DOI: https://doi.org/10.30525/2256-0742/2022-8-4-40-49

ABOUT DATA PROTECTION STANDARDS AND INTELLECTUAL PROPERTY REGULATION IN THE DIGITAL ECONOMY: KEY ISSUES FOR UKRAINE

Tetiana Voloshanivska[1], Liudmyla Yankova[2], Oleksandr Tarasenko[3]

Abstract. Changes that are constantly taking place in the digital economy cause increasing instability of legislation in the field of data protection and security. For example, in Ukraine, under martial law, there is an urgent need to adapt the legal regulation to European data protection standards (in terms of personal data processing). First of all, the correlation between EU law, national law of the EU Member States and national legislation of the EU candidate countries results in the principle of direct effect of EU law. In addition, EU data protection law has become an essential source for EU Member States in regulating artificial intelligence (AI), e-commerce and the Internet of Things (IoT). The article considers the specific topic of the conditions of approximation of international norms and legislation of Ukraine to EU law, trying to answer the questions of personal data protection in the conditions of martial law that have arisen. This work is based on a comparative analysis of the General Data Protection Regulation 2016/679 and internal data protection rules in Ukraine. At present, the research purpose of the article is to reveal the fact that data protection is a specific category of procedural law based on the principles of intellectual property law regarding data access rights and data ownership rights in the digital economy.

Key words: data protection standards, digital economy, General Data Protection Regulation, information security, intellectual property (IP), personal data.

JEL Classification: G14, O34

1. Introduction

At present, the research purpose of the article is to reveal the fact that data protection is a specific category of procedural law based on the principles of intellectual property law regarding data access rights and data ownership rights in the digital economy.

In his futuristic opinion Guido Noto la Diega states that: "One may naively believe that your own phone is your own property. It is not. The phone belongs to the copyright holders for the code that runs in it, the manufacturers for its design, the patents for how it works, and the trademarks not only for the logos but also for things like the way it "swipes". What happens when embedded software and other IP-protected digital content is no longer an exclusive feature of computers and phones? What happens when patented things and closed systems are everywhere: in the bedroom, in the bathroom, in the body? Our behaviour becomes severely constrained by the de facto, legal and technical control that IoT companies retain over their Things – and which we consequently lose. We have become digital tenants, not owning or controlling any of the objects around us and the data about us. To the point where we can say that we no longer own: we are owned." (Guido Noto la Diega, 2022)

One way or another, it can be argued that we are still the owners of personal data. Although data protection legislation is very young, many data protection rules are universal and based on common values.

Florent Thouvenin and Aurelia Tamò-Larrieux note that "the literature on data ownership as a property right is divided: While some authors argue

[1] Odessa State University of Internal Affairs, Ukraine *(corresponding author)*
E-mail: t.voloshanivska@gmail.com
ORCID: https://orcid.org/0000-0002-1060-5412
[2] Interregional Academy of Personnel Management, Ukraine
E-mail: sky_2012@ukr.net
ORCID: https://orcid.org/0000-0003-0650-1087
[3] Department of Science and Innovation of the Board of Education, Science and Sports of the Ministry of Internal Affairs of Ukraine, Ukraine
E-mail: a.s.7.tarasenko@gmail.com
ORCID: https://orcid.org/0000-0003-0369-520X

that the existing regulatory system is inadequate to protect individuals in the digital economy, others consider it adequate (or adequate enough) and therefore discourage the establishment of data ownership rights. The first group of authors highlights the potential threats of big data and global trade to the protection of fundamental rights and freedoms of European citizens. In their view, data ownership can help mitigate some of the negative effects of the digital economy." (Florent Thouvenin, Aurelia Tamò-Larrieux)

Thor Berger and Carl Benedikt Frey noted that "digital transformation has impacted society on various levels, mainly on the economic level. The automation of various business operations, such as increasing production, reducing costs and improving operational structures, has given businesses a huge advantage in terms of sustainability. The digital economy has offered new opportunities for business and the labour market. The wide and diverse range of services offered by the digital economy has created numerous new jobs, which has impacted both the business and labour markets. The digital economy uses vast amounts of data and information for its operational structure, which has helped to deliver the same public services such as healthcare and education more efficiently. A sustainable digital economy has also impacted social governance mechanisms by improving the quality of interaction between governments and citizens." (Thor Berger, Carl Benedikt Frey, 2017)

It is noteworthy that the regulatory framework for the digital economy has begun to influence and replace national legislation, which raises some concerns.

