LEGAL BASIS OF PERSONAL DATA PROTECTION IN UKRAINE AND GERMANY: ORGANIZATIONAL AND MANAGERIAL ASPECT

Bratasyuk Oksana

Annotation. *The author emphasizes that the European General Data Protection Regulation (GDPR) is effective. It applies directly to all member states of the European Union. However, there are exceptions where member states can also adopt their own rules for certain areas. German lawmakers have used these introductory provisions in the Federal Data Protection Act (BDSG) and adapted national data protection laws in accordance with the GDPR so that they can continue to exist.*

The system of federal data protection authorities in Germany is more complex than in other EU countries. In practice, this sometimes creates problems and indirectly becomes a competitive disadvantage for German companies. Although the introduction of the GDPR helped harmonize data protection rules across member states, regional differences still exist in Germany. Nevertheless, various instruments ensure better coordination between the data protection authorities of the individual federal states at the national level, as well as between the authorities in different EU member states at the European level, compared to the time before the GDPR came into force.

Keywords: *Germany, right to personal data protection, federal protection system, Stasi archives, data protection officer, GDPR.*

1. Introduction.

One of the negative consequences of the introduction of information and telecommunication technologies in all spheres of public life is the violation of important human rights, which is manifested in the illegal collection, use and dissemination of personal data, including on the Internet. Inadequate legislative protection and ineffective personal data protection mechanisms in this area have led to an increase in human rights violations. Respect for the right to privacy is the foundation of social justice and harmony. Therefore, to eliminate gaps in Ukrainian legislation, we propose to analyze the German experience.

2. Analysis of the recent studies and publications.

Many scientific works of both international and domestic researchers have been devoted to the issues of personal data protection in Germany: Gefenas, E., Lekstutiene, J., Lukaseviciene, V., Hartlev, M., Mourby, M., and Cathaoir, K.Ó. Gefenas, V., Kühling, Jürgen, Martini, Mario, Siehe Weichert, etc.

3. Purpose.

The purpose of the article is to analyze the legal experience of the State regulation of personal data protection in the Federal Republic of Germany with a view to improving the system of Ukrainian legislation.

4. Main material.

After a thorough systematic analysis of the foreign regulatory framework, identifying priorities and negative aspects, national legislation can be improved. According to D. Erdos (2021), the undisputed leader of European countries in the field of legal regulation and protection of personal data is the Federal Republic of Germany [8, p. 28].

Since the mid-twentieth century, Germany has begun to formulate legislation in the field of personal data protection. In 1970, the world's first regulatory act regulating the protection of personal data was adopted. According to B. Baran (B. Baran, K. Południak-Gierz (2017)), was proposed by the federal state of Hesse, and later supported by other federal states [5].

The Hessian government has drafted a bill on data protection in the field of administrative management, which defines two main objectives:

– first, to prevent interference with the private sphere of German citizens through new information technologies;

– secondly, to prevent changes in the distribution of executive powers in parliamentary bodies due to the emergence of an "information advantage" as provided for in the Constitution.

In 1977, a similar law was adopted at the federal level. Since then, German citizens have the right to make their own decisions regarding the disclosure of their personal data, and the protection of their rights in this matter is ensured by independent personal data protection commissioners elected by the parliaments of the states. We believe that in the context of informatization, specific legal acts play an important role in ensuring the rights of a person and a citizen to personal data protection and personal inviolability [1, p. 1].

In accordance with the provisions of the law, citizens personally decide on the disclosure of their personal data. The main idea and purpose of this legislative act is primarily to protect a person from attacks on the inviolability of his or her private life by manipulating his or her personal data. According to the German law, the purpose of personal data protection is "to prevent harm to the properly protected interests of the individual" [20, p. 41].

