UDC 342.7
DOI: 10.56215/naia-herald/4.2023.68

Formation of the institute of personal data protection and experience of its implementation in the countries of the EU

Bohdan Yakymenko*
Postgraduate Student
Kyiv International University
03179, 49 Lvivska Str., Kyiv, Ukraine
https://orcid.org/0009-0008-7704-2934

■ **Abstract**. The development of digital technologies in the modern world led to an increase in interference in the private life of a person and the number of human rights violations related to private life. Ukrainian legislation on personal data protection does not meet the latest trends and standards of the European Union (EU) in this area and needs to be updated. The article is intended to analyse the development of the institute of personal data protection in the world to identify ways to adapt the national legislation of Ukraine to the current personal data protection standards of the EU. To carry out the research, the following scientific methods were used: inductive, deductive, dialectical, analysis and synthesis, comparative legal, historical legal. According to the results of the research, the personal data protection institute has gone through a significant path of development from individual notions and concepts to a structured set of standards and tools legally established at the EU level. A characteristic feature of this development is the adoption of new legal acts on personal data protection, as well as increasingly strict and comprehensive regulation of issues related to personal data processing. Ukrainian personal data protection legislation, although historically improved in line with European standards, as of 2023 is based on the outdated Directive 95/46/EC, which has already been rejected by the EU. Compared to the legal systems of neighbouring countries such as Poland, Bulgaria and Romania, Ukrainian personal data protection legislation is not only inferior, but also significantly lags behind in terms of detail, definition of key terms and principles. The results of the research can be used in law-making work, in particular, when drafting a new bill of the basic data protection law and for further research on ways to improve Ukrainian laws and laws of other candidates for membership in the European Union on personal data protection

■ **Keywords**: human rights; privacy; personal and family life; personal data processing; General Data Protection Regulation

■ Introduction

During the 20th and 21st centuries, information technologies, digital and electronic communication tools are rapidly developing in the world. Activities involving operations with personal data are performed every day. The development of digital technologies, collection of personal data by programs and websites on an ongoing basis create new challenges to privacy. As the relations in the field of personal data become more and more complicated, the scope of personal data processing is constantly expanding. The number of security breaches, including personal data breaches, is on the rise and keeps increasing as technologies continue to develop. One such example is a cyberattack using Petya.A virus on a number of public and private institutions and organizations of Ukraine, carried out on July 27, 2017 (Bezugliy, 2018). Another,

■ **Suggested Citation:**
Yakymenko, B. (2023). Formation of the institute of personal data protection and experience of its implementation in the countries of the EU. *Scientific Journal of the National Academy of Internal Affairs,* 28(3), 68-79. doi: 10.56215/naia-herald/4.2023.68.
■ *Corresponding author
■ Received: 16.09.2023; Revised: 29.11.2023; Accepted: 29.12.2023

more recent example is a leak of personal data from over 533 million Facebook accounts in April 2021 that led to the imposition of a fine of 265 million EUR on Meta (Roth, 2022). These circumstances create additional risks for human rights and require the governments to take action to implement new legal measures to secure privacy and protect personal data.

Problems of the development of the personal data protection institute were studied by a number of scientists. O.V. Hron & A.K. Pogorelenko (2018) identified certain problems in the personal data protection area and outlined main directions to enhance Ukrainian legislation on personal data protection. The need to enhance personal data protection is particularly relevant because of the advancement of digital and telecommunication systems, which makes it necessary to regulate the accessibility of personal data by establishing specific, meaningful requirements in the legislation (Nazimko *et al.*, 2022).

The study of the process of formation of privacy and its place among other basic human rights is necessary to highlight the process of formation of the institute of personal data protection. The place of the right to privacy in the system of human rights generations is studied by R.B. Saglam *et al.* (2022) and S. Bulavina & T. Davydova (2018), who attribute this right to the third generation of global human rights. T. Popovych & A. Shavarin (2019) view the right of the individual to protect his personal data as a right of the fourth generation of human rights. T. Popovych (2021) in the context of this generation considers theoretical and legal issues of personal data protection on the Internet.

When studying the establishment and development of the personal data protection institute, it is important to refer to the General Data Protection Regulation (hereinafter – the Regulation)[1], which is currently the main legal act of the EU regulating personal data processing. S.R. Asiryan & K.A. Aleksanyan (2021) examines the impact of the Regulation on national personal data laws in other countries, emphasizing that the Regulation has become a kind of standard, the norms of which are implemented by countries into national legislation.

Scientists pay a lot of attention to the application and impact of the Regulation on personal data protection. Authors analyse how the Regulation influences internal policies and processes of companies related to personal data processing and highlight key areas where such influence takes place, including the need to update existing practices, the appointment of officials responsible for personal data processing, increased attention to the selection of counterparties and the need to put obligations regarding personal data protection on such counterparties (Hoofnagle *et al.,* 2019; Novoitenko & Malynovskyi, 2020). Considerable attention is also paid to compliance with the technical and organizational requirements of the Regulation (Tamburri, 2019).

The purpose of the study was to identify key stages of formation of the institute of personal data protection and analyse peculiarities of its implementation in the EU countries in order to highlight possible ways to enhance Ukrainian legislation in the personal data protection area.

Materials and Methods

To reach the tasks of the study, a number of methods, including general methods of science and special methods of legal science, were used. Inductive and deductive methods were used for a comprehensive analysis of the evolution of the personal data protection institute. Individual cases that stipulated the formation of the notion "privacy", were analysed using the inductive method. In this regard, the events that caused this process and case law were viewed. The deductive method helped to formulate general conclusions regarding specific stages of formation and development of the personal data protection institute, to distinguish general trends of such development. Dialectical method helped to comprehend the nature and dynamics of changes occurring in the privacy and personal data protection area, and social processes that stipulated such changes. With the help of methods of analysis and synthesis, separate components of the personal data protection institute were considered both individually and collectively, problematic aspects of the development of this institute were identified. The historical legal method played a key role in the research. This method was applied to investigate the chronology of development of the personal data protection institute in the world and consistently identify the main stages of the development of Ukrainian and European personal data protection laws. Comparative legal method helped to compare the norms regulating personal data protection in the EU and Ukraine and formulate conclusions regarding the current state of conformity of provisions in Ukrainian laws with similar provisions of the EU legislation in this area.