The application of the General Data Protection Regulation 2016/679[1] (hereinafter – GDPR) by the EU Member States and candidate countries for accession to the EU can be considered a problematic issue of procedural law.

In the EU, the procedural rules for the protection of personal data are set out in the following documents:
– Regulation (EU) 2016/679 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 and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)[2];
– Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (Regulation (EU) 2016/794);
– Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Regulation (EU) 2018/1725);
– Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust) replacing and repealing Council Decision 2002/187/JHA (Directive (EU) 2016/680);
– Directive (EU) 2016/680 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 by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or for the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA (Directive (EU) 2016/680);
– Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and on the protection of privacy in the electronic communications sector (Privacy and Electronic Communications Directive) (Directive 2002/58/EC), etc.

It is striking that in the regulations and directives the data protection provisions mainly concern the control of the transposition of Member States' legislation.

2. European Digital Single Market and legal mechanisms of data protection in the EU and Ukraine

In this study, the authors agree with Endre Győző Szabó, Vice President of the National Authority for Data Protection and Freedom of Information of Hungary, that "GDPR, as a legal act of the European Union aimed at the highest level of harmonization, requires Member States to establish independent data protection authorities to protect the rights of individuals and ensure the free flow of personal data within the Union." (Endre Győző Szabó, 2018)

Under the GDPR, a person has following rights:
a) the right of access to stored personal data, art. 15 GDPR;

[1] The GDPR came into force on the 25th of May, 2018 and repealed the Data Protection Directive 95/46/EC. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[2] Ibid.

b) if incorrect personal data are processed, there is a right to rectification, Art. 16 GDPR;
c) under legal conditions, there is a right to demand erasure or restriction of processing and the right to object to processing, Art. 17, 18, 21 GDPR;
d) in case of consenting to data processing or signing a data processing contract and the data processing is carried out by automated means, there is a right to data portability, Art. 20 GDPR;
e) the right to lodge a complaint with the competent state officer for data protection, Art. 77 GDPR[3].

The revocation does not affect the lawfulness of data processing carried out on the basis of contracts or letters of consent before the revocation.

By Florent Thouvenin, Aurelia Tamò-Larrieux "While the GDPR certainly facilitates the free flow of personal data within the EU by establishing a (relatively 16) uniform regime across all EU Member States, it also imposes significant restrictions on the processing of personal data and thereby limits the free development and introduction of digital goods and services. Although innovation remains possible, the GDPR has at least increased its cost, sometimes to a level that makes the introduction of innovative digital goods and services economically unfeasible. There are many flexible provisions in the GDPR that allow Member States to "introduce national provisions to further clarify the application of the rules" of the GDPR, to introduce "sectoral laws in areas requiring more specific provisions", or to "clarify the rules, including for the processing of special categories of data."[4]

For comparison, these rights are also contained in the provisions of Ukrainian laws related to the right to privacy. The legal basis for data protection in Ukraine is determined by the national norms establishing the right to information.

The right to information is a constitutional principle and is based on international documents: Universal Declaration of Human Rights of the United Nations (1948), International Covenant on Civil and Political Rights, Convention for the Protection of Human Rights and Fundamental Freedoms (1950).

The Constitution of Ukraine of 28 June, 1996[5] guarantees the right to information in provisions of these articles and following its provisions the right to information includes the right to open data and information on public administration activities and the right to information about the status of environmental security, etc.

