Biuletyn Stowarzyszenia Absolwentów i Przyjaciół Wydziału Prawa Katolickiego
Uniwersytetu Lubelskiego t. XVI, 18 (1) 2021, s. 205-222
https://doi.org/10.32084/sawp.2021.16.1-12

Anna Pawlak

STANDARDS OF PERSONAL DATA PROTECTION IN CENTRAL AND EASTERN EUROPEAN COUNTRIES

Introduction

The beginnings of data protection can be found in one aspect of the right to privacy. The right to privacy is a much older concept than granting a person the right to data protection. However, the right to privacy results from the wider value of human freedom and autonomy. As a social being, man, in order to develop harmoniously, requires interaction with the society to which he belongs. These interactions impose many limitations on human autonomy, both natural (moral, custom, religious, etc.) and normative. Therefore, we allow a state organization, as well as other people, to enter the sphere of our freedoms in order to reap tangible benefits (such as security, order, harmony, predictability of other people's behavior, self-development, wealth, fame). With regard to personal data, we provide our information on a daily basis for the purpose of executing various types of agreements, but we also provide a lot of information about ourselves with incredible easiness, just to be noticed by other people. With the development of technology, information society – our freedom, our privacy has been shrinking at an unprecedented rate. In the age of social media, the relationship between two aspects of humanity is disrupted – the autonomy of being an individual and the individual being a part of larger community. Man as an individual is worth less and less, and the most important is to appear in a larger group and applaud the crowds. The fear of social rejection causes the increasingly intimate information to be passed on to a wider audience. The right to be left alone ceases to exist, in favour of the right not to be rejected by society. What is worse, a person starts to be worth as much as his personal data is worth. Intangible goods, such as information, are often worth more than material goods. In the information

Dr. Anna Pawlak, Institute of Legal Sciences, University of Economics and Human Sciences in Warsaw; correspondence address: ul. Okopowa 59, 01-043 Warszawa, Poland; e-mail: a.pawlak@vizja.pl; https://orcid.org/0000-0001-6112-8743

society – information has become a key element of socio-economic activity and change, and richly developed means of communication and information processing are the basis for creating most of the national income and provide livelihoods for many people [Krzysztofek and Szczepański 2002, 170]. All this makes the autonomy of human person and the protection of personal data one of the most important human freedoms, which today should be subject to special protection.

The paper presents an evolution in the approach to the protection of personal data that has taken place in recent years, with a special focus on Central and Eastern European countries. These countries include very different levels of legal protection. These are both the Visegrad Group countries such as Poland, the Czech Republic, Slovakia and Hungary; the countries formed after the collapse of the Soviet Union – rich Baltic states such as Lithuania, Latvia and Estonia, as well as Ukraine and Belarus, which are struggling with many problems; and the Balkan countries – Croatia, Bosnia and Herzegovina, Serbia, Montenegro, Northern Macedonia; Albania, Bulgaria; and finally Russia, Romania and Slovenia. The legal regime for the protection of personal data in these countries is primarily determined by membership of international organizations such as the Council of Europe and the European Union, as well as the UN. The paper presents some of the most important international legal acts regulating personal data protection.

1. The right to privacy and personal data protection law

Attempts to define privacy were made as early as at the end of the 19th century. At that time, American lawyers – Warren and Brandeis, according to the individualistic concept characteristic of American legal thought, described the right to privacy as "the right to be left alone" [Warren and Brandeis 1980, 193-200]. In terms of freedom, privacy is defined as: a state in which a person makes decisions without the interference of third parties [Mielnik 1996, 29]. More specifically, privacy can be defined as: "the individual's right to live own life, arranged according to own will, with all external interference limited to the necessary minimum" [Kopff 1972, 6]. Taking into account the sociological and psychological aspect, it is indicated that the experience of privacy is a universal and culturally independent phenomenon, it is related to the concept of the individual's self-image [Rojszczak 2019,

39]. External interference limiting the individual's will is necessary to some extent, but the protection of the right to privacy should ensure that it meets the conditions of purpose and necessity.

