PROTECTION OF PERSONAL DATA IN THE LAW OF UKRAINE: CURRENT STATUS AND RECOMMENDATIONS FOR CHANGES

Natalia Semchuk[1]

DOI: https://doi.org/10.30525/978-9934-26-310-1-18

Abstract. The chapter presents the results of a study of ways to improve the protection of personal data in Ukraine, conducted as part of a postdoc internship. *The subject* of the study is the question of compliance of Ukrainian legislation in the field of personal data protection with EU standards. The methods used in the work are dogmatic and comparative. *The object* of the analysis was a comparison of the legislation of the European Union, Ukraine and Poland regarding the protection of personal data. The foreign theory on the protection of personal data, the practice of such protection and the peculiarities of foreign training of specialists in the field of personal data are also analysed. Specifies the parameters by which Ukraine could receive a decision on the adequate state of personal data protection before the EU accession procedure is fully completed according to article 45 of the GDPR. *The purpose* of the work is to compare European and Ukrainian legislation on the protection of personal data with the aim of adapting it to European standards. The study made it possible to draw a number of conclusions. On the basis of the conducted research, it is proposed for Ukraine to adopt a new law on the protection of personal data, and the concept of such a law has been developed. *The main proposals are:* implements the GDPR as part of the national legislation of Ukraine; predict that all terms and concepts used in the GDPR have priority in application in case of discrepancies with other regulatory acts; determine a new official "personal data protection Commissioner" as a supervisory authority within the meaning of GDPR;

[1] PhD, Associate Professor of the Department of Criminal Law,
National Aviation University, Ukraine;
Researcher of the Warsaw University Postdoc Program, Poland
ORCID: https://orcid.org/0000-0002-9357-9108
Supervisor: Arwid Tadeusz Mednis
dr hab., Professor of Law and Administration Faculty,
Warsaw University, Collegium Iuridicum I, Poland
ORCID: https://orcid.org/0000-0001-8130-7108

establish requirements for the personal data protection inspector; pay attention to such issues as: peculiarities of regulating the powers of an administrator performing a public task; issues of personal data protection and national security; accreditation of entities applying for certification in the field of personal data protection; conditions and certification procedure; codes of conduct; the status of the Commissioner and the procedure for his or her appointment; guarantees of independence of the Commissioner; significantly increase fines for violation of personal data protection rules and improve the procedure for imposing them.

1. Introduction

The main regulatory act of the European Union in the field of personal data protection, which establishes uniform requirements within the European Union and the European Economic Area, is 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) (further – GDPR) [14].

According to GDPR, clauses 104 and 105 of the preamble, articles 5-7, 9, 45-47, 49 [14], a country that is not a member of the European Union can receive the status of a country that adequately ensures the protection of personal data and to which data can be freely sent from the European Union.

However, the legislation of Ukraine already contains quite a lot of requirements for the fulfilment of the information obligation, which are quite close to the GDPR [14].

Article 45 of the GDPR specifies the parameters by which Ukraine could receive a decision on the adequate state of personal data protection before the EU accession procedure is fully completed [14]. Such parameters are divided into three groups: a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules etc.; b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing

compliance with the data protection rules, including adequate enforcement powers etc.; c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments.

Since some of these parameters can be assessed only during a large monitoring mission (for example, the state of democracy). Since it is not possible independently investigate such aspects, the data of international ratings will be used in these questions with appropriate clarifications.

The World Justice Project Rule of Law Index (further – WJP Rule of Law Index) which involves the evaluation of many parameters such as the rule of law, human rights standards and law and order in 2022, before the war, placed Ukraine in 76th place in the overall rating, while Hungary as a member of the EU was in 73rd place [50]. According to some parameters of this rating, for example, respect for international human rights norms and standards Ukraine ranks 55th, and Poland 52nd [50]. Ukraine should improve its position, but now Ukraine is very close to the European Union countries.

Other ratings also indicate Ukraine's progress. In particular, such conclusions are contained in the European judicial systems Evaluation Report of the European Commission for the Efficiency of Justice (abbreviated – European judicial systems CEPEJ Evaluation Report 2022 Evaluation cycle) [13].