The basis of the article is a study of EU legislation regarding privacy and personal data protection. In this

[1] Regulation of the European Parliament and of the Council No. 2016/679 "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)". (2016, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

regard, most important European legal instruments have been analysed, such as Convention No. 108[1], Directive 95/46/EC[2] and the Regulation[3] which replaced Directive 95/46/EC and applies from 2018. The article also contains analysis of Ukrainian data protection laws from the standpoint of their correspondence with relevant legal acts of the EU. In particular, attention is paid to the review of the Law of Ukraine "On Protection of Personal Data"[4], which is a basic Ukrainian law in the personal data protection area.

Results and Discussion

The institute of personal data protection began its formation at the end of the 19th century with the emergence of the concept of privacy. American lawyers S. Warren & L. Brandeis (1890) described privacy as "the right to be left alone". The above-mentioned interpretation of privacy appeared as a result of technological development in the USA at the end of the 19th century, in particular, the spread of the press and photographs. These media invaded personal life through the publication of unverified information. In this regard, S. Warren & L. Brandeis (1890) noted that new technologies invaded man's privacy and inflicted pain and suffering greater than bodily injury.

The category of right to privacy was recognized by the courts and subsequently widely used in the judicial practice of the USA. In 1905, in the decision in the case "Pavesich vs. New England Life Ins. Co."[5] the court satisfied the claim of a man who was depicted in an advertising advertisement without his consent. When making the decision, the court noted that a person is entitled to choose the way, time, and place he would like to be submitted to the attention of the public and such submission requires a person's consent. In 1965, US Supreme Court Justice Douglas in the case of Griswold vs. Connecticut[6] carved out the "right to privacy" from the First Five Amendments to the US Constitution. In his opinion, these amendments protect various zones of privacy. The judge also noted that the right to privacy emerged before the Bill of Rights.

Despite the importance of introducing the idea of privacy, there is criticism of the definition of privacy given by S. Warren & L. Brandeis (1890) among scientists. Critics believe that the definition of privacy as the right to be left alone is too vague and does not clarify the essence of privacy. Furthermore, the right to be left alone does not account for other significant concepts, for example freedom of speech (Solove, 2002). Thus, the concept of privacy was formed and used in judicial practice at the end of the 19th – the beginning of the 20th century, that is, before the peak of development of information technologies.

The introduction of the idea of privacy had a major influence on the establishment and evolution of the system of human rights and freedoms. In the theory of state and law, it is customary to divide human rights into four generations depending on their nature (Popovych & Shavarin, 2019). The first generation of human rights occurred as a result of the Age of revolutions and includes rights of political and civil nature. These rights were enshrined in the constitutional acts of the 17th-18th centuries. In science, such rights have been called "negative", as they are designed to ensure the freedom of a citizen from external interference by the state (Kozyubra, 2015).

Economic and social development of society, broad support in society for the ideas of social justice and solidarity led to the emergence and normative consolidation of human rights of the second generation (Kozyubra, 2015). This generation includes economic, social and cultural rights, such as the right to rest, the right to work, the right to medical and social security, the right to education. These rights were legally enshrined in the Universal Declaration of Human Rights[7] and the International Covenant on Economic, Social and Cultural Rights of 1966[8] and are named as "positive" in science.

[1] Convention of the Council of Europe No. 108 "On the Protection of Individuals with Regard to Automated Processing of Personal Data". (1981, January). Retrieved from https://rm.coe.int/1680078b37.

[2] Directive of the European Parliament and of the Council No. 95/46/EC "On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data". (1995, October). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.

[3] Regulation of the European Parliament and of the Council No. 2016/679 "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)". (2016, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[4] Law of Ukraine No. 2297-VI "On Protection of Personal Data". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text.

[5] Justice of the Supreme Court of Georgia No. 50 SE 68,122 Ga. 190 "Pavesich v. New England Life Ins. Co." (1905, March). Retrieved from https://case-law.vlex.com/vid/pavesich-v-new-england-888103034.

[6] Appeal From the Supreme Court of Errors of Connecticut No. 381 U.S. 479 "Griswold v. Connecticut". (1965, June). Retrieved from https://supreme.justia.com/cases/federal/us/381/479/.

[7] Universal Declaration of Human Rights. (1948, December). Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[8] International Covenant on Economic, Social and Cultural Rights. (1966, December). Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights.

The third human rights generation emerged following the Second World War as a result of the need to maintain peace, protect the environment and development of the liberation movements for independence. The rights of the third generation are "collective" rights, that is, they do not concern a specific person, but an entire community – a separate nation or the whole of humanity. The emergence of these rights is caused by problems of a global nature, therefore third generation rights include rights concerning peace, self-determination of nations, natural resources, safe environment and sustainable development.

The fourth generation of human rights emerged at the end of the 20th and during the 21st century due to the development of biology, psychology, medicine, digital technologies and informatization (Table 1). This category of rights is debatable, it includes rights of different content, including the right to peace and nuclear safety, informational and environmental rights, the right to sex change, organ transplantation, cloning, artificial reproduction, abortion, euthanasia, etc. In the context of privacy and personal data protection, the ability to safeguard privacy and personal data online is a fundamental entitlement.