As A. Mednis points out – in the category of the right to privacy, the so-called right to informational privacy, consisting in controlling the circulation and content of information concerning a given person, is distinguished [Mednis 1999, 167]. This information gained the term "personal data" and the right to informational privacy is nothing more than the right to protection of personal data. The right to privacy was first proclaimed in the Universal Declaration of Human Rights of 10 December 1948, which is a resolution of the United Nations General Assembly which states in Article 12 that "No one shall be subjected to arbitrary interference with his private, family, domestic or correspondence life […]." This right was also included in Article 17 of the International Covenant on Civil and Political Rights of 19 December 1966.[1] Although these acts were adopted over half a century ago, it should be noted that the Covenant of 1966 is the only international legal act binding on Belarus. Belarus does not belong to any of the regional international organizations that set standards for the protection of personal data in other countries of Central and Eastern Europe, and only membership in the UN obliges Belarus to ensure the citizens' right to privacy, including the protection of data concerning them. As it turns out – despite ratification of the ICCPR in 1973, Belarus does not meet the standards set in the Act, and the control of the Human Rights Committee in this respect shows signs of failure.

The main law regulating the issue of personal data protection in Belarus is the Law on Information, Information Systems and Data Protection of 10 November 2008. According to this law – information concerning private life and personal data belongs to the category of information the dissemination and disclosure of which is limited. The Law defines the procedure for collection, processing and storage of such information. However, nobody has the right to demand from a person to disclose information about his private life or personal data or to obtain such information in any other way against the will of the person concerned, except as provided for by the Law of Be-

[1] Journal of Laws of 1977, No. 38, item 167 [hereinafter: ICCPR].

larus. Unfortunately – there are many such exceptions and most of them are described in the Presidential Decree No. 60 of 1 February 2010.[2] In this regard, the Human Rights Committee is concerned by reports that the legislation provides for extensive powers of oversight, and the interception of all electronic communications, including through a system of operational investigative measures that allow remote access to all user communications without notification to providers, does not provide sufficient protection against arbitrary interference with the privacy of individuals.[3]

The legal regime of the Council of Europe (to which all the countries of Central and Eastern Europe belong, with the exception of the above-mentioned Belarus) proclaimed the right to privacy as early as in 1950, enshrining it in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950.[4] This Act is of particular importance due to an effective mechanism for monitoring compliance with the provisions of the Convention by Member States, in the form of being subject to the case law of the European Court of Human Rights, with its seat in Strasbourg. The Court reviews complaints concerning non-compliance with the provisions of the Convention by states – parties to the Convention. The Court derives from the right to privacy, inter alia, the right to the protection of personal data. In its judgment of 4 December 2008 in S. and Marper v. the United Kingdom (No. 30562/04 and 30566/04), the Court points out that one of the elements in respecting the right to private life may be ensuring the protection of personal data. The guarantees of their protection are to be provided by national legislation.

Although the European Court of Human Rights in its rulings focuses on the need to guarantee the right to privacy in a broad sense, it also builds certain standards for the protection of personal data, which is an aspect of "privacy." The Court addresses issues related to the protection of personal data at the vertical level (i.e. in relations between the state and the person), but it

[2] Fifth periodic report submitted by Belarus under article 40 of the Covenant pursuant to the optional reporting procedure, 30.03.2017, CCPR/C/BLR/5, http://docstore.ohchr.org/ [accessed: 14.04.2020], p. 32-33.

[3] Concluding observations on the fifth periodic report of Belarus, 22.11.2018, CCPR/CO/BLR /5, http://docstore.ohchr.org/ [accessed: 14.04.2020], p. 9.

[4] Journal of Laws of 1993, No. 61, item 284 as amended.

has no mandate to provide guidance in a horizontal space, i.e. in relations between people or business. Therefore, the European Court has expressed its opinion, among others, on the lawfulness of personal data processed by the governments of Member States and their representatives, the quality of protections provided by the national systems, or the necessity to ensure effective mechanisms of asserting own rights in case of violation of personal data by state representatives.