Among decisions on the recognition of adequacy, a good example is the decision regarding the Republic of Korea [34]. The main text of this act includes: an introduction; analysis of rules applying to the protection of personal data (general situation; definition of personal data, processing, personal information controller and "outsourcee"; special provisions for information and communication service providers; lawfulness and fairness of processing, processing of special categories of personal data; purpose limitation; data accuracy and minimisation; storage limitation; data security; transparency; individual rights; onward transfers; accountability; special rules for the processing of personal credit information; oversight and enforcement); access and use of data to be obtained from the EU by public authorities; conclusions and proposals.

This system can also be used to assess the personal data protection system of Ukraine for compliance with the specified requirements and to determine the prospects of obtaining a similar solution.

2. Literature review

European scientists pay a lot of attention to various aspects of personal data protection. The first surge of interest in the topic began in the 1970s, the second after the adoption of the GDPR [19; 29, p. 563].

J. Zhang et al. indicates that theoretical provisions and practical guidelines for the use of GDPR are in the formative stage. In this case, the main thing is the balance of privacy protection and minimization of consequences for business [48].

J. Kurek writes that personal data serve to achieve public goals, such as national security and public order, as well as the welfare of a personal nature, the protection of which determines the security of a person in the personal dimension, in particular the protection of privacy [21, p. 3]. The legal basis for privacy protection in Poland is Article 47 of the Constitution, according to which everyone has the right to protection of private, family life, honour and good name, as well as to decide about his private life. On the other hand, protecting personal data is part of cyber security [10].

J. Olszewska & M. Nowikowska draw attention to the close connection between personal data protection and access to information, including public information [35, p. 17; 37, p. 1175].

Modern works, which are devoted to the protection of personal data after the adoption of GDPR, can be conditionally divided into two groups. The first group of works is devoted to the analysis of the general principles of GDPR application, and the second to specific aspects in the context of particular issues. Regarding the first group of works dedicated to general principles, the following works should be noted.

M. Todorova – Ekmekci highlights that a person has the following basic rights during data processing: the right to information, the right to access of personal data free of charge and in an accessible format, the right to object processing of their data or part of their data if they have not given their consent, the rights in relation to automated decision making and profiling, the right to be forgotten, the right to data portability of personal data to themselves or to another controller, the right to restrict processing [44, p. 33–34]. L. Jasmontaitė-Zaniewicz et al. indicates such rights: right to transparency and information, right to access, right to rectification, right to erasure, a.k.a. right to be forgotten, right to restriction of processing, right to data portability, right to object,

right to not be subject to a decision based solely on automated decision-making or profiling [18, p. 64–74].

C. Negri-Ribalta et al. highlights the following data protection principles: lawfulness, fairness, and transparency, purpose limitations, data minimization, accuracy and storage limitation, integrity and confidentiality, accountability, non-discrimination, fair balance [31, p. 238–239]. D. Sybilski indicates the priority of applying the GDPR in the protection of personal data and the fairness of such an approach [43].

E. Politou et al. point out the following data protection principles consent and purpose limitation, the right to be forgotten, the right to data portability, the obligation for data protection impact assessments, and privacy by design, among others [40, p. 2].

Important principles are the right to data access [15, p. 29–31], digital privacy and digital autonomy, effective restrictions on the use of such systems [4], privacy by design and controlled data transfer to third countries [6].

GDPR also includes the following requirements of data handlers: consent of subjects for data processing providing data breach notifications, safely handling the transfer of data across borders, requiring certain legal entities to appoint a data protection officer to oversee GDPR compliance, anonymizing collected data to protect privacy [44, p. 34].

A. Cieślik et al. indicates the following main points of data processing: compliance with the general principles provided for in Art. 5 GDPR, compliance with the law within the framework of Art. 6-11 GDPR, assurance of performance of duties by the administrator (Articles 24-31 GDPR), assurance of processing security (Articles 32-36 GDPR), data protection inspector control (Articles 27-43 GDPR), legality of data transfer to third countries (Articles 44-49 GDPR) [5, p. 26].

A. Gnatowska & A. Szeliga conclude that the subject matter, purpose, and reference to the administrator are primary in the data conversion clause. The importance of the conditions of data transformation by the controller and the processor is also indicated [16]. It is also important to stress the definition of data processor: an entity that deals with personal data as instructed by a controller for specific purposes and services offered to the controller that involve personal data processing. In this case the controller corresponds to the data subject and the processor corresponds to the consumer. Another entity takes the role of data processor, standing between providers and

consumers: the "aggregator" fulfils the sensing service, gathering data from individual data subjects and producing anonymized aggregated data, ready to be acquired by consumers. Data subjects provide data to the aggregator and both parties agree on predefined policies regarding their rights and obligations [49].