Table 1. Periodization of the development of the institution of personal data protection as a part of the genesis of human rights

Generation of human rights	Dating	Legislative consolidation	Rights	Privacy and personal data protection institution
I	17th-18th century	Habeas Corpus Act (1679)[1], Bill of Rights (1688)[2]	Civil and political rights (personal freedom, equality before law, freedom of speech, right to vote etc.)	Has not formed yet.
II	during 20th century	Universal Declaration of Human Rights (1948)[3], International Covenant on Economic, Social and Cultural Rights (1966)[4]	Economic, social and cultural rights (right to rest, right to work, right to education etc.)	Right to privacy begins to form (Art. 12 of the Universal Declaration of Human Rights[5]).
III	end of the 20th century (following the Second World War)	Stockholm Declaration (1972),[6] Rio Declaration (1992)[7]	Collective rights (right to peace, self-determination of nations, safe environment etc.)	With the development of communications, the right to privacy as a right of collective nature begins to transform into data protection institute.
IV	end of the 20th – during 21st century	Charter of Fundamental Rights of the EU (2000)[8]	Nuclear safety, informational and digital rights, cloning, abortion, euthanasia etc.	Personal data protection institute has been established and continues to evolve with the development of digital technologies (Art. 8 of the Charter of Fundamental Rights of the EU[9]).

Source: developed by the author

Due to the collective nature of privacy, it seems justified to attribute the right to privacy to third generation (Bulavina & Davydova, 2018). This right also has other features of the third generation of human rights: interdependence with other rights, extraterritoriality, belonging to different generations of humanity (Ivankiv, 2016). At the same time, there are different views in the literature regarding the place of the right to privacy in the system of generations of human rights. There is an opinion that the right to privacy belongs to the first generation (Sofiyuk, 2018).

[1] Habeas Corpus Act. (1679, May). Retrieved from https://www.legislation.gov.uk/aep/Cha2/31/2/data.pdf.
[2] Bill of Rights. (1688, December). Retrieved from https://www.legislation.gov.uk/aep/WillandMarSess2/1/2/introduction.
[3] Universal Declaration of Human Rights. (1948, December). Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights.
[4] International Covenant on Economic, Social and Cultural Rights. (1966, December). Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights.
[5] Universal Declaration of Human Rights. (1948, December). Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights.
[6] Declaration of the United Nations Conference on the Human Environment. (1972, June). Retrieved from https://www.un.org/en/conferences/environment/stockholm1972.
[7] Rio Declaration on Environment and Development. (1992, June). Retrieved from https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_CONF.151_26_Vol.I_Declaration.pdf.
[8] Charter of Fundamental Rights of the European Union. (2000, December). Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf.
[9] Ibidrm, 2000.

Following the Second World War, in 1948, the Universal Declaration of Human Rights was adopted (hereinafter – the Declaration)[1], which enshrines the basic inalienable human rights. Among other rights, the Declaration recognizes the right to privacy (Article 12) and grants its protection by law. Similar provisions regarding privacy are established by the European Convention on Human Rights[2]. According to the European Convention on Human Rights, the intervention of public authorities into privacy is possible only in cases provided by the law, on reasonable grounds such as public interest, security, and safety[3]. Protection from interference into privacy is also declared in the International Covenant on Civil and Political Rights[4].

Over time, the concept of privacy has been replaced by the concept of personal data protection, which is considered as informational sovereignty of a person. The right of a person to control the procedure and method of personal data processing activities, to provide or withdraw consent to such processing is recognized. Further development of the institute of personal data protection is connected with enactment of a number of legislative acts at the level of the EU and individual countries. In 1981, the Council of Europe adopted Convention No. 108 for the Protection of Individuals with regard to Automated Processing of Personal Data (hereinafter – the Convention)[5]. The purpose of the Convention is to secure the right to privacy of individuals in connection with processing of personal data by automated means. The Convention provides individuals with a number of rights regarding their personal data, in particular to prove that the automated file with their personal data exists, obtain information about the purposes of its existence and obtain details of the data controller; to verify the fact of personal data storage and receive such data in an understandable form; to demand correction or deletion of the data and use legal means if the request is not satisfied[6]. The Convention is actually the first document adopted at the EU level that exclusively regulates personal data protection matters. In 2001, an Additional Protocol was adopted (Protocol)[7] was adopted. The Protocol sets an obligation on signatory states not to transfer personal data to states that do not ensure the necessary protection of personal data. Ukraine ratified the Convention and the Protocol in 2010[8].

In 1995, Directive 95/46/EC was adopted[9]. This document laid the foundations for personal data protection in the EU for subsequent years. Directive 95/46/EC defined key concepts related to the processing of personal data, established its principles, determined the subjects of personal data processing relations, their rights, and duties. In particular, the Directive expressly defined when personal data can be lawfully processed. The Directive also established special categories of data, which include data regarding a person's race and origin, political views and beliefs, membership in trade unions, health, and sex life. Processing of such data is generally prohibited by the Directive.