As it is known, "the Digital Single Market strategy aims to provide better access for consumers and businesses to online goods and services across Europe, for example, by removing barriers to cross-border e-commerce and access to online content, while enhancing consumer protection". An environment in which digital networks and services can thrive The Digital Single Market aims to create the right environment for digital networks and services by providing high-speed, secure and reliable infrastructure and services, supported by an appropriate regulatory environment. Key issues are cybersecurity, data protection/e-privacy, and fairness and transparency of online platforms. The Digital Single Market Strategy aims to maximise the growth potential of the European digital economy so that every European can fully benefit from it – in particular by developing digital skills, which are essential for an inclusive digital society."[6]

Similarly, Thomas Cottier and Michelangelo Temmerman write: "The elevation of intellectual property to the realm of international law, in an attempt to coordinate and even harmonize different legal orders in order to serve a transnational and increasingly globalized economy, has resulted in transparency taking on additional features that go beyond the classic principles of publicity and accessibility of the law." (Cottier, Thomas, Temmerman, Michelangelo, 2010)

The basic law on personal data protection is the Law of Ukraine "On Personal Data Protection" No. 2297-VI dated June 1, 2010 (hereinafter – the PDP Law) and three by-laws approved by the Order of the Ukrainian Parliament Commissioner for Human Rights No. 1/02-14 dated January 8, 2014 "On Approval of Documents in the Field of Personal Data Protection"[7]:
– typical procedure for personal data processing;
– the procedure for the Human Rights Commissioner of the Verkhovna Rada of Ukraine to monitor compliance with the legislation on the protection of personal data;
– the procedure for notifying the Ukrainian Parliament Commissioner for Human Rights about the processing of personal data that poses a particular risk to the rights and freedoms of personal data subjects, about the structural unit or responsible person who organizes the work related to the protection of personal data during their processing, as well as the publication of this information.

[3] Op cit.
[4] Op cit, p. 320
[5] Constitution of Ukraine. Available at: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
[6] For more about the Digital Single Market see the Report of the Directorate-General 'Communications Networks, Content and Technology. Available at: https://ec.europa.eu/digital-singlemarket/en/digital-single-market)
[7] The Decree of the Commissioner of the Verkhovna Rada of Ukraine for Human Rights "On approval of documents in the field of personal data protection. Available at: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

The Law of Ukraine "On Personal Data Protection" regulates legal relations related to the protection and processing of personal data. The Law regulates legal relations related to the protection and processing of personal data, aims to protect the fundamental rights and freedoms of man and citizen, in particular the right to privacy, in connection with the processing of personal data.

The PDP Law applies to the processing of personal data, which is carried out in whole or in part by automated means, as well as to the processing of personal data contained in the file or intended to be included in the file, using non-automated means.

1. The subjects of relations related to personal data are:
– the subject of personal data;
– owner of personal data;
– personal data administrator;
– third party;
– Commissioner of the Verkhovna Rada of Ukraine on human rights.

2. The owner or administrator of personal data may be enterprises, institutions and organizations of all forms of ownership, public authorities or local self-government bodies, individual entrepreneurs who process personal data in accordance with the law.

3. The administrator of personal data, the owner of which is a public authority or local self-government body, except for these bodies, can only be an enterprise of state or communal ownership.

4. The personal data owner may entrust the processing of personal data to the personal data controller in accordance with the agreement concluded in writing.

5. The personal data controller may process personal data only for the purpose and to the extent specified in the contract.

It should be noted that the GDPR and the PDP Law have many similarities in principles:
– lawfulness;
– fairness;
– transparency;
– data minimization;
– purpose limitations;
– accountability;
– storage limitations;
– data integrity;
– confidentiality, etc.

The next similarities with GDPR and the PDP Law, that need to be mentioned in this paper, are:
– legal grounds of data processing and of "legitimate interests";
– unified and extended GDPR-like terminology;
– updated concept of sensitive data with a comprehensive list of legal grounds for processing such data;
– data protection rules about video surveillance;
– data protection rules concerning the use of tracking technologies in electronic communications;
– requirements for data processing agreements, etc.

