przetwarzanie danych osobowych – wybrane problemy postępowania kontrolnego NIK*, „Kontrola Państwowa" 2012/6.

Kozik P. (2017). *Zakres swobody regulacyjnej państw członkowskich przy wdrażaniu ogólnego rozporządzenia o ochronie danych osobowych do prawa krajowego*, „Europejski Przegląd Sądowy" 2017/5.

Krzysztofek M. (2014). *Ochrona danych osobowych w Unii Europejskiej*, Lex a Wolters Kluwer business, Warszawa.

Szpor G. (2013). *Kierunki zmian w ustawodawstwie dotyczącym ochrony danych osobowych*, (in:) *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, Mednis A. (ed.), Warszawa.

Legal sources

Act of 29 August 1997 on the protection of personal data. Official Journal of 1997 No. 133, pos. 883.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995.

Draft Act on the Protection of Personal Data of 28 March 2017, (https://mc.gov.pl/aktualnosci/projekt-ustawy-o-ochronie-danych-osobowych), 15.05.2017.

Ordinance of the Ministry of Interior and Administration of 29 April 2004 on the processing of personal data and the technical and organizational conditions

which should be met by the equipment and information systems used to process personal data. Official Journal No 200, pos. 1024.

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 (General Data Protection Regulation), Official Journal L 119/1.

Jurisprudence

Judgment of the Provincial Administrative Court in Cracow of 11 October 2013, II SA/Kr 682/13

Judgment of the Provincial Administrative Court in Warsaw of 9 July 2014, II SA/Wa 2393/13

Judgment of the Supreme Administrative Court in Warsaw of 11th December 2000, II KKN 438/00, OSNKW 2001/3-4 / 33

Judgment of the Supreme Administrative Court in Warsaw of 19 May 2011, SK 1079/10

Judgment of the Supreme Administrative Court of 4th March 2002, II SA3144 /01