The Declaration of the Charter of Fundamental Rights of the EU in 2000[10] (hereinafter – Charter) was the next important stage in the development of the personal data protection institute. The Charter was enacted with as the Lisbon Treaty[11] entered force in 2009. The Charter enshrines a person's right to respect for privacy (Article 7), as well as the right to the protection of personal data, which includes the right to access and rectify such data (Article 8)[12]. Since the Charter is mandatory for EU member

[1] Universal Declaration of Human Rights. (1948, December). Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights.
[2] European Convention for the Protection of Human Rights and Fundamental Freedoms. (1950, November). Retrieved from https://www.echr.coe.int/european-convention-on-human-rights.
[3] Ibidem, 1950.
[4] International Covenant on Civil and Political Rights. (1966, December). Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.
[5] Convention of the Council of Europe No. 108 "On the Protection of Individuals with Regard to Automated Processing of Personal Data". (1981, January). Retrieved from https://rm.coe.int/1680078b37.
[6] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (1981, October). Retrieved from https://rm.coe.int/1680078b37.
[7] Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows. (2001, November). Retrieved from https://rm.coe.int/1680080626.
[8] Law of Ukraine No. 2438-VI "On Ratification of Convention for the Protection of Individuals with Regard to Automated Processing of Personal Data and Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows". (2010, July). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2438-17?lang=uk#Text.
[9] Directive of the European Parliament and of the Council No. 95/46/EC "On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data". (1995, October). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.
[10] Charter of Fundamental Rights of the European Union. (2000, December). Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf.
[11] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Signed at Lisbon. (2007, December). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12007L%2FTXT.
[12] Charter of Fundamental Rights of the European Union. (2000, December). Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

states, their state bodies and institutions, its entry into force created additional guarantees and means to protect personal data. After being included in the Charter, the right to the protection of personal data finally acquired the features of a fundamental right, which include belonging to a person from the moment of birth, inalienability, inalienability, universality, and interdependence (the fundamental right can be exercised only in connection with other fundamental rights) (Custers & Malgieri, 2022).

In 2008, Directive 95/46/EC was supplemented by the Council Framework Decision No. 2008/977/JHA[1]. The aim of the decision is to protect the privacy rights of natural persons by regulating cooperation of police and judicial bodies within data processing activities. In order to strengthen cooperation on personal data protection within the EU in the field of activities of courts and law enforcement agencies, the Council Decision 2008/615/JHA[2] (Prüm Decision) and Council Framework Decision (EU) 2009/315/JHA[3] were adopted. The Prüm decision aims to strengthen cross-border cooperation through improvement of communication and data flow between police and judicial bodies. The decision regulates the interaction of EU member states in such areas as the automated transfer of DNA profiles, dactyloscopic information and national data on vehicle registration; transfer of data regarding significant cross-border events; transfer of data to prevent terrorism; various conditions and measures to strengthen cross-border police cooperation. Council Framework Decision (EC) 2009/315/JHA establishes ways for member states to transfer information about convicted citizens of other member states, defines the obligations of a member state to store information about its convicted citizen and the methods used in responses to requests for criminal record information; introduces regulatory frameworks for computerized conviction information exchange systems between member states.

The evolution of the personal data protection institute in the EU led to the adoption of the General Data Protection Regulation (Regulation (EU) 2016/679)[4] on April 26, 2016. The Regulation became a qualitatively new legislative act regulating personal data protection and repealed Directive 95/46/EU. An important feature of the Regulation is its extraterritorial effect. The provisions of the Regulation apply to the processing of personal data of data subjects located in the EU, even if such data is processed by an entity located outside the EU that supplies services or goods to data subjects in the EU or monitors the behaviour of the latter within the EU. The Regulation establishes the principles of processing personal data, in particular, such as fairness, lawfulness, and transparency of processing; data minimization; accuracy; limitation of personal data storage; integrity and confidentiality; accountability of data controller. The Regulation establishes fairly strict requirements for the subjects involved in personal data processing. However, these requirements are not always detailed enough. Article 24 of the Regulation requires the data controller to apply measures of organizational and technical nature to ensure data processing in accordance with the Regulation[5].

Such technical and organizational measures are not expressly mentioned in the Regulation, there are only general guidelines as to what these measures can be. For example, such a measure as pseudonymization is mentioned in Article 25 of the Regulation[6]. Thus, a significant administrative and financial burden is imposed on companies and organizations, caused by the need to enforce suitable technical and organizational safeguards. The regulation also obliges to review and, if necessary, update such measures, as well as appoint an official responsible for the protection of personal data. It is important that to establish a greater level of personal data protection, the Regulation singles out in a separate category "sensitive" personal data. Such data include person's race and origin, political views and beliefs, membership in trade unions, health and sex life, genetic and biometric data. The processing of such data is generally prohibited by the Regulation, except for certain exceptions established in paragraph 2 of Article 9 of the Regulation[7]. In case of non-compliance with the requirements of the Regulation, the entities may face fines that vary depending on the severity of the violation and can reach up to 20 000 000 EUR or 4% of the company's total global revenue for the previous financial year, whichever is higher.

[1] Council Framework Decision No. 2008/977/JHA "On the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters. (2008, November). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977.

[2] Council Decision No. 2008/615/JHA "On the Stepping up of Cross-border Cooperation, Particularly in Combating Terrorism and Cross-border Crime". (2008, June). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008D0615.

[3] Council Framework Decision No. 2009/315/JHA "On the Organisation and Content of the Exchange of Information Extracted from the Criminal Record Between Member States". (2009, February). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009F0315.

[4] Regulation of the European Parliament and of the Council No. 2016/679 "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)". (2016, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[5] Ibidem, 2016.

[6] Ibidem, 2016.

[7] Ibidem, 2016.

After Ukraine became independent, the institute of personal data protection gradually began to form in Ukraine. Article 32 of the Constitution of Ukraine[1] declares the right of everyone to non-interference in his private life and prohibits usage of a person's confidential information without his consent[2]. Separate norms regarding personal data and the basic principles of their processing were later established in the Law of Ukraine "On Information". In particular, Article 2 of the law enshrines such a principle of information relations as security of person's private life[3]. Protection of personal data processed in the systems was regulated by the Law of Ukraine "On Protection of Information in Information and Communication Systems"[4]. The Law of Ukraine "On Access to Public Information" established a special legal regime for personal data contained in public information[5].