Comparing the GDPR and the Law of Ukraine "On Personal Data Protection", it should be noted that the objects of protection in both documents are personal data.[8]

In parallel and in comparison to the GDPR, the PDP Law starts with the definition of personal data, while the GDPR mostly indicates the relationship between data subjects and data.

In the PDP Law, "personal data" may be referred to as confidential information about a person by law or by the person concerned. Personal data related to the exercise of official or official powers by a person authorized to perform the functions of the state or local self-government is not confidential information.

The Ukrainian act provides for a specific qualification of personal data specified in the declaration of a person authorized to perform the functions of the state or local self-government, which is submitted in the form determined in accordance with the Law of Ukraine "On Prevention of Corruption", does not belong to information with restricted access, except for information specified by the Law of Ukraine "On Prevention of Corruption".

Supplement Article 2 of the PDP Law with instructions that:
– personal data base – a named set of ordered personal data in electronic form and/or in the form of personal data files;
– the owner of personal data is a natural or legal person who determines the purpose of processing personal data, establishes the composition of these data and procedures for their processing, unless otherwise provided by law;
– consent of the subject of personal data is a voluntary expression of will of an individual (subject to his/her awareness) to grant permission to process his/her personal data in accordance with the specified purpose of their processing, expressed in writing or in a form that allows to conclude that it has been granted.

The key issue of this provision is that "in the field of e-commerce, the consent of the personal data subject may be provided during registration in the information and communication system of the e-commerce entity by marking the consent to the processing of his personal data in accordance with the stated purpose of their processing, provided that such system does not create opportunities for processing personal data before the marking":
– depersonalization of personal data – deletion of information that can directly or indirectly identify a person;

[8] For additional information about GDPR. Available at: https://www.itgovernance.co.uk/articles-of-the-gdpr

– file – any structured personal data accessible according to certain criteria, regardless of whether such data is centralized, decentralized or separated by functional or geographical principle;
– processing of personal data – any action or set of actions, such as collection, registration, accumulation, storage, adaptation, modification, updating, use and dissemination (distribution, sale, transfer), depersonalization, destruction of personal data, in particular with the use of information (automated) systems;
– the recipient is a natural or legal person to whom personal data is provided, in particular a third party;
– personal data – information or a set of information about a natural person who is identified or can be specifically identified;
– personal data manager – a natural or legal person who is authorized by the owner of personal data or by law to process this data on behalf of the owner;
– the subject of personal data is a natural person whose personal data is processed;
– third party – any person, except for the subject of personal data, the owner or manager of personal data and the Ukrainian Parliament Commissioner for Human Rights, to whom the owner or manager of personal data transfers personal data.

Data subjects are data processors and controllers, organizations that have the right to possess and process personal data, which are obliged to keep records of the personal data they possess, as well as their processing activities.

The data controller is a natural or legal person who, alone or jointly with others, determines the purposes or means of processing personal data (e.g., names, e-mail addresses, etc.). The controller also checks whether the legal conditions for protecting the rights of data subjects are met.

Unlike the Ukrainian law, the notification of the personal data subject about the fact of data processing is regulated in detail in the GDPR.

Although the GDPR understands that the required level of expertise should be determined, in particular, in light of the data processing operations carried out and the protection required for the controller.

The data controller is a natural or legal person who, alone or jointly with others, determines the purposes or means of processing personal data (e.g., names, e-mail addresses, etc.). The controller checks whether the legal conditions for protecting the rights of data subjects are met. Data processors are required to keep records of the personal data they hold and their processing activities.