The right to privacy in international acts is of a vertical nature, while regulations protecting personal data set standards both vertically and horizontally. The right to the protection of personal data derives from the right to privacy, but has been given a broader scope of protection in the personal aspect. When discussing the standards of personal data protection in the countries of Central and Eastern Europe, the right to privacy proclaimed by the UN takes on a special importance, because it is the only standard that intersects with the right to personal data protection, which is currently in force in Belarus.

2. Universal standards

The universal standards setting organization is the United Nations (UN), with its seat in New York. The universality, or in other words, the universality of UN action refers to several aspects of this system: territorial, indicating that it covers practically the whole world; objective, as it takes into account all basic categories of human rights; and subjective, which means that the system covers all UN member states [Jabłoński and Jarosz-Żukowska 2004, 178]. Under the auspices of the UN, there are fragmentary regulations related to the protection of human personal data. However, they concern the protection of privacy rather than data protection in the strict meaning of the word. The United Nations with regard to the protection of personal data in the strict sense has been limited to issuing recommendations in the form of resolutions. In 1979, Resolution 34/169 called the "Code of Conduct for Law Enforcement Officials" was issued, where Article IV contains a recommendation to officials on how to deal with personal data they obtain by virtue of their functions. The data obtained in this way may be disclosed only for the purpose of performing official duties as well as for the purposes of the justice system. In 1990, the UN General Assembly adopted guidelines on the regu-

lation of computerized personal data files (Resolution 45/95). The resolution includes recommendations on the guarantees to be provided in national legislation on the computer processing of personal data. Resolution 45/95 sets out the principles (i.e. lawfulness, fairness, accuracy, purpose limitation, access by the person concerned, non-discrimination and security) that should be the basis for regulation of national laws.

The Universal Declaration on the Human Genome and Human Rights of 11 November 1997 developed by UNESCO, a specialized UN organization, is also a universal document. The Declaration lays down standards for the protection of genetic data, which in accordance with Article 7, must be kept confidential. The Declaration protects the genetic data of identifiable persons, regardless of the purpose for which the data are collected, and the restriction of confidentiality principle may only take place within the limits of established law [Kondratiewa-Bryzik and Sękowka-Kozłowka 2013, 21ff] All the countries of Central and Eastern Europe are members of UNESCO, thus this standard should be respected in this region of the world.

3. Regional standards

Data protection standards for the European region have been set by two organizations – the Council of Europe and the European Union. The Council of Europe has been at the forefront of their determination in Europe for many years. The Council of Europe has been issuing resolutions and recommendations on the protection of personal data since the seventies of the 20th century, whereas in the 1970s these were resolutions on the protection of the privacy of individuals (Resolution 22 (73) of the Committee of Ministers on the use of electronic data banks in the private sector and Resolution 29 (74) on the public sector). However, starting from 1981, the Committee of Ministers issued a number of recommendations concerning various aspects of personal data protection (such areas as: data processing in telecommunications, for payment, social security, direct marketing, research and statistics, used on the Internet, in the context of electronic data banks in the private sector, or automated medical data banks, as well as the transfer of data to third parties by public institutions and used in the police sector were taken into account). The most recent recommendation dated 2010 concerns the protection of individuals with regard to automatic processing of personal data during profi-

ling.[5] Although the Council of Europe Resolutions and Recommendations are not binding, they undoubtedly set the preferred protection level for Member States.

One of the most important legal acts concerning the protection of privacy and the protection of personal data is Convention 108 drawn up in Strasbourg on 28 January 1981 for the protection of individuals with regard to automatic processing of personal data adopted by the Council of Europe regime. This Convention is of particular importance in view of the large number of countries that have ratified it and its binding nature for States Parties. Until today, it has been repeatedly supplemented and adapted to technological progress. As M. Czerniawski points out: Convention 108 is "the first and so far most important step towards the harmonization of personal data protection regulations at the international level" [Czerniawski 2020, 28].