D. Mănescu emphasizes that the legal guarantees provided to data subjects for the protection of personal data can be divided into: the obligation of the operator to inform the state body about a high-risk data security breach [25, p. 427].

Regarding the second group of works devoted to specific aspects, it is first of all worth paying attention to the works on the topic of profiling.

Along with the specific moments of profiling and automated decision-making provided for in the GDPR, general legal obligations and grounds for the administration of personal data apply. That is, the obligation to inform, the right to access data, the right to eliminate data, the right to restrict data transformation, the first transfer of data, the obligations to assess risk and ensure data security apply during profiling in full [27, p. 256, 221].

Profiling is a special method of data processing, the foundations of which are laid by the GDPR. At the same time, profiling may or may not lead to the adoption of automated decisions. During profiling, special attention is paid to what personal data will be processed, for what purpose and in what way. Profiling includes: data collection, profile creation, profile application [27, p. 27, 131]. Anonymization of such data is possible at the stage of data collection for building a profile, then the application of a profile to a specific person concerns his or her personal data. At the same time, tracing the profile to a specific person can have many disadvantages due to the inaccuracy of the model itself, the use of stereotypes, etc. In such a case, the individual has the right to object to profiling and must be able to opt out. In addition to the threat of incorrect profiling, there is the threat of excessive profiling, including the use of excessive biometric data [27, p. 25, 174–175, 109–110].

The following aspects also attracted the interest of scientists: protection of personal data in the metaverse [22; 28; 36]; biometric authentication [40]; using data for scientific purposes [20]; using sensitive personal data [12]; using of personal data in the school system [30]; using of personal data during e-learning [3]; using in the work of banks [23]; work of trade union labour inspectors [47]; protection of personal data of employees [46];

protection of personal data in church activities [24]; protection of personal data by the state [45; 42].

From the study of modern literature, it can be stated that the issue of personal data protection refers to the fundamental right to privacy and is related to the right to access to information.

Different scientists define the principles of personal data protection in different ways. However, the most common are such principles as: the right to transparency and information, the right to access of personal data free of charge and in an accessible format, the rights in relation to automated decision making and profiling, the right to be forgotten, the right to data portability of personal data to themselves or to another controller; the right to restrict processing, digital privacy and digital autonomy, privacy by design, right to rectification, consent of subjects for data processing, safely handling the transfer of data across borders, anonymizing collected data to protect privacy, assurance of performance of duties by the administrator, assurance of processing security, lawfulness, fairness, purpose limitations, data minimization, accuracy and storage limitation, integrity and confidentiality, non-discrimination, fair balance.

Issues of profiling and biometrics occupy a special place. Also, among narrower issues, scientists are investigating such aspects as: protection of personal data in the metaverse; using data for scientific purposes; using sensitive personal data; using of personal data in education; using in the work of banks; work of trade union labour inspectors; protection of personal data of employees; protection of personal data in church activities; protection of personal data by the state.

3. The legislation of Ukraine: current situation

As it was mentioned, in order to obtain a positive conclusion according to Art. 45 of the GDPR, in practice the main parameters are the following [34]: general situation; definition of personal data, processing, personal information controller and "outsourcee"; special provisions for information and communication service providers; lawfulness and fairness of processing, processing of special categories of personal data; purpose limitation; data accuracy and minimisation; storage limitation; data security; transparency; individual rights; onward transfers; accountability; special rules for the processing of personal credit information; oversight and enforcement);

access and use of data to be obtained from the EU by public authorities. We will consider these and other parameters in Ukrainian law for compliance with the requirements of the European regulator.