At the same time, Ukraine lacks a system of justice in the field of personal data protection that would demonstrate how court decisions are made in the digital era. In contrast, in the EU, the sphere of data protection regulation is associated with well-known data protection cases. For example, in the Facebook/WhatsApp merger case, the European Commission decided for the first time in its history to impose fines on a company for providing incorrect or misleading information since the Merger Regulation of 2004 entered into force.[9] The Commission's previous decisions on this matter were taken under the 1989 Merger Regulation in accordance with other fining rules.[10]

The case Weltimmo s. r. o. vs. Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C 230/14[11], shows that companies should take into consideration that in case of doing business in multiple EU Member States, data protection legislation could be closer to the targeting customers. The request for the preliminary ruling has been made in proceedings between Weltimmo s. r. o. ('Weltimmo'), a company which has its registered office in Slovakia, and the Nemzeti Adatvédelmi és Információszabadság Hatóság (national data protection and freedom of information authority; "Hungarian data protection authority") concerning a fine imposed by the latter for infringement of Law CXII of 2011 on the right to self-determination as regards information and freedom of information (az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény; the Law "On Information"), which transposed Directive 95/46 into Hungarian law. When considering collecting personal data in a new jurisdiction, it is worth considering conducting a privacy impact assessment, as recommended in the proposed EU Data Protection Regulation, to ensure that local rights are not infringed; but if there is significant presence in any EU Member State or a particular nationality is targeted by your activities, local consultation should be taken. In its judgment (case C-230/14 of 1 October 2015), the European Court of Justice demonstrated the ability of the national regulators of the EU Member States in the field of personal data protection to resolve issues related to organizations located outside their borders.

3. Rights of access to data, possession of personal data and their processing

According to the Law PDP, "It is prohibited to collect, store, use and disseminate confidential information about a person without his/her consent,

[9] Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation). Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32004R0139

[10] For more see https://ec.europa.eu/commission/presscorner/detail/pl/IP_17_1369

[11] Case C 230/14, REQUEST for a preliminary ruling under Article 267 TFEU from the Kúria (Hungary), made by decision of 22 April 2014, received at the Court on 12 May 2014, in the proceedings Weltimmo s. r. o. vs Nemzeti Adatvédelmi és Információszabadság Hatóság.

except in cases determined by law, and only in the interests of national security, economic welfare and human rights (Article 32 of the Constitution of Ukraine). Confidential information about an individual includes, in particular, data on his/her nationality, education, marital status, religious beliefs, health status, as well as address, date and place of birth (Article 11 of the Law of Ukraine No. 2657-XII "On Information" dated 2 October 1992)." (The Law of Ukraine "On information")

Information about an individual (personal data) – information or a set of information about an individual who is identified or can be specifically identified. Article 32 of the Constitution of Ukraine stipulates that it is not allowed to collect, store, use and disseminate confidential information about a person without his/her consent, except in cases determined by law, and only in the interests of national security, economic welfare and human rights.

Information on the receipt by an individual of budget funds, state or municipal property in any form, structure, principles of formation and amount of remuneration, remuneration, additional benefits of the head, deputy head of a legal entity of public law, manager, deputy does not belong to information with restricted access. Head, member of the supervisory board of a state or municipal enterprise or a state or municipal organization aimed at making a profit, a person who permanently or temporarily holds the position of a member of the executive body or is a member of the supervisory board of an economic entity in the authorized capital of which more than 50 percent of shares (stakes, shares) directly or indirectly belong to the state and/or territorial community, except as provided for in Article 6 of the Law of Ukraine "On Access to Public Information". (The Law of Ukraine "On Access to Public Information")

The consent of the subject to the processing of his personal data must be voluntary and informed. The consent may be given by the subject in written or electronic form, which makes it possible to conclude that it has been given. Documents (information) confirming the consent of the subject to the processing of his personal data are stored by the owner during the processing of such data:

– in the absence of consent, the transfer of personal data is allowed provided that it is provided for in part 16 of Article 2297 of the Law No 2297 and is conditioned by the interests of national security, economic welfare and human rights;

– the procedure for access of third parties to personal data is determined by the terms of the consent of the personal data subject provided by the owner of personal data to the processing of this data, or in accordance with the requirements of the law (Article 16 of Law No 2297);

– personal data are objects of protection (Article 5 of Law No 2297), information or their aggregate about a natural person who is identified or can be specifically identified (Article 2 of Law No 2297). Information about a natural person is confidential, and access to confidential information is limited.