Convention 108 is binding at the vertical level, imposing obligations on countries that have ratified the Convention without obliging citizens of member states. The metanorm, which is introduced by Convention 108, is the principle of minimum protection of personal data, consisting in obliging the parties to the Convention to adapt their legal systems to the basic principles introduced by the Convention (Article 4 of the Convention) [Litwiński 2009, 19]. These basic principles are: fairness and lawfulness of processing, adequacy of data, the principle of being bound by the purpose of collection, the obligation to protect the data collected and to respect the rights of data subjects. Moreover, Convention 108 in Article 6 distinguished the category of sensitive data that cannot be processed automatically, and provided individuals with access to their data, the possibility to rectify them, to obtain information about the data, or to object to a refusal to provide such information (in Article 8). The standards set by the Council of Europe in Convention 108 have been developed in EU law. Convention 108 is the basis for subsequent legal regulations.

Convention 108 indicates the most important principles of personal data protection, directing Member States towards given legal solutions, while leaving "a certain margin of freedom in shaping solutions corresponding to

[5] Recommendations, resolutions and guidelines, Council of Europe 2020, https://www.coe.int/en/web/cdcj/recommendations-resolutions-guidelines [accessed: 01.05.2020].

a given legal system" [Barta, Fajgielski, and Markiewicz 2015, 46]. Thanks to this margin of freedom, the Convention has been ratified by the majority of the Council of Europe countries (47 countries) and 8 non-member countries (e.g. Mauritius, Mexico, Argentina or Uruguay). Among the countries of Central and Eastern Europe, Slovenia (1994) and Hungary (1997) were the first to ratify the Convention. The remaining countries ratified Convention 108 already in the 21st century: in 2000 – Slovakia; in 2001 – the Czech Republic, Lithuania, Latvia, Estonia; in 2002 – Poland, Bulgaria and Romania; in 2005 – Croatia, Serbia, Montenegro and Albania; in 2006 – Bosnia and Herzegovina and North Macedonia; then Ukraine (2010) and Russia (2013). These statistics show that the implementation of an adequate level of personal data protection in this area of Europe has taken time and appropriate preparation. In the 1980s, only the countries of Western and Northern Europe were ready to ratify the document.[6]

It should be borne in mind that Convention 108 was adopted in the early 1980s, and therefore work on modernizing its content has continued for several years. On 10 October 2018 the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) was signed. The amended Convention adopted working name 108+. To date, 38 countries have signed Convention 108+, although it has not yet entered into force due to too few ratifications. Among the countries of our region, the following countries have not signed it so far: Albania, Bosnia and Herzegovina, Romania and Ukraine.[7] The amending protocol strengthens the principles of personal data protection expressed in Convention 108 in terms of new technologies and practices. Furthermore, it introduces protection for the transfer of personal data between countries. Convention 108+ is a further step towards the harmonization of international standards for the protection of personal data, as it is in line with global standards, and in particular European Union law. Moreover, it allows international organizations (including the EU) to join the Convention.

[6] Chart of signatures and ratifications of Treaty 108, Council of Europe 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures [accessed: 02.05.2020].

[7] Chart of signatures and ratifications of Treaty 223, Council of Europe 2020, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures [accessed: 03.05.2020].

The first milestone towards the standardization and harmonization of personal data protection rules within the European Union was the adoption of 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.[8] A directive is an act of Union law which establishes an objective for the Member States, leaving them free to adopt measures. By the end of 1998, all EU countries at that time had adopted appropriate legislative solutions. However, it should be noted that none of the Central and Eastern European countries were members of the European Union in 1998, thus it was only when they joined the EU that they were obliged to meet the standards set by the Directive. Nevertheless, Directive 95/46/EC was consistent with the provisions of Convention 108 adopted by the Council of Europe regime, and what is more, Recital 11 of the Directive explicitly stated that it preserves and reinforces the principles of personal data protection as expressed in the Council of Europe Convention.