The Law of Ukraine "On Personal Data Protection" (further – the Law of Ukraine) is the main legislative act in the field of personal data protection in Ukraine. It is available for viewing in the nationwide electronic system of normative acts of Ukraine and includes 30 articles, each of them has a title: scope of the law, definitions, legislation on personal data protection, subjects of relations related to personal data, protection objects, general requirements for personal data processing, special requirements for personal data processing, rights of the personal data subject, notification of personal data processing, use of personal data, grounds for the processing of personal data, personal data collection, personal data accumulation and storage, personal data dissemination, personal data deletion or destruction, personal data access procedure, postponement or denial of access to personal data, appealing a decision on personal data access postponement or refusal, payment for personal data access, amendments and additions to personal data, notification of actions with personal data, monitoring compliance with Law of Ukraine, powers the Commissioner for Human Rights in the field of personal data protection, providing personal data protection, restraints on the validity of this Law, provision of finance for personal data protection works, application of this law provisions, liability for violation of the law on personal data protection, international cooperation and personal data transfer, final provisions [1].

According to the Law of Ukraine [1, art. 11], grounds for the personal data processing are:1) personal data subject's consent to the processing of his personal data; 2) permission to process personal data granted to the personal data owner in accordance with the law solely for the exercise of his powers; 3) conclusion and execution of a transaction to which the personal data subject is a party or which is concluded in favour of the personal data subject or for the implementation of measures preceding the transaction conclusion at the request of the personal data subject; 4) protection of the personal data subject's vital interests; 5) requirement to fulfil the personal data owner's obligation, which is provided for by law; 6) requirement to protect the legitimate interests of the personal data owner or a third party to whom the personal data is transferred, except in cases where the

requirement to protect the fundamental rights and freedoms of the personal data subject in connection with his data processing is dominated by such interests. According to Art. 6 of the Law of Ukraine personal data shall be processed openly and transparently using means and way that meet the specific purposes of such processing [1].

According to Art. 2 of the Law of Ukraine, personal data includes details about the individual, which is or may be explicitly identified [1]. Personal data processing is any action or set of actions, such as collection, registration, accumulation, storage, adaptation, change, renewal, use and distribution (circulation, sale, transfer), depersonalisation, destruction of personal data, including using information (automated) systems [1, art. 2].

Ukrainian legislation uses the term „personal data manager" instead of „personal information controller and "outsourcee". Personal data manager is a natural or legal person who is granted the right by the personal data owner or by law to process this data on behalf of the owner [1, art. 2].

In Ukraine the legislator use the term "Personal data manager", who is a natural or legal person who is granted the right by the personal data owner or by law to process this data on behalf of the owner [1]. Enterprises, institutions and organizations of all forms of ownership, state or local authorities, individuals who process personal data in accordance with the law can be personal data owners or managers. Manager of personal data, the owner of which is a state or local authority, in addition to these authorities, can only be an enterprise of state or municipal ownership that belongs to the sphere of this authority management. Personal data manager can entrust the personal data processing to the personal data manager in accordance with a written agreement. Personal data manager may process personal data only for the purposes and to the extent specified in the agreement. Articles 8, 15, 16, 20, 24 provide for the specific duties of such a manager regarding information processing [1].

According to the Law of Ukraine, processing of personal data on racial or ethnic origin, political, religious or ideological beliefs, membership in political parties and trade unions, criminal conviction, as well as processing of data related to health, sexual life, biometric or genetic data is prohibited (however, certain exceptions are also given in this article) [1, art. 7].

Personal data subject's consent is a voluntary expression of the individual's will (subject to his/her awareness) regarding the granting of

permission to process his/her personal data in accordance with the stated purpose of their processing, expressed in writing or in a form that allows concluding that consent has been provided [1, art. 2]. Consent can also be expressed electronically. Article 14 provides for cases and conditions of data processing without consent [1, art. 14]. Personal data shall be deleted or destroyed in the case of expiration of the data storage period determined by the personal data subject's consent to the processing of this data or by law [1, art. 15]. Personal data access procedure for third parties is determined by the conditions of personal data subject's consent [1, art. 16].

According to Art. 6 and 8 of the Law of Ukraine, personal data composition and content shall be appropriate, adequate and non-excessive with respect to the specific purpose of their processing. The subject has the right to submit a reasoned request for modification or destruction of his personal data by any personal data owner and manager, if this data is processed illegally or is unreliable [1].