The main law regulating the personal data institute in Ukraine is the Law of Ukraine "On Protection of Personal Data", which was adopted in 2010[6]. This law was developed on the basis of the provisions of Directive 95/46/EC[7]. The law defines main concepts regarding personal data, such as personal data, processing of personal data, personal data subject, owner, manager, and recipient. The Law of Ukraine "On the Protection of Personal Data" is a fundamental act in the area of personal data protection in Ukraine, since only this law regulates relations related to personal data processing so thoroughly and comprehensively, establishes and defines the subject of these relations, rights, and obligations of personal data subjects, general requirements for processing personal data and measures to ensure personal data protection. It is to be noted that there is no definition of the concept of privacy in Ukrainian legislation, this concept is used only in relation to property relations (private property) in Art. 41 of the Constitution of Ukraine[8]. In general, this corresponds with the state of the EU legislation, where privacy also does not have a clear legal definition (Bryzhko & Pylypchuk, 2021).

Ukrainian researchers have analysed the provisions of the Law of Ukraine "On Protection of Personal Data", highlighting its drawbacks and inconsistencies. O.V. Hron & A.K. Pogorelenko (2018) point out that the Regulation enhanced several rights in relation to personal data, such as the right of the individual to be informed about data processing, which is exercised through providing consent; the right to demand deletion of the data and the right to prohibit data processing. The mentioned rights of data subject are not detailed enough in the Law of Ukraine "On Protection of Personal Data", which stipulates the need to revise the respective provisions of the law. In this regard, it is not clear from the provisions of the law how personal data can be transferred to competent bodies without individual's consent and there is a need to elaborate the definition of personal data subject's consent so that it becomes unambiguous and more specific in terms of informing the individual on operations with his data.

Another important point raised by researchers is the necessity to create a competent data protection authority with specific functions, such as control over compliance with data protection laws, improvement of Ukrainian legislation in the area and interaction with the EU data protection authorities (Pylypchuk & Bryzhko, 2017). Agreeing with this point, it is to be noted that currently the functions of such body are performed by the Ukrainian Parliament Commissioner for Human Rights, hereinafter – the Commissioner. Functions regarding data protection are not fully consistent with the nature of the constitutional and legal status of the Commissioner, whose constitutional function is parliamentary control over the observance of constitutional rights. It is illustrative that according to the Commissioner's 2022 annual report, only 7% of appeals to the Commissioner concern issues related to personal data (Report on the Observance and Protection…, 2022). Because of its complexity, data protection is an area that requires the attention of a specially designated body. Appointing the data protection authority is required under the Regulation and is a standard practice in the EU countries which began to form before the Regulation was adopted. For example, the German data protection act[9] passed in the land of Hesse in 1970 already envisaged the

[1] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
[2] Ibidem, 1996.
[3] Law of Ukraine No. 2657-XII "On Information". (1992, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2657-12#Text.
[4] Law of Ukraine No. 80/94-BP "On Protection of Information in Information and Communication Systems". (1994, July). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
[5] Law of Ukraine No. 2939-VI. "On Access to Public Information". (2011, January). Retrieved from https://zakon.rada.gov.ua/laws/show/2939-17#Text.
[6] Law of Ukraine No. 2297-VI "On Protection of Personal Data". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text.
[7] Directive of the European Parliament and of the Council No. 95/46/EC "On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data". (1995, October). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.
[8] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
[9] Law of the Hessen No. GVBI II 300-10 "Data Protection Act". (1970, October). Retrieved from https://starweb.hessen.de/cache/GVBL/1970/00041.pdf.

post of Data Protection Commissioner, who was independent of other bodies and had the power to oversee activities related to personal data. In addition to introducing an independent data protection body, it is suggested that this body is granted sufficient power to prevent data protection violations and impose fines.

As noted, the Law of Ukraine "On Personal Data Protection"[1] is based on Directive 95/46/EC[2], which was cancelled and replaced by the Regulation. In view of this, it cannot be considered fully compliant with current EU legislation. This concerns the conceptual and categorical apparatus, mechanisms for ensuring personal data protection, requirements for subjects to ensure personal data protection, responsibility for data breaches, establishment of specific types of sensitive personal data and legal regime for their protection, etc. This situation is not favourable for Ukraine at the state level, because according to Article 15 of the EU-Ukraine Association Agreement, Ukraine agreed to cooperate with the EU in order to meet the international and European data protection standards[3]. The inconsistency of domestic legislation may create difficulties on Ukraine's road to accession to the EU. Also, the inconsistency of national personal data protection legislation creates risks for Ukrainian companies focused on exporting goods and services to the EU. Since the Regulation has an extraterritorial effect, if personal data of data subjects from the EU is processed by Ukrainian companies, such companies risk being held liable by European data protection supervisory authorities for breaches of the Regulation.

Ukraine could use the examples of the countries with similar legal systems that have entered the EU in the 21st century to bring national data protection legislation in line with the European standards. Such countries already have the necessary experience in implementation of the Regulation to their national legislation. For example, Poland has updated its data protection law in 2018 and introduced the President of the Office of Personal Data Protection as a new data protection authority. Bulgaria took a similar approach by updating its Personal Data Protection Act, while Romania adopted a separate implementing law[4], which in essence repeats the provisions of the Regulation. Ukrainian lawmakers should take into account this experience when choosing the best way to integrate the provisions of the Regulation into Ukrainian law and develop an effective data protection model in harmony with the best standards and practices of the EU.

In this regard, it appears that Ukraine could use a complex approach similar to the one used by Poland. In particular, Poland has not only replaced its main data protection law, but also made extensive changes to its national legislation to cover different areas of the economy from a data protection standpoint. The 2019 GDPR Implementation Act[5] introduced changes to more than 160 acts concerning various areas, including labour, consumer protection and electronic communications. For example, the Polish Labour Code[6] was amended to establish specific cases when the employer can require personal data from a potential employee and the categories and scope of such personal data. The code provides the candidate for employment with a right to refuse to provide personal data to the employer or withdraw consent to personal data processing. Ukrainian legislation needs a similar complex update, as it contains provisions regarding data protection in various laws apart from the Law of Ukraine "On Personal Data Protection"[7], for example, the Labour Code of Ukraine[8], the Law of Ukraine "On Access to Public Information"[9] and others. Therefore, all Ukrainian legal acts need to be amended systematically to correspond with the provisions of the Regulation.