Following the enactment of Directive 95/46/EC, a number of directives were issued within the EU structures, aimed at standardizing the principles of personal data protection in Europe. Among others, Directive 2000/31/EC of the European Parliament and of the Council, regulating the rights and obligations of information society service providers and recipients, dates from 2000. Its most important message is that the provision of services via the Internet should be subject to the principle of transparency of the service provider and respect for the privacy of the service recipient, which means, inter alia, limiting the data collected to the minimum necessary and even granting the right to use the services anonymously or under a nickname. In 2002, Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) was issued. It obliges Member States to ensure an equivalent protection level of the right to privacy with respect to the processing of personal data in the electronic communications sector and to ensure the free movement of these personal data within the Community. The European Union has also regulated standards for the retention of certain data by providers of pu-

[8] OJ L 281 of 1995.

blicly available electronic communications services or of a public communications network in order to ensure that these data are used in specific situations for the purpose of detecting and investigating serious crime as defined in national legislation (Directive 2006/24/EC of the European Parliament and of the Council). The European Union places a very strong emphasis on ensuring that personal data protection is guaranteed for the citizens of Member States in the context of their use of electronic services.

In the context of developing information society, the right to the protection of personal data has taken on particular importance and has been recognized as a fundamental right of the European Union. The EU Charter of Fundamental Rights, which was made legally binding in 2009, is a fundamental human rights document. Article 7 of the Charter refers to the obligation to protect privacy, while Article 8 contains regulations on personal data protection. Both of these provisions should be read together, because: "personal data are protected in view of their special importance in private and family life" [Jurczyk 2009]. The recognition of the right to personal data protection as a fundamental right shows the importance of this issue and the right to personal data protection has been enshrined alongside the values commonly recognized by various international instruments.

Article 8 of the Charter of Fundamental Rights ensures everyone's right to the protection of their personal data (paragraph 1), and indicates that these data must be processed fairly, for specified purposes, on a statutory basis, and that everyone has the right of access to and rectification of their data. The Charter not only provides everyone with the right to the protection of personal data, but also establishes a guarantee of this right, indicating that control of the processing of personal data should be exercised by an independent authority. The substantive aspect of this right is closely related to the institutional element [Rokita 2016, 4ff]. The right to the protection of personal data has been placed in Title II of the Charter – "Freedom." M. Czerniawski emphasizes that "in the era of information society and the Internet, the "freedom" aspect, controlling and disposing of own personal information, including personal data, seems to gain importance […]" [Czerniawski 2020, 21].

The European Union has set a goal of harmonizing personal data protection rules in the Member States. For this purpose, an EU Act such as the dire-

ctives has proved to be an insufficient measure. In 2012, work on data protection reform in the EU began. The main objectives of the new comprehensive approach to personal data protection were to strengthen individuals' rights, harmonize the rights and obligations of data controllers, amend the rules on personal data protection within the police and judicial cooperation in criminal matters, provide better institutional arrangements for enforcing the application of personal data protection rules and the global dimension of data protection [Gajda 2014, 81]. The work on the new rules was completed on 27 April 2016 with the adoption of the Regulation of the European Parliament and of the Council (EU) on the protection of individuals 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).[9]

The provisions on personal data protection have taken the form of an EU regulation, resulting in their direct application in all EU Member States. The general data protection regulation entered into force on 24 May 2016, while in the Member States it became applicable on 25 May 2018. This regulation revolutionized data protection laws and introduced a new level of protection in the 11 Central and Eastern European countries that are members of the EU, i.e. the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Slovakia, Slovenia, Hungary, Bulgaria, Romania and Croatia. The EU regulation is intended to guarantee more effective protection of personal data, which in the era of digitization and globalization is not an easy task [Pawlak and Kosowska-Korniak 2018, 3]. The Regulation on the protection of personal data has introduced principles according to which personal data are to be processed. These are: processing in accordance with the law, reliability and correctness of processing, transparency, integrity and confidentiality, processing for a strictly defined purpose, to the minimum necessary extent and for the shortest necessary time, as well as in a way that is transparent for the person whose data are processed. The obligation to respect the principles relating to the processing of personal data is the responsibility of data controllers, who in accordance with the principle of accountability, must demonstrate that they comply with these principles. They are required to implement appropriate organizational and technical measures to ensure that their activities comply with all the principles. However, the General Data Protection

[9] OJ EU L 119, 4.5.2016, p. 1.