The 1977 Personal Data Protection Act does not apply to widely known or verbally transmitted information about a person, as well as data stored in special acts and files to which access is strictly limited. Data collected and processed for the purpose of further publication, display or disclosure by means of cinema, radio and the press are also not subject to protection. However, the law applies to the collection, processing and use of personal data collected by state federal bodies (no state regulation mechanisms) and non-governmental institutions if they process and use personal data for commercial or professional purposes [12, p. 262].

These standards apply to all NATO member states and contain some of the most important principles of regulation of public relations in the field of personal data protection, namely:

1) responsibility – the organization is responsible for the personal data under its control and must appoint one or more persons to monitor the compliance of the organization's behavior with legal principles;

2) determination of the purpose – the purpose of collecting information must be determined by the organization before the start of the information collection process;

3) consent – a mandatory condition for the collection, use or dissemination (disclosure) of personal data is the subject's awareness and consent to the collection of information about him or her, unless it is not appropriate;

4) limited collection – the collection of personal information should be limited to the purposes defined (identified) by the organization. Information may be collected only for fair and legitimate purposes;

5) restriction of use, dissemination, storage (personal information should be used only for the purpose of collection), unless the person agrees or it is required by law. Personal information should not be stored for longer than necessary to achieve the specified purpose;

6) accuracy – personal information must be accurate, complete and relevant to meet the purpose for which it was collected;

7) security – personal information must be protected by ensuring a level of security that meets the requirements of the "sensitivity" of the information;

8) openness – the organization must provide individuals with specific information about the organization's policy and practice of managing personal information;

9) personal access – an individual must be informed about the existence, use and sharing of his or her personal information and have access to the information upon request. An individual must be able to verify the accuracy and completeness of the information and, if necessary, correct such information;

10) verification of compliance – a person should be able to send requests to verify the compliance of operations with personal data with legal principles. [2, p. 157].

The new Federal Law of 1990 "On Data Protection" came into force on June 1, 1991, replacing the 1977 Federal Law. The law was created with the experience of the practice of applying the 1977 Federal Law, which was in force before it, it takes into account new technical achievements in the field of data processing and protection, as well as the case law of the Federal Constitutional Court, namely the decisions on data protection issues that became a catalyst for revising the provisions of the 1977 Law "On Personal Data Protection." However, the decisive factor was the judgments of the Constitutional Court related to the 1983 population census.

According to these decisions of the German Constitutional Court, there is a need to protect the data of a citizen for the free development of his or her personality, which is expressly established in paragraph 1 of Article 2 of the German Constitution. The Court interpreted this fundamental right as endowing any individual with the so-called "informationelles Selbstimmungsrecht" [10], i.e. the basic right to make decisions regarding the notification, transfer and use of their personal data. However, the Constitutional Court also recognized the existence of certain limits to this right of self-determination.

The prevailing interests of society as a whole should be able to allow for restrictions on this personal freedom. Such exceptions, however, must be contained in a law that meets the constitutional requirements (principles of clarity and reasonableness). In addition, the court ruled that it is up to the legislature to ensure the functioning of the data protection system in practice by adopting appropriate administrative and procedural provisions into the law. After all, as noted by Lynskey Orla (2016), on October 3, 1990, some specific problems in the field of data protection were identified that were directly related to the reorganization of the state as a whole, namely the unification of the German Democratic Republic and the Federal Republic of Germany [17].

Since then, in accordance with the Unification Treaty, the 1990 Data Protection Act was also to apply to the five new Länder that were part of the territory of the then former German Democratic Republic. Accordingly, on October 3, 1990, the Federal Data Protection Act was applied to the newly annexed Länder in special transitional provisions [3]. According to Article 1, paragraph 22 of the 1990 Data Protection Act, the Federal Data Commissioner is elected by the Bundestag, the Federal Assembly, on the proposal of the Federal Government, and appointed by the Federal President.