Bulgaria is another interesting example in terms of implementing the Regulation. This country also up-

[1] Law of Ukraine No. 2297-VI "On Protection of Personal Data". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text.

[2] Directive of the European Parliament and of the Council No. 95/46/EC "On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data". (1995, October). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.

[3] Association Agreement between the European Union and Ukraine. (June, 2014). Retrieved from https://www.kmu.gov.ua/en/yevropejska-integraciya/ugoda-pro-asociacyu.

[4] Law of Romania No. 190/2018 "On Measures for the Application of Regulation (EU) 2016/679 of the European Parliament and 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)". (July, 2018). Retrieved from https://platform.dataguidance.com/legal-research/law-no-1902018-implementing-general-data-protection-regulation-regulation-eu-2016679.

[5] Act of the Sejm of the Republic of Poland No. 730 "On Amending Certain Acts in Connection with Ensuring the Application of 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 Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation)". (2019, February). Retrieved from https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190000730.

[6] Labor Code of the Republic of Poland. (1974, June). Retrieved from https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19740240141/U/D19740141Lj.pdf.

[7] Law of Ukraine No. 2297-VI "On Protection of Personal Data". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text.

[8] Labor Code of Ukraine No. 322-VIII. (1971, June). Retrieved from https://zakon.rada.gov.ua/laws/show/322-08#Text.

[9] Law of Ukraine No. 2939-VI "On Access to Public Information". (2011, January). Retrieved from https://zakon.rada.gov.ua/laws/show/2939-17#Text.

dated its main data protection law in 2019[1]. Bulgarian lawmakers have introduced a stricter regulation of certain personal data aspects, in particular relating to copying identity documents such as identification cards and driving licences, prohibiting copying such documents without specific legal grounds. Another peculiarity of the Bulgarian approach to data protection is the introduction of the second supervisory authority in addition to the authority that existed before implementation of the Regulation. Consequently, Bulgaria has two data protection authorities: the Commission for Personal Data Protection (CPDP), which has general jurisdiction over data protection matters and the Inspectorate of the Supreme Judicial Council, which has special jurisdiction over data processing in the judicial system when such processing is performed to carry out justice. The Bulgarian experience may be useful for Ukraine in the context of harmonizing its legislation with the Regulation, in particular, the idea of a separate supervisory data protection body for the judicial system deserves attention.

An illustration of the opposite approach is Romania, which adopted law No. 190/2018[2] implementing the Regulation. The mentioned law contains a concise description of data protection requirements and mostly refers to the provisions of the Regulation. At the same time, Romanian data protection authorities are among the most active in the EU in imposing fines on the companies. Romania was ranked third among the EU by the number of imposed fines related to personal data processing for mas of 2022 (Legal and Communication Department, 2022). Such an approach does not appear to be optimal for Ukraine as it does not provide a sufficient level of legal certainty, which may cause unfair behaviour of the subjects that process personal data or supervise such activities.

Legal studies pay attention to the evolution of privacy in the global system of human rights, examining its nature and place in the system of human rights generations. T.O. Sofiyuk (2018) views privacy as a part of a more general category of informational rights, which include the right to correspondence, individuality, secrecy about health, freedom of information and informational sovereignty. The author delineates the notion of the right to privacy should not be viewed as a static concept, but should rather be applied as a dynamic concept that ensures the possibilities and mechanisms to protect rights. Considering the technological advancement and increasing risks to personal data, such opinion deserves attention and should be reflected in the Ukrainian legislation. S. Bulavina & T. Davydova (2018) view privacy as the right of the third generation which has fundamental nature and underline that it is closely connected with other rights, such as dignity and freedom of speech. An important conclusion drawn by the authors is that privacy right belongs to the third generation because of its collective nature, however, it began to establish before the rights of the third generation were enshrined in legal acts. T. Popovych & A. Shavarin (2019) express their own opinion on the rights to personal data, attributing them to the fourth generation along with other related virtual rights, such as confidentiality on the internet. B. Custers & G. Malgieri (2022) view data protection right through the prism of fundamental rights, pointing out that as a fundamental right, this right cannot be alienated or transferred from a person. These studies are of significant value for the reason that they help to track the process of evolution of the categories of privacy and data protection, find out their place in the system of human rights and establish their connection with other related rights.

Scientists investigate the impact of the Regulation on the internal processes and policies of the companies in the context of technical requirements, pointing out that the Regulation requires to implement privacy by design systems, which, in turn, need to be balanced from the view of achieving balance between data protection and functionality (Tikkinen-Piri *et al.,* 2018; Tamburri, 2019). Ch.J. Hoofnagle *et al.* (2019) state that the Regulation requires companies to approach data protection similarly to antitrust and anti-corruption laws and pay significant attention to developing technical and legal practices and procedures in compliance with the Regulation. Similar studies that investigate the nature of the Regulation and its practical implementation are essential to identify the best approaches to ensuring data protection (Kovaliv *et al.,* 2020). N. Mentukh & O. Shevchuk (2023) note that design of the updated information protection model should consider the establishment of a robust state policy for safeguarding information within electronic registries, aligning with the legal standards of the European Union. This includes the establishment of the Office of the Information Protection Commissioner and the incorporation of specialists in the field of personal data protection within enterprises, consistent with EU regulations. The author of this study agrees that it is of utmost importance to study best practices and ways to implement organizational and technical require-

[1] Law of the Bulgaria "Personal Data Protection Act". (2002, January). Retrieved from https://www.cpdp.bg/en/index.php?p=element&aid=1194.