Regulation does not provide for specific solutions or minimum technical standards required for data protection. It is the responsibility of each controller to choose the most appropriate measures. The Regulation differentiates the obligations imposed on controllers according to the amount of data that are processed and their type. It imposes direct obligations on all those who process personal data in the Member States (except for processing for private purposes). Therefore, the EU standards have been taken over from the level of obligations addressed to the contracting parties' countries to the level of imposing specific obligations on national operators in different sectors.

The Regulation imposes a number of obligations on data controllers, with which the rights of data subjects are linked. These include the right of access to the data, which is expressed in the possibility to obtain a copy of data, but also to obtain a range of transparent information about their data, including confirmation of whether a particular entity is processing a person's personal data (Article 15 of the Regulation). Individuals also have the right to rectify inaccurate data or supplement them (Article 16). The Regulation introduced a previously unknown right to be forgotten, requiring the immediate deletion of personal data (Article 17(1)), as well as the right to restrict processing on request of the data subject in specific cases (Article 18(1)). The data subject also has the right to transfer the data directly to another controller (expressed in Article 20(2) of the Regulation). Furthermore, a person dissatisfied with the controller's actions may lodge a complaint with the supervisory authority, which must be established in each EU country. By introducing a mandatory control mechanism, the data protection guarantees can be effectively enforced.

The General Data Protection Regulation has raised awareness among many Europeans on the protection of their personal data. The implementation of the Regulation represents a further protection level (compared to universal standards and the Council of Europe). The General Regulation was adopted in conjunction with Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection and prosecution of criminal offences and the execution of penalties, on the free movement of such data and repealing

Council Framework Decision 2008/977/JHA.[10] This is the so-called "Police Directive," which aims to protect the personal data of actors (witnesses, victims, perpetrators) and to increase the exchange of information between law enforcement authorities, thereby improving security in the EU. It is important to note the multifaceted nature of the activities of EU bodies towards a real increase in personal data protection.

4. Other international standards

Some Central and Eastern European countries are members of the Organization for Economic Cooperation and Development (OECD), which comprises of highly developed countries all over the world. This organization has also had a significant impact on the development of personal data protection standards through the Recommendation of 23 September 1980 on guidelines for the protection of privacy and transfer of personal data between countries. They were adopted as a Recommendation of the Council of the Organization for Economic Cooperation and Development and support three principles binding on the Member States: pluralistic democracy, respect for human rights and a free market economy. The principles contained in the Privacy Guidelines are clear and flexible with regard to their application, and the generality level of their formulation allows them to adapt to technological change. These principles include the principles of limited collection, data quality, purpose limitation, use limitation, security, disclosure, individual participation, and responsibility. The principles apply both at national and international level. They have been used in a considerable number of regulatory instruments over the past years and are still widely used in the public and private sectors.[11] All the countries of Central and Eastern Europe that joined the European Union in 2004 belong to the organization: Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Slovakia, Slovenia. In these countries, the organization's guidelines were of the greatest importance until the time of accession to European structures.

[10] OJ EU L 119/89.

[11] See http://www.oecd.org/sti/ieconomy/15590241.pdf [accessed: 03.05.2020], p. 2.

Conclusion

Standards on the protection of personal data, set by international organizations, evolve along with the development of technology and new opportunities of the information society. It should be noted that no global protection level has been developed and therefore these standards vary between regions of the world. Moreover, even in one region, the legal regulations related to personal data protection are not uniform. An example of such a region is Central and Eastern Europe, where the legislation level is very different in individual countries. The standards of protection in countries are determined by membership of different types of international organizations and ratification of documents developed within these organizations. The influence of international organizations in this respect is enormous and many countries have implemented individual solutions under international "pressure" as well as due to the need to ensure standards for the flow of this data between individual countries. Table 1 presents the area of influence concerning the protection of personal data in the countries of Central and Eastern Europe by the discussed international organizations and their standards.