However, in October 1991, one of the five new Länder, Thuringia, adopted its own data protection law, which in most provisions mirrored the federal law. The widespread use of personal identification numbers in the old system of the German Democratic Republic led to the need to destroy these numbers as soon as possible and to re-configure the information so that these numbers were no longer needed. Human rights activists, including the President of the Federal Republic of Germany, Joachim Gauck, insisted on this. There are groups of articles that set out the procedure for providing information from the Stasi archives, which indicates the legislator's willingness and desire to give a political, legal, and historical assessment of the Stasi's activities, as well as the regime of the German Democratic Republic itself.

This law was limited to a fixed period, until 2011, and was subsequently extended until 2019 by amendments to it, which established special organizational measures for the handling of truly explosive personal information contained in the archives of the state security service of the former German Democratic Republic (the so-called "Stasi" (Ministerium für Staatssicherheit – "Stasi")) [7].

In Germany, the protection of human rights to privacy is a matter of administrative law. The provisions of administrative law, for example, in the field of social insurance (Social Code Act) or on the protection of privacy rights in the Federal Identity Card Act (Article 3), etc., are supplemented by the provisions of criminal law (Criminal Code (Code) of the Federal Republic of Germany - Deutsches Strafgesetzbuch (StGB)), which provide for criminal punishment for violation of the rights of citizens to privacy.

The drafting government is currently amending the law to bring it in line with EU standards. Sections VI and VII of the General Data Protection Regulation define the scope of powers, establishment, responsibility, cooperation and independence of the supervisory authority. Local jurisdiction depends on the location of the non-governmental body. In almost all federal states, responsibilities have been consolidated in such a way that public data protection officers are responsible for the public and non-public spheres [15].

The independent data protection authorities of the federal and state governments meet twice a year at the Data Protection Conference (DPC) and, after the preliminary work of numerous working groups, adopt agreed resolutions, recommendations, standardizations and statements [16].

The Office of the State Commissioner for Data Protection and Freedom of Information of Baden-Württemberg [21] is an independent, statutory authority responsible for data protection and freedom of information. The Office of the State Commissioner monitors compliance with data protection rules in governmental and non-governmental bodies. It provides consultations, informs and explains data protection issues and helps citizens to exercise their rights. [24]

As Germany is a federal state, data protection is also a major concern of the federal states. Here, the Commissioner for Public Data Protection is responsible for the implementation and protection of data.

At the level of the federal states, there is also a federal commissioner responsible for data protection and freedom of information in each state. In turn, broadcasting organizations and religious organizations have their own supervisory authorities. Each federal state has an office of a federal data protection commissioner. In most cases, this person is responsible for the public and non-public spheres, namely government authorities and state-owned companies, as well as private companies, clubs, associations and political parties [24].

The only exception is Bavaria: here, the state data protection commissioner is responsible exclusively for data protection in the public sector. The state data protection supervisory office in Ansbach is responsible for issues that are not in the public domain.

The Federal Data Protection and Freedom of Information Commissioner, in turn, is responsible for all federal agencies. Companies in the telecommunications and postal sectors are also subordinated to it.

The Federal Data Protection Commissioner and 17 state agencies together form the Conference of Independent Federal and State Data Protection Authorities and, as noted by Diaz, P. (2022), ensures mutual coordination [9, p. 17]. Thus, the responsibility is vested in the individual data protection authorities of the federal states – in the case of Bavaria, according to M. Hartlev (Gefenas, E., Lekstutiene, J., Lukaseviciene, V., Hartlev, M., Mourby, M., and Cathaoir, K.Ó. (2021)), it is the state data protection supervisory authority [13].

There is a broadcast data protection officer for public organizations in the broadcasting sector. In Germany, there is no central broadcast data protection authority, but several regional authorities. In some cases, however, the responsibilities of the broadcast data protection officer are combined so that one broadcast data protection officer is responsible for several broadcasters. In Germany, the Church of Christ also has a separate data protection authority. Protestants and Catholics have different rules.

The German Evangelical Church has a data protection officer. The only exceptions are parts of Brandenburg, parts of Hamburg, Schleswig-Holstein, and the North Church in Mecklenburg-Vorpommern, which have their own data protection officers.