[2] Law of Romania No. 190/2018 "On Measures for the Application of Regulation (EU) 2016/679 of the European Parliament and 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)". (July, 2018). Retrieved from https://platform.dataguidance.com/legal-research/law-no-1902018-implementing-general-data-protection-regulation-regulation-eu-2016679.

ments under the Regulation, and this issue certainly requires further research.

In their publications, Ukrainian researchers have analysed the process of formation of Ukrainian national legislation on personal data protection and its transformation to meet the European legal standards. V.M. Bryzhko & V.G. Pylypchuk (2021) provide a review of the stages of development of the Ukrainian data protection system, pointing out on the areas that require improvement, such as legal and organizational mechanisms, responsibility for violations and enforcement of liability for violations in data protection area. These recommendations are valuable because Ukrainian laws on personal data protection, in particular the Law of Ukraine "On Protection of Personal Data"[1], have still not been adapted to the EU standards in terms of main concepts, categories, principles, and mechanisms for protecting the rights of data subjects. Concerning the Law of Ukraine "On Protection of Personal Data"[2], there is an opinion that this law should be cancelled and replaced by the bill "On personal data flow and processing"[3] (Rizak, 2015). The author of this article does not support this opinion because the established approach at the level of the EU legislation puts an emphasis on protection of personal data. Such conclusion can be made by analysis of key European legal acts, such as Directive 95/46/EC[4], Convention No. 108[5] and the Regulation[6]. The full names of all these legal acts begin with the word "protection", accentuating that it is crucial to implement and maintain security measures to protect personal data. Ukraine's intent to join the EU stipulates the need for further research in this area, which could be based on the ideas proposed by the above authors, as well as analysis of current European legislation and practices regarding data protection.

Conclusions

The article examines the global experience of formation and development of personal data protection institute. The foundations of this institute were laid at the end of the 19th century with the introduction of the idea of privacy. During the following years, especially in the second half of the 20th and the beginning of the 21st century, the right to privacy and protection of personal data developed along with basic human rights, gained international recognition and were consolidated at the level of EU legislation. In the view of digitalization, the need to implement efficient means to protect personal data only increases, which determines the need to improve legal regulation.

The key legislative act regulating personal data protection in the EU currently is the Regulation. Ukrainian personal data protection legislation has historically tried to follow European standards, however, as of today, it is grounded on the outdated Directive 95/46/EC, which is no longer valid in the EU. Experience in implementation of the Regulation by countries with similar legal systems that recently entered the EU, such as Poland, Bulgaria, and Romania, could be used by Ukrainian lawmakers to choose the best model to implement the changes into national legislation. Compared to the legislation of these countries, Ukrainian national laws on personal data protection lack sufficient level of detail, definitions of key terms, concepts, and principles that are present in the European legislation. Another issue is the absence in Ukraine of a separate data protection authority with specific jurisdiction. The establishment of at least one data protection body is a common practice in the EU and is explicitly required under the Regulation.

Therefore, the legislation of Ukraine needs to be improved to ensure compliance with the current EU legislation. Mechanisms and possible ways of integrating relevant European norms and practices regarding personal data protection into Ukrainian legislation require further research.

Acknowledgements

None.

Conflict of Interest

None.

[1] Law of Ukraine No. 2297-VI "On Protection of Personal Data". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text.
[2] Ibidem, 2010.
[3] Draft Law of Ukraine No. 8153 "On Personal Data Protection". (2022, November). Retrieved from https://itd.rada.gov.ua/billInfo/Bills/Card/40707.
[4] Directive of the European Parliament and of the Council No. 95/46/EC "On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data". (1995, October). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.
[5] Convention Convention of the Council of Europe No. 108 "On the Protection of Individuals with Regard to Automated Processing of Personal Data". (1981, January). Retrieved from https://rm.coe.int/1680078b37.
[6] Regulation of the European Parliament and of the Council No. 2016/679 "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)". (2016, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

References

[1] Asiryan, S.R., & Aleksanyan, K.A. (2021). GDPR as a standard for personal data protection in the European Union. *Law and Society*, 6, 298-302. doi: 10.32842/2078-3736/2021.6.43.

[2] Bezugliy, D.S. (2018). Information security of Ukraine: An overview of recent trends. *Physical and Mathematical Education*, 2(16), 13-17. doi: 10.31110/2413-1571-2018-016-2-002.

[3] Bryzhko, V.M., & Pylypchuk, V.G. (2021). Security of personal data: Legal standards of the European Union and contemporary applied problems. *Information and Law*, 1(36), 17-28. doi: 10.37750/2616-6798.2021.1(36).238174.

[4] Bulavina, S., & Davydova, T. (2018). The right to privacy in the system of generations of human rights. *Historical and Legal Journal*, 1(13), 10-14.

[5] Custers, B., & Malgieri, G. (2022). Priceless data: Why the EU fundamental right to data protection is at odds with trade in personal data. *Computer Law & Security Review*, 45, article number 105683. doi: 10.1016/j.clsr.2022.105683.

[6] Hoofnagle, Ch.J., van der Sloot, B., & Borgesius, F.Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, 28(1), 65-98. doi: 10.1080/13600834.2019.1573501.

[7] Hron, O.V., & Pogorelenko, A.K. (2018). Problems of personal data protection in the context of modern communication. *Scientific Bulletin of the Uzhhorod National University. Series: International Economic Relations and World Economy*, 19(1), 102-108.

[8] Ivankiv, I.B. (2016). Distinctive features of third generation human rights. *Scientific Notes of National University of Kyiv-Mohyla Academy. Legal Sciences*, 181, 54-57.