Table 1 – Area of influence as regards personal data protection in Central and Eastern European countries by the standards of selected international organizations

Central and Eastern European country	**UN Standards**	**Council of Europe standards** (year of ratification of Convention 108)	**EU standards**	**OECD standards**
Albania	+	+ (2005)		
Belarus	+			
Bulgaria	+	+ (2002)	+ since 2007	
Bosnia and Herzegovina	+	+ (2006)		
Croatia	+	+ (2005)	+ from 2013	
Montenegro	+	+ (2005)		
Czech Republic	+	+ (2001)	+ since 2004	+
Estonia	+	+ (2001)	+ since 2004	+
Lithuania	+	+ (2001)	+ since 2004	+
Latvia	+	+ (2001)	+ since 2004	+
North Macedonia	+	+ (2006)		

Poland	+	+ (2002)	+ since 2004	+
Russia	+	+ (2013)		
Romania	+	+ (2002)	+ since 2007	
Serbia	+	+ (2005)		
Slovakia	+	+ (2000)	+ since 2004	+
Slovenia	+	+ (1994)	+ since 2004	+
Ukraine	+	+ (2010)		
Hungary	+	+ (1997)	+ since 2004	+

Source: Own elaboration

The universal standards developed within the UN – although limited to guaranteeing the right to privacy – have an impact on the personal data protection legislation of UN Member States. This results from the current broad understanding of the right to privacy, as well as from the monitoring activities of the Human Rights Committee and the assessment of regular reports on the implementation of appropriate guarantees. The UN standards are of particular importance for the state of Belarus, which does not belong to any of the regional organizations. The countries that belong to the Council of Europe are of the greatest importance for the Central and Eastern European region in terms of standardization of personal data protection. The breakthrough Convention 108 has been ratified by all member countries of the Council of Europe, located in this region of the world. Although some countries implemented it quite late (such as Russia in 2013 or Ukraine in 2010), this does not change the fact that it is a visible step forward in providing better guarantees for personal data protection for their citizens. The highest level of personal data protection takes place in the Member States of the European Union, on the territory of which the General Data Protection Regulation of 2016 is directly applicable. It should be noted that all the countries of our region, which joined the EU in 2004, had already used the guidelines of the Organization for Economic Cooperation and Development, which undoubtedly made it easier for them to prepare for implementation of the General Data Protection Regulation. However, the high level of personal data protection guaranteed by the EU regulation does not remain without influence on other countries – as already the "effect of the regulation" consisting in drawing patterns from EU standards by other countries is mentioned [Czerniawski 2020, 57].

The legislation of European countries is influenced by many different guidelines, recommendations, directives, or finally, obligations of international organizations gathering individual countries. Most of the countries remain "in the crossfire" of different regulations that complement each other, and overlap in some parts. These regulations are consistent with each other and increase the level of personal data protection in the Member States in real terms. The multitude of international documents shows a great need for a broader than national perspective view on the protection of personal data the flow of which knows no territorial boundaries. Therefore, ensuring a similar level of data protection in different countries – although very difficult – is extremely important and is an important priority for international organizations.

REFERENCES

Barta, Janusz, Paweł Fajgielski, and Ryszard Markiewicz. 2015. *Ochrona danych osobowych*. Warsaw: Wolters Kluwer.

Czerniawski, Michał. 2020. "Ochrona danych osobowych w prawie międzynarodowym." In *Meritum. Ochrona danych osobowych*, edited by Dominik Lubasz, 1-27. Warsaw: Wolters Kluwer.

Gajda, Anastazja. 2014. "Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie unii europejskiej." *Kwartalnik Kolegium Ekonomiczno-Społecznego. Studia i Prace* 4:55-91.

Jabłoński, Mariusz, and Sylwia Jarosz-Żukowska. 2004. *Prawa człowieka i systemy ich ochrony. Zarys wykładu*. Wrocław: Wydawnictwo Uniwersytetu Wrocławskiego.