In the Catholic Church, the situation is more complicated: each Diocese has its own data protection officer. The diocesan data protection officers meet to coordinate their relations. The data protection officer of the German Evangelical Church is also regularly invited. There is also the German Diocesan Association, which has appointed a data protection officer for the association.

This clearly shows that the structure of the data protection officer in Germany is much more complex than in other countries, where there is usually only one supervisory authority. This is mainly for historical reasons. The national data protection officer (also) interprets national rules and laws. In this way, government data protection officials know the national rules and can react accordingly.

A striking example is provided by E. Gefenas (Gefenas, E., Lekstutiene,J., Lukaseviciene, V. (2022)) – data collection after the corona crisis [11, p. 25]. Due to the pandemic, all federal states have issued protective regulations individually adapted to the needs of the federal state. For example, when restaurants, hairdressers, or physiotherapy clinics were allowed to reopen after protective measures were relaxed, many federal states decided to record contact details of guests, customers, or patients. The national data protection officer provides assistance and provides sample forms for data entry upon national request.

If there is only one federal agency in this case, it must first know the specific protection provisions of the individual federal states. Since the national data protection officers are already familiar with the national regulations, they can act more quickly and respond to the specific circumstances of the individual federal states.

The GDPR stipulates that data protection authorities must be independent. Member States have to ensure this, as does every national data protection authority. Many authorities in Germany invoke this independence, which means that public data protection officials may have different views on the interpretation of the law, especially the GDPR.

If there is only one federal agency in this case, it must first know the specific protection provisions of the individual federal states. Since national data protection officers are already familiar with national regulations, they can act more quickly and respond to the specific circumstances of the individual federal states.

In Ukraine, personal data protection is regulated by the Law of Ukraine "On Personal Data Protection", which came into force in 2011. In 2012, a special body, the State Service of Ukraine for Personal Data Protection, was established to implement its provisions and fulfill its tasks. However, two years later, it was liquidated, and the main function of personal data protection was assigned to the Ukrainian Parliament Commissioner for Human Rights and the courts.

This law regulates the following main issues of personal data processing: requirements for personal data processing; rights of personal data subjects; grounds for personal data processing; procedure for the main processes of personal data processing (collection, use, accumulation and storage, distribution, deletion); procedure for processing personal data, the processing of which poses a particular risk to the rights and freedoms of personal data subjects, etc.

However, in the era of rapid development of digital technologies, the current legislation on personal data protection does not meet modern requirements. It does not provide adequate protection of personal data subjects when processing personal data using information technologies and does not contain sufficient guarantees of the rights of data subjects in case of leakage of personal data contained in the databases of the personal data owner.

Due to the changes in the economy and social life, Ukrainian legislation needs to be completely updated to regulate the processing of personal data.

It is unprecedented that the General Data Protection Regulation has not only a territorial effect limited to the borders of the European Union. This Regulation also applies to persons who process personal data of European Union subjects in connection with the sale of goods or services in the EU and monitor the behavior of European data subjects.

Therefore, Ukrainian business entities that perform the above actions also fall under the scope of the General Data Protection Regulation. In this regard, Ukrainian businesses operating in the European Union have already been forced to bring their internal processes in line with the requirements of the Regulation and adapt their document flow.

According to Article 15 of the EU-Ukraine Association Agreement, Ukraine and the European Union have agreed to cooperate to ensure an adequate level of personal data protection in accordance with the

highest European and international standards, in particular the relevant documents of the Council of Europe.

For Ukraine, this means implementing European personal data protection standards into Ukrainian legislation.

On June 7, 2021, the Verkhovna Rada of Ukraine registered the Draft Law "On Personal Data Protection" No. 5628, which provides for the reform of the personal data protection sector in Ukraine and brings Ukrainian legislation on personal data protection in line with the European one.