[9] Kovaliv, M., Yaremko, V., & Holovach, T. (2020). Protection of personal data as a component of information security. *Social & Legal Studios*, 1(7), 47-52. doi: 10.32518/2617-4162-2020-1-47-52.

[10] Kozyubra, M.I. (2015). Law and man: Lines of interrelationships and development trends. *Scientific Notes of National University of Kyiv-Mohyla Academy. Legal Sciences*, 168, 3-9.

[11] Legal and Communication Department. (2022). *European Fines Top*. Retrieved from https://www.dataprotection.ro/index.jsp?page=Comunicat Presa 10 01 2022&lang=en.

[12] Mentukh, N., & Shevchuk, O. (2023). Protection of information in electronic registers: Comparative and legal aspect. *Law, Policy and Security*, 1(1), 4-17.

[13] Nazimko, E.S., Malakhovska, I.B., & Ponomaryova, T.I. (2022). Legal regulation of personal data protection in electronic communication networks. *Legal Novels*, 18, 169-175. doi: 10.32847/ln.2022.18.25.

[14] Novoitenko, I.V., & Malynovskyi, V.V. (2020). Protection of personal data as a business trend. *Intellect XXI*, 3, 65-68. doi: 10.32782/2415-8801/2020-3.13.

[15] Popovych, T. (2021). The right of a person to protect personal data on the Internet: Theoretical and legal aspects. *Analytical and Comparative Jurisprudence*, 2, 51-54. doi: 10.24144/2788-6018.2021.02.9.

[16] Popovych, T., & Shavarin, A. (2019). Essential fulfilment of the fourth generation of human rights. *Entrepreneurship, Economy and Law*, 12, 266-271. doi: 10.32849/2663-5313/2019.12.49.

[17] Pylypchuk, V.G., & Bryzhko, V.M. (2017). Reform and development of the personal data protection system in Ukraine. *Information and Law*, 3(22), 5-21. doi: 10.37750/2616-6798.2017.3(22).273029.

[18] Report on the observance and protection of human and civil rights and freedoms in Ukraine in 2022. (2023). Retrieved from https://ombudsman.gov.ua/report-2022/en/.

[19] Rizak, M.V. (2015). The creation of a real legal mechanism for the protection of personal data as a necessary element of guaranteeing the inviolability of a person's private life in the conditions of the formation of an information society in Ukraine. *Scientific Bulletin of the Uzhhorod National University. Series: Law*, 2(35), 190-193.

[20] Roth, E. (2022). *Meta fined $276 million over Facebook data leak involving more than 533 million users*. Retrieved from https://www.theverge.com/2022/11/28/23481786/meta-fine-facebook-data-leak-ireland-dpc-gdpr.

[21] Saglam, R.M., Nurse, J.R.C., & Hodges, D. (2022). Personal information: Perceptions, types and evolution. *Journal of Information Security and Applications*, 66, article number 103163. doi: 10.1016/j.jisa.2022.103163.

[22] Sofiyuk, T.O. (2018). The right to protection of personal data in the system of generations of human rights. *Dictum Factum*, 2, 13-17.

[23] Solove, D.J. (2002). Conceptualizing privacy. *California Law Review*, 90, 1087-1156.

[24] Tamburri, D.A. (2019). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems*, 91, article number 101469. doi: 10.1016/j.is.2019.101469.

[25] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134-153. doi: 10.1016/j.clsr.2017.05.015.
[26] Warren, S.D., & Brandeis, L.D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193-220.

Становлення інституту захисту персональних даних і досвід його впровадження в країнах ЄС

Богдан Якименко
Аспірант
Київський міжнародний університет
03179, вул. Львівська, 49, м. Київ, Україна
https://orcid.org/0009-0008-7704-2934

■ **Анотація.** Розвиток у сучасному світі цифрових технологій призвів до розширення втручання в приватне життя людини та збільшення кількості випадків порушень прав людини, що стосуються приватного життя. Законодавство України не відповідає сучасним тенденціям і стандартам Європейського Союзу в цій сфері та потребує оновлення. Метою статті є дослідження розвитку інституту захисту персональних даних у світі для виявлення шляхів адаптації національного законодавства до сучасних стандартів захисту персональних даних на рівні ЄС. Для проведення дослідження використано такі наукові методи: індуктивний, дедуктивний, діалектичний, аналізу й синтезу, порівняльно-правовий, історико-правовий. З'ясовано, що інститут захисту персональних даних пройшов тривалий шлях розвитку від окремих понять і концепцій до структурованої сукупності стандартів й інструментів, законодавчо закріплених на рівні ЄС. Відмітними особливостями такого розвитку є прийняття нових нормативно-правових актів, а також дедалі жорсткіше та комплексне регулювання питань, пов'язаних з обробкою та використанням персональних даних. У цьому контексті постає необхідність удосконалення та адаптації національного законодавства до стандартів ЄС. Українське законодавство про захист персональних даних, попри те, що історично вдосконалювалося відповідно до європейських стандартів, станом на 2023 рік ґрунтується на застарілій Директиві 95/46/ЄС, що вже не діє в ЄС. Порівняно з правовими системами сусідніх країн – Польщі, Болгарії та Румунії, українське законодавство про захист персональних даних не лише поступається, а й істотно відстає за рівнем деталізації, визначення ключових термінів і принципів. Результати дослідження може бути використано під час законотворчої роботи, зокрема під час розроблення нового проєкту базового закону у сфері захисту персональних даних і для подальшого дослідження шляхів удосконалення законодавства України й інших кандидатів на членство в Європейському Союзі у сфері захисту персональних даних

■ **Ключові слова:** права людини; приватність; особисте життя; сімейне життя; обробка персональних даних; Загальний регламент про захист даних