It is noteworthy that in the conditions of martial law, according to the authors, there are several exceptions to the above rules concerning the activities of state military administrations and other legal entities, namely:

– limits of the right to information in times of martial law;

– limits for the sake of national security, sovereignty and territorial integrity;

– limits for the sake of the necessity to respect individual and public interest;

– limits in criticism and opinion expression;

– limits in interference in the work of public authorities.

In the European Union, the processing of personal data (collection, storage and transfer to third parties) is carried out exclusively on the basis of the express consent of the legal representative or the subject of personal data, that is, in accordance with Art. 6 Paragraph 1 Letters a-f GDPR, which defines it as:

"1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to the conclusion of the contract;

(c) the processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) the processing is necessary for the protection of the vital interests of the data subject or another natural person;

(e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) the processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of the personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."[12]

[12] Op cit.

Ukrainian legislative acts describe these situations in a slightly different way.

According to the Decision of the Constitutional Court of Ukraine No. 2-рп/2012 dated January 20, 2012, information about personal and family life of a person (personal data about him/her) is any information or a set of information about an individual who is identified or can be specifically identified, namely: nationality, education, marital status, religious beliefs, health status, property status, address, date and place of birth, place of residence and stay, etc. data on personal property and non-property relations of this person with other persons, including family members, as well as information on events and phenomena that have taken place or are taking place in everyday, intimate, social, professional, business and other spheres of a person's life, except for information related to the exercise of powers by a person who holds a position related to the performance of functions of the state or local self-government bodies.

Such information about a person and his/her family members is confidential and may be disseminated only with his/her consent, except in cases specified by law, and only in the interests of national security, economic welfare and human rights.

The list of personal data recognized as confidential information is not exhaustive.

In the Law "On Personal Data Protection" the processing of personal data means any action or set of actions, such as collection, registration, accumulation, storage, adaptation, modification, updating, use and dissemination (distribution, sale, transfer), depersonalization, destruction of personal data, including with the use of information (automated) systems.

The processing of personal data is carried out in an open and transparent manner, using means and in a manner consistent with the defined purposes of such processing.

Accordingly, the subjects of relations related to personal data are:

– subject of personal data is a natural person whose personal data is processed;

– the owner of personal data is a natural or legal person who determines the purpose of personal data processing, establishes the composition of this data and the procedures for their processing, unless otherwise specified by law;

– personal data controller – a natural or legal person who is authorized by the controller of personal data or by law to process this data on behalf of the controller;

– third party – any person, except for the subject of personal data, the owner or manager of personal data and the Ukrainian Parliament Commissioner for Human Rights, to whom the owner or manager of personal data transfers personal data;

The Verkhovna Rada Commissioner for Human Rights is an official who, independently of other state bodies and officials, exercises parliamentary control over the observance of constitutional rights and freedoms of man and citizen.

The owner or administrator of personal data may be enterprises, institutions and organizations of all forms of ownership, public authorities or local governments, individual entrepreneurs who process personal data in accordance with the law (public authority, bank within the framework of contractual relations, supermarket, if a cone card is issued, etc.).

For this purpose, the grounds for processing personal data are defined:

– consent of the personal data subject to the processing of his personal data;

– permission to process personal data granted to the owner of personal data in accordance with the law solely for the exercise of his powers;

– conclusion and execution of a transaction to which the subject of personal data is a party or which is concluded in the interests of the subject of personal data or for the implementation of measures preceding the conclusion of a transaction at the request of the subject of personal data;

– protection of the vital interests of the subject of personal data;

– the need to fulfill the obligation of the owner of personal data, which is provided by law;

– the need to protect the legitimate interests of the personal data controller or a third party to whom the personal data is transferred, unless the need to protect the fundamental rights and freedoms of the personal data subject in connection with the processing of his/her data prevails over such interests.