The GDPR stipulates that data protection authorities must be independent. Member States must ensure this, as must each national data protection authority. Many authorities in Germany refer to this independence, which means that public data protection officials may have different views on the interpretation of the law, especially the GDPR [18, c. 23].

However, due to Germany's federal system, the GDPR may be interpreted differently in different federal states. This actually contradicts the idea of comprehensive harmonization of the GDPR and can complicate the situation for companies operating in several federal states of Germany and several EU member states. In such cases, the regulators may disagree, but ultimately the European Court of Justice will decide on the application of the law. Individuals and companies can appeal to the data protection regulator. However, in some cases, it is unclear who is responsible.

Article 56(1) of the GDPR introduces the so-called single window mechanism. Thus, in the context of cross-border data processing, there is a primary supervisory authority as a single point of contact for controllers or processors of personal data. This means that a company only needs to deal with one regulator for the same data processing, regardless of whether other regulators are involved or not.

In addition to the single window mechanism, there is also the possibility of so-called consensus procedures. During this process, controversial issues are referred to the European Data Protection Board for a binding decision. There are other forms of cooperation, such as administrative mutual assistance.

For example, when dealing with a case or exchanging information, a data protection authority may request support, i.e. administrative assistance, from another data protection authority in Europe. This also contributes to a Pan-European consistent interpretation and application of the GDPR. [14].

5. Conclusions.

The European General Data Protection Regulation (GDPR) is in effect. It applies directly to all member states of the European Union. However, there are exceptions where member states can also adopt their own rules for certain areas. German lawmakers have used these introductory provisions in the BDSG and adapted national data protection laws in accordance with the DS-GVO so that they can continue to exist.

The system of federal data protection authorities in Germany is more complex than in other EU countries. In practice, this sometimes creates problems and indirectly becomes a competitive disadvantage for German companies. Although the introduction of the GDPR helped to harmonize data protection rules across member states, there are still regional differences in Germany. Sometimes this is also useful, as it allows the federal states to act more quickly, as was the case during the COVID-19 pandemic.

Nevertheless, the various instruments ensure better coordination between the data protection authorities of the individual federal states at the national level, as well as between the authorities in different EU member states at the European level, compared to the time before the GDPR came into force in May 2018.

We propose to implement an organizational structure of the UkrDPR that will meet the requirements of the GDPR and take into account the continental GDPR jurisdiction (e.g. Germany). We also emphasize the need to create a specially authorized body for personal data protection, such as the National Commissioner for Personal Data Protection, which is a prototype of the Federal Commissioner for Personal Data Protection in Germany. This will be the beginning of the creation of a national effective system of personal data protection on a par with European countries.

References:

1. Siehe Weichert in Kühling/Buchner (Hrsg), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO/BDSG2 (2018) Art. 4 Nr. 15 Rz 1.
2. Vgl. Weichert in Kühling/Buchner (Hrsg), DSGVO-Kommentar Art. 4 Nr. 15 Rz 2; siehe auch Hödl in Knyrim (Hrsg), DatKomm (2018) Art. 4 DSGVO Rz 157.
3. Siehe DSB 23. 5. 2014, DSB-D213.131/0002-DSB/2014; vgl. auch Knyrim, Darf ich die Sozialversicherungsnummer zur Personenidentifizierung verwenden? Dako 2016/46, 71.
4. Anderson, D., Abiodun, O. P., and Christoffels, A. (2020). Information Security at South African Universities-Implications for Biomedical Research. Int. Data Privacy L. 10, 180–186. doi:10.1093/idpl/ipaa007.
5. B. Baran, K. Południak-Gierz - Perspektywa regulacji prawa do bycia "zapomnianym" w Internecie: zarys problematyki, Zeszyty Naukowe Towarzystwa Doktorantów Uniwersytetu Jagiellońskiego 2017, № 2.
6. Biasiotto, R., Pramstaller, P.P., and Mascalzoni, D, (2021). The Dynamic Consent of the Cooperative Health Research in South Tyrol (CHRIS) Study: Broad Aim within Specific Oversight and Communication. BioLaw J. – Rivista Di BioDiritto 21, 277–287. doi:10.15168/2284-4503-786
7. Data protection in the EU: an official website of the European Union. URL: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.
8. David Erdos (2021) The 'right to be forgotten' beyond the EU: an analysis of wider G20 regulatory action and potential next steps, Journal of Media Law, 13:1, 1-35, DOI: 10.1080/17577632.2021.1884947.
9. Diaz, P. (2022). Data protection: legal considerations for research in Switzerland. FORS Guide No. 17, Version 1.0. Lausanne: Swiss Centre of Expertise in the Social Sciences FORS. doi:10.24449/FG-2022-00017.
10. Dove, E.S., and Chen., J. (2020). Should Consent for Data Processing Be Privileged in Health
11. Gefenas, E., Lekstutiene, J., Lukaseviciene, V. et al. Controversies between regulations of research ethics and protection of personal data: informed consent at a cross-road. Med Health Care and Philos 25, 23–30 (2022). https://doi.org/10.1007/s11019-021-10060-1.
12. Benkert, Daniel: Beschäftigtendatenschutz, in: NJW-Spezial, 2021, S. 562- 563.
13. Gefenas, E., Lekstutiene, J., Lukaseviciene, V., Hartlev, M., Mourby, M., and Cathaoir, K.Ó. (2021). Controversies between Regulations of Research Ethics and protection of Personal Data: Informed Consent at a Cross-Road. Med. Health Care Philos. doi:10.1007/s11019-021-10060-1.
14. General Data Protection Regulation. Regulation (EU) 2016/679 (General Data Protection Regulation) in the current version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.
15. Judgment of the European Court of Justice in case Flaminio Costa v. E.N.E.L. of 15 July 1964, court case No. 6/64. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61964CJ0006.
16. Kruegel, S. (2019). The informed consent as legal and ethical basis of research data production. FORS Guide No. 05, Version 1.0. Lausanne: Swiss Centre of Expertise in the Social Sciences FORS. https://forscenter.ch/fors-guides/fg-2019-00005/.
17. Lynskey, Orla (2016) The Europeanisation of data protection law. Cambridge Yearbook of European Legal Studies . ISSN 1528-8870 DOI: 10.1017/cel.2016.15.
18. Maritsch, F., Cil, I., McKinnon, C. et al. Data privacy protection in scientific publications: process implementation at a pharmaceutical company. BMC Med Ethics 23, 65 (2022). https://doi.org/10.1186/s12910-022-00804-w.

19. Oksana Bratasyuk, Oksana Shevchuk Protection of children's information (digital) rights who were illegally exported from the territory of Ukraine during the war or in occupation. Visegrad Journal on Human Rights. № 2/2022 P. 21 – 26.

20. Oksana Shevchuk International legal experience in financing information security in the financial sphere Visegrad Journal on Human Rights. № 1/2022. 2022 P. 140–143.

21. Oleksandr O Bryhinets, Ivo Svoboda, Oksana R Shevchuk, Yevgen V Kotukh, Valentyna Yu Radich Public value management and new public governance as modern approaches to the development of public administration Revista San Gregorio T. 1, № 42.

22. Recommendation CM/Rec (2016)5 of the Committee of Ministers to member States on the Internet freedom. URL: https:// search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa.

23. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=ENм.

24. Kühling, Jürgen/Martini, Mario et al., Die Datenschutz-Grundverordnung und das nationale Recht, Münster. 2016.

Oksana Bratasyuk,
PhD in Law,
Researcher of Osnabrueck University,
Associate Professor of Constitutional,
Administrative and Financial law
West Ukrainian National University (Ternopil)
e-mail: rosoliak@gmail.com
ORCI ID: https://orcid.org/ 0000-0002-5871-4386