Rights of the personal data subject specified in Art. 8 of Law of Ukraine [1]. Personal data subject has the right to: know about the sources of collection, location of his or her personal data, purpose of their processing, location or place of residence (stay) of the personal data owner or manager, or give an appropriate order to receive this information to persons authorised by him or her, 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 or her personal data is transferred; access to his personal data; not later than thirty calendar days from the date of request receipt, except in cases provided for by law, receive a response on whether his personal data is being processed, as well as receive the content of such personal data; submit a reasoned request to the personal data owner with an objection to the processing of his or her personal data; submit a reasoned request for modification or destruction of his or her personal data by any personal data owner and manager, if this data is processed illegally or is unreliable; protect his or her personal data from illegal processing and accidental loss, destruction, damage due to deliberate concealment, failure to provide data or its untimely provision, as well as protect against providing information that is unreliable or discredits the individual's honour, dignity and business reputation; submit complaints about the his or personal data processing to the Commissioner for Human Rights or to

the court; apply legal remedies in case of violation of the law on personal data protection; make reservations regarding the restriction of the right to process his or her personal data when providing consent; withdraw consent to the personal data processing; know the mechanism of automatic personal data processing; be protected from an automated solution that has legal consequences for him or her.

A number of articles of the Law of Ukraine indicate the necessity of processing "with the provision of appropriate protection" for example art 6, 7, 10, 11 [1]. However, the provisions regarding the requirements for such protection are not specified.

Personal data owners or managers are obliged to make amendments to personal data on the reasoned written request from the personal data subject [1, art. 20]. Personal data owner shall notify the personal data subject of the personal data transfer to a third party within ten working days, if required by the conditions of his consent or otherwise not provided for by law [1, art. 21].

The Law of Ukraine establishes the peculiarities of sensitive data. The subject of personal data has the right, among other things: apply legal remedies in case of violation of the law on personal data protection and make reservations regarding the restriction of the right to process his personal data when providing consent [1, art. 8]. Use of personal data provides for any actions of the owner to process this data, actions to protect it, as well as actions to grant partial or full right to process personal data to other subjects of relations associated with personal data, performed with the consent of the personal data subject or in accordance with law consent [1, art. 10].

The legislation of Ukraine does not provide for any special requirements for the data protection inspector and even his/her mandatory appointment. Only for so-called sensitive data, persons responsible for data processing must notify the Commissioner for Human Rights about the person or unit responsible for processing personal data. There are no requirements for such subdivision or person [33]. The Order of the Commissioner for Human Rights "On the approval of documents in the field of personal data protection" perform the specified tasks of the responsible person: ensures the realization of the rights of the subjects of personal data; uses access to any data that is processed by the owner/manager and to all premises of the owner/manager where such processing is carried out; in the event of detection of violations of the legislation on the protection of personal

data and/or this Procedure, notifies the head of the owner/manager for the purpose of taking necessary measures; analyses threats to the security of personal data. The requirements of the responsible person for measures to ensure the security of personal data processing are mandatory for all employees who process personal data [33].

The situation with the qualifications of persons who protect personal data in Ukraine is extremely poor. However, there are no requirements for such a person, which means that a secretary or an accountant who do not have the necessary competencies can be appointed as the responsible person.

Education on the protection of personal data in Ukraine, especially in the context of fulfilling the requirements of GDPR, is virtually absent. Such a qualification cannot be obtained in official educational institutions, and unofficial trainings do not have experienced teachers in these matters. Currently, almost all personal data protection specialists in Ukraine were forced to acquire knowledge in the European Union or work for years under the leadership of a person who received a foreign education. Therefore, for a real improvement in the quality of personal data protection in Ukraine, it is worth adopting not only the experience of the formation of legislation and the practice of its application, but also the issue of training data protection specialists.

Issues regarding banks and providers are not directly regulated by the legislation on the protection of personal data.

At the same time, issues related to oversight and enforcement; access and use of data to be obtained from the EU by public authorities; accountability and some others will be analysed below.

Law of Ukraine "On Access to Public Information" [32] provides both the peculiarities of personal data processing by public bodies and the right of the individual to access to information about him/her, which is being gathered and stored.