It is important to clarify how GDPR affects businesses in terms of regulating the protection, storage and disposal of sensitive digital documents.

At the same time, the GDPR adds several additional requirements to the existing requirements for the protection of personal data against unauthorized or unlawful processing and/or accidental loss and damage.

According to the GDPR, everyone whose personal data is stored by an organization has the right to be forgotten, the right to data portability and the right to object.[13]

An individual should know:

– responsibilities when it comes to hard copy personal data processing, storage and destruction;

– rights under GDPR (incl. demands to report GDPR breaches to the regulator, requirements on demonstrating compliance to the regulator).

According to the article 11 of the PDP Law "the subject of personal data has the right to:

[13] For more see https://gdpr-info.eu/

– know about the sources of collection, location of their personal data, the purpose of their processing, location or place of residence (stay) of the owner or administrator of personal data or to give an appropriate order to obtain this information to authorized persons, except in cases established by law;
– receive information about the conditions for granting access to personal data, in particular information about third parties to whom his personal data is transferred;
– access to his/her personal data;
– receive no later than thirty calendar days from the date of receipt of the request, except in cases provided by law, a response on whether his personal data are processed, as well as to receive the content of these personal data;
– submit a motivated request to the personal data controller with an objection to the processing of their personal data;
– make a reasoned request to change or destroy their personal data by any owner and administrator of personal data, if these data are processed illegally or are unreliable;
– protect his/her personal data from illegal processing and accidental loss, destruction, damage due to intentional concealment, failure to provide or untimely provision of data, as well as protection from providing information that is unreliable or dishonors the honor, dignity and business reputation of a physical person individuals;
– file complaints about the processing of his/her personal data with the Commissioner or the Court;
– apply legal remedies in case of violation of the legislation on the protection of personal data;
– enter a reservation regarding the limitation of the right to process his/her personal data when giving consent;
– withdraw consent to the processing of personal data;
– know the mechanism of automatic processing of personal data;
– protect against an automated decision that has legal consequences for him."

It is noteworthy that there are no additional procedural rules related to the protection of data protection rights. On the contrary, the fines for violations of these provisions differ in the laws depending on the type of violation and the severity of the violation. The PDP Law proposes to establish the following fines: for individuals – from UAH 10,000 to UAH 300,000, and for legal entities – from UAH 30,000 or 0.05 percent of the total annual turnover to 5 percent of the total annual turnover (but not less than UAH 300,000).[14]

This is provided by Article 8 of the Law of Ukraine "On Personal Data Protection":

"The subject of personal data has the right to receive any information about himself/herself from any subject of relations related to personal data, subject to the provision of information about the surname, name and patronymic, place of residence (place of stay) and details of the document certifying the individual who submits the request, except in cases established by law. The subject of personal data has the right to submit a reasoned request to the owner of personal data to prohibit the processing of his personal data (part thereof) and/or change their composition / content. Such request shall be considered by the controller within 10 days from the date of its receipt.

If, as a result of consideration of such a request, it is established that the personal data of the subject (part of it) is processed illegally, the controller is obliged to stop processing the personal data of the subject (part of it) and notify the subject of personal data. If, as a result of consideration of such a request, it is established that the personal data of the subject (part of it) is unreliable, the owner is obliged to stop processing the personal data of the subject (part of it) and/or change their composition / content and notify the subject of personal data. In case of impossibility to satisfy the request, the personal data subject is provided with a reasoned answer about the absence of grounds for its satisfaction."

Taking into account the presented legislative approach, the appeal against the failure to satisfy the request or motivated demand of individuals to the Commissioner or to the court with the provision of supporting materials (screenshots or photos, copies of the request or motivated demand and the contested response, etc.) is controlled by procedural norms.