Jurczyk, Tomasz. 2009. *Prawa jednostki w orzecznictwie Europejskiego Trybunału Sprawiedliwości*. Warsaw: Oficyna.

Kondratiewa-Bryzik, Jelena, and Katarzyna Sękowka-Kozłowka (eds.). 2013. *Prawa człowieka wobec rozwoju biotechnologii*. Warsaw: Wolters Kluwer.

Kopff, Andrzej. 1972. "Koncepcja praw do intymności i do prywatności życia osobistego (Zagadnienia konstrukcyjne)." *Studia Cywilistyczne* 20:3-30.

Krzysztofek, Kazimierz, and Marek Szczepański. 2002. *Zrozumieć rozwój. Od społeczeństw tradycyjnych do informacyjnych*. Katowice: Wydawnictwo Uniwersytetu Śląskiego.

Litwiński, Paweł. 2009. *Ochrona danych osobowych w ogólnym postępowaniu administracyjnym*. Warsaw: Oficyna.

Mielnik, Zbyszko. 1996. "Prawo do prywatności (wybrane zagadnienia)." *RPEIS* 2:29-41.

Mednis, Arwid. 1999. "Ochrona prawna danych osobowych a zagrożenia prywatności – rozwiązania polskie." In *Ochrona danych osobowych*, edited by Mirosław Wyrzykowski, 167-95. Warsaw: Instytut Spraw Publicznych.

Pawlak, Anna, and Ewa Kosowska-Korniak. 2018. *Inspektor Ochrony Danych (DPO)*. Lublin: Fundacja VCC.

Rojszczak, Marcin. 2019. *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*. Warsaw: Wolters Kluwer.

Rokita, Krzysztof. 2016. "Niezależność organów ochrony danych osobowych w ogólnym rozporządzeniu o ochronie danych." *Europejski Przegląd Sądowy* 7:4-12.

Warren, Samuel D., and Louis D. Brandeis. 1890. "The right to Privacy." *Harward Law Review* 4:193-220.

Standards of Personal Data Protection in Central and Eastern European Countries

Abstract

The paper is a review of the most important standards of personal data protection developed by international organizations including the countries of Central and Eastern Europe. The paper describes both universal standards of the United Nations, as well as regional standards (Council of Europe and European Union) and the Organization for Economic Cooperation and Development. It presents the development of international regulations concerning the protection of personal data, indicating at the same time in which countries of Central and Eastern Europe the particular documents apply. The paper constitutes an attempt to assess the consistency of international solutions and their real impact on national legislation.

Keywords: personal data protection, international standards, Central and Eastern Europe

Standardy ochrony danych osobowych w krajach Europy Środkowo-Wschodniej

Streszczenie

Artykuł stanowi przegląd najważniejszych standardów ochrony danych osobowych wypracowanych przez organizacje międzynarodowe skupiające m.in. kraje Europy Środkowo-Wschodniej. W opracowaniu opisano zarówno standardy uniwersalne Organizacji Narodów Zjednoczonych, jak i regionalne (Rady Europy oraz Unii Europejskiej), a także Organizacji Współpracy Gospodarczej i Rozwoju. Przedstawiono rozwój międzynarodowych regulacji dotyczących ochrony danych osobowych, wskazując przy tym, w których krajach Europy Środkowo-Wschodniej obo-

wiązują poszczególne dokumenty. Artykuł stanowi próbę oceny spójności międzynarodowych rozwiązań oraz ich realnego wpływu na ustawodawstwa krajowe.

Słowa kluczowe: ochrona danych osobowych, międzynarodowe standardy, Europa Środkowo-Wschodnia

Informacje o Autorze: Dr ANNA PAWLAK, Instytut Nauk Prawnych, Akademia Ekonomiczno-Humanistyczna w Warszawie; adres do korespondencji: ul. Okopowa 59, 01-043 Warszawa, Polska; e-mail: a.pawlak@vizja.pl; https://orcid.org/0000-0001-6112-8743