Currently, the Law of Ukraine does not mention the peculiarities of information processing by the police during the investigation of crimes. There is such information in the Criminal Procedure Code of Ukraine [9]. The information concerns the procedures for obtaining access to various information by investigative bodies (for example, with the permission of the investigating judge according to the prescribed procedure for obtaining such permission). According to Art. 258, 264 of the Criminal Procedure

Code of Ukraine [9], nobody may be subjected to interference in private communication without the investigating judge's ruling. Obtaining information from electronic information systems or parts thereof the access to which is not restricted by the system's owner, holder or keeper, or is not related to circumventing a system of logical security shall not require permission of the investigating judge.

In Ukraine, all offenses regarding the protection of personal data for which criminal punishment can be imposed are contained in one law – the Criminal Code [8, art. 182, 361-2, 362]. It is prohibited by law: Illegal collection, storage, use, destruction, dissemination of confidential information about a person or illegal alteration of such information; unauthorised actions with information, which is processed in the computers; unauthorised actions with information, which is processed in the electronic computing machines [7, art. 188-39-188-40, 255, 291, 294].

According to the Code of Ukraine on Administrative Offenses [7], a fine is provided for: failure to notify or untimely notification of the processing of personal data or the change of information that is the subject of processing, notification of incomplete or inaccurate information; failure to comply with the inspector's legal requirements; non-compliance with the procedure for personal data protection, which led to illegal access to them or violation of the rights of the subject of personal data [7].

According to the Code of Ukraine on Administrative Offenses, a fine is provided for: failure to notify or untimely notification of the processing of personal data or the change of information that is the subject of processing, notification of incomplete or inaccurate information; failure to comply with the inspector's legal requirements; non-compliance the procedure for personal data protection, which led to illegal access to them or violation of the rights of the subject of personal data. According to the established procedure, the inspector draws up a protocol, and the court imposes a fine. The maximum amount of the fine in conversion is 850 euros [7].

In Ukraine, the issue of authority to conduct inspections is provided for in Art. 23 of the Law, and the procedure for their implementation is regulated by a subordinate act [1]. As can be seen from a comparison of the legislation of Ukraine and Poland, the general issue of inspections is regulated in a similar way. However, the legislation of Poland regulates these issues at the level of the law itself, and in Ukraine it is regulated by

an Order, which can be changed quite often and which does not provide the same level of protection as the law. Therefore, when developing a new Law of Ukraine on the protection of personal data, it is worth introducing these provisions directly into the Law.

Inspector draws up a protocol, and the court imposes a fine. Taking into account the above, it is necessary to fundamentally change the system of fines for violations of personal data processing in Ukraine.

First of all, radically increase their size and empower the relevant authority to fine the culprits directly. It is also worth providing for a separate responsibility for improper security of personal data, taking into account the degree of fulfilment of the duty to protect and obliging the relevant person to report existing security problems to the state body under the threat of even greater sanctions.

It also assesses the existence and effective functioning of one or more independent supervisory authorities in a third country.

Such a body is the Commissioner for Human Rights. He or she is the head of the personal data protection system and appointed to the position and dismissed from the position by the Verkhovna Rada of Ukraine by secret ballot by submitting ballots. A citizen of Ukraine who has reached the age of 40 on the day of election, speaks the state language in accordance with the level determined by the National Commission for State Language Standards, has high moral qualities, experience in human rights activities and has lived in Ukraine for the past five years can be appointed as the Commissioner for Human Rights.

The Commissioner for Human Rights carries out administrative procedures in the field of personal data. This does not correspond to the best foreign practices in this field, because the Commissioner does not have a very large staff. The Commissioner for Human Rights has a high status, but deals with many issues, among which the protection of personal data is not the main one. The Commissioner imposes the appropriate monetary fines [7].

He or she has the minimum necessary powers and formally meets the criteria of the GDPR. However, in the future, Ukraine needs a separate body with the appropriate level of authority to protect personal data. After joining the European Union, it will greatly complicate international cooperation and rapid integration. Therefore, Ukraine needs a separate head of the personal data protection system.

The issue of international data transfer is problematic.

According to Art. 29 of the Law of Ukraine, transfer of personal data to foreign subjects of relations associated with personal data is carried out only given that the relevant state ensures adequate personal data protection in cases established by law or an international treaty of Ukraine [1]. Member states of the European Economic Area, as well as states that have signed the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, are recognized to ensure an adequate level of personal data protection. The Cabinet of Ministers of Ukraine determines the list of states that ensure proper personal data protection. Personal data may not be disseminated for any purpose other than that for which it was collected.

Personal data may be transferred to foreign subjects of relations associated with personal data, also in the case of: 1) granting by the personal data subject an unambiguous consent to such transfer; 2) requirement to conclude or execute a transaction between the personal data owner and a third party that is the personal data subject in favour of the personal data subject; 3) requirement to protect the vital interests of personal data subjects; 4) requirement to protect the public interest, establish, implement and ensure the legal requirement; 5) provision by the personal data owner of appropriate guarantees of non-interference in the personal and family life of the personal data subject.

Currently, the signatories of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data include the aggressor state, the Russian Federation. Therefore, before making changes to Art. 29 of the Law of Ukraine [1], there is a significant risk of a completely automatic transfer of personal data further to the Russian Federation. Therefore, the mechanism provided for in Art. 29, needs significant improvement [1].

An example of the negative impact of insufficient attention of the Ukrainian parliament to issues of personal data protection can be the policy of the most common social network in Ukraine – Facebook. Now, despite the war with Russia and the ban on Facebook in Russia, complaints about the actions of users and the processing of user data from Ukraine are handled by the office in Moscow. Repeated petitions to move the provisions on such processing to the Warsaw office have not been successful.

After all, Polish legislation applies the provisions of the GDPR, which are quite strict in terms of privacy protection. Ukraine has not adopted such a strong protection, on the contrary, it allows the problem-free transfer of personal data to Russia. Of course, a private company with an office in the USA (where there is still no federal law on the protection of personal data) will not pay for its money to protect the personal data of Ukrainians better than the law requires.

A big shortcoming that Ukraine must urgently correct is the lack of a rule on informing the person who protects personal data on behalf of the state about incidents during the processing of personal data. However, despite the similar wording, Ukraine provides the controller of personal data with more opportunities in order to obtain the broadest possible consent for processing at the beginning and then actually care little about the subject of personal data. For example, in the consent itself to take permission for the transfer of data abroad, transfer to third parties and not even to inform about it. This situation simplifies economic activity, but provides slightly less data protection than in the EU. In order to correct this situation and further successful integration into the EU, these possibilities should be narrowed down a bit. In this case, it is not advisable to rewrite the provisions of the European Regulation as completely as possible, because it is significant in scope and duplicating its provisions will make the main legislation of Ukraine on the protection of personal data excessively voluminous and difficult to understand. It is possible to use the Polish model and, after the ratification of the EU Regulation, simply provide the relevant references in the updated legislation of Ukraine.

The legislation of Ukraine does not provide yet any procedures for accreditation and certification in the field of personal data. Polish legislation is also at the stage of formation of these procedures, they are not yet fully operational.

Also, the issue of Ukraine's participation in multilateral or regional systems, in particular regarding the protection of personal data, needs revitalization, so far the work in this direction is quite slow.

As can be seen from the analysis, Ukraine is approaching the parameters that the GDPR determines for the decision on compliance of the level of protection of a third country. However, in order to recognize such a level, it is necessary to improve both the fulfilment of certain rating requirements

and the provision of amendments to the legislation on the protection of personal data. In order to formulate specific proposals, it is necessary to conduct a detailed comparison of the legislation of Ukraine and Poland on these issues.

4. Modern Polish legislation in the field of personal data protection

As mentioned above, the main regulatory act of Poland in the field of personal data protection is GDPR [14].

However, some additional and specific points are regulated by a separate national law. "The Polish personal data protection act" (further – the Law of Poland) includes 176 articles [39]. Articles in the Law of Poland do not have titles, but are divided into 14 sections (13 are currently in effect): general regulations, appointment of a data protection officer, conditions and procedure for granting accreditation to the certification subjects, development and approval of codes of conduct, conditions for accreditation of the subject of control over their compliance, head of the Office, proceedings in cases of violation of personal data protection, European administrative cooperation, monitoring of compliance with provisions on personal data protection, civil liability and legal proceedings, provisions on administrative and criminal penalties, transitional and adaptation provisions, final provisions.

The Law of Poland outlines the scope of application and covers a much wider range of issues: for example, regarding accreditation, certification, codes of conduct, fines and penalties, and many other issues [39]. It has a larger volume and regulates some issues that have not been regulated in Ukraine so far. In this regard, a number of provisions of the Law of Poland cannot be directly compared with the Law