GDPR has a broader legal framework for data management compared to the Law of Ukraine "On Personal Data Protection".

The publication of personal data and performance of a task in the public interest based on norms resulting from Art. 6 Paragraph 1 Point (e) and Paragraph 3 of GDPR in conjunction with special legal norms, e.g., arising from the data protection laws of EU member states. Art. 6 Paragraph 3 GDPR stipulates that:

"The grounds for the processing referred to in points (c) and (e) of Paragraph 1 the following are:

1. Union law.

2. The legislation of the Member State to which the controller is subordinated.

[14] For more see https://yur-gazeta.com/dumka-eksperta/chi-realno-prityagti-do-vidpovidalnosti-za-porushennya-zahistu-personalnih-danih-v-ukrayini.html

The purpose of the processing must be specified in that legal basis or, in the case of processing referred to in Point (e) of Paragraph 1, must be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

This legal framework may contain specific provisions to tailor the application of the rules of this Regulation, in particular: general conditions governing the lawfulness of processing by the controller; types of data to be processed; data subjects concerned; subjects to whom and for what purpose personal data may be disclosed; purpose limitation; retention periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing, such as those relating to other specific processing situations as provided for in Chapter IX. Union or Member State legislation must be justified by an objective of public interest and be proportionate to the legitimate aim pursued."

4. Conclusions

In summary, it should be noted that in order to document the free movement of personal data and their processing, the GDPR is considered as a data protection legal framework for the protection of specific rights of individuals, albeit for candidate countries. The preliminary review has shown that the provisions set out in the GDPR and the PDP Law are quite similar. For Ukraine, given the function of personal data protection authorities, it is extremely important to use the experience of the European public sector in developing the free movement of data in the digital single market. Undoubtedly, the GDPR is a valuable source for improving the practice of data protection functions and influencing the system of protection of citizens' rights.

References:

Guido Noto la Diega (2022.) Internet of things and the law. Legal strategies for consumer-centric smart technologies, Routledge Research in the Law of Emerging Technologies, London and New York, 2022, p. 276. DOI: https://doi.org/10.4324/9780429468377

Florent Thouvenin, Aurelia Tamò-Larrieux. Data Ownership and Data Access Rights Meaningful Tools for Promoting the European Digital Single Market? in Burri, Mira. Big Data and Global Trade Law, Cambridge University Press, 2021. P. 321. DOI: https://doi.org/10.1017/9781108919234

Thor Berger & Carl Benedikt Frey (2017). Industrial renewal in the 21st century: evidence from US cities, Regional Studies, 51:3, 404–413. DOI: https://doi.org/10.1080/00343404.2015.1100288

The GDPR came into force on the 25th of May, 2018 and repealed the Data Protection Directive 95/46/EC. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0794

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32018R1725

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32018R1727

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

Endre Győző Szabó (2018). About specific issues of the GDPR of the European Union in Hungarian Yearbook of Interantional Law and European Law 2017, Eleven International Publishing, 2018 the Netherlands, p. 365.

Constitution of Ukraine. Available at: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

For more about the Digital Single Market see the Report of the Directorate-General 'Communications Networks, Content and Technology. Available at: https://ec.europa.eu/digital-singlemarket/en/digital-single-market)

Cottier, Thomas, Temmerman, Michelangelo (2010). Transparency and Intellectual Property Protection in International Law. DOI: https://doi.org/10.1017/CBO9781139108843.011

The Decree of the Commissioner of the Verkhovna Rada of Ukraine for Human Rights "On approval of documents in the field of personal data protection. Available at: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

The Law of Ukraine "On information". Available at: https://zakon.rada.gov.ua/laws/show/2657-12#Text

The Law of Ukraine "On Access to Public Information". Available at: https://zakon.rada.gov.ua/laws/show/2939-17#Text

Received on: 20th of September, 2022
Accepted on: 25th of October, 2022
Published on: 30th of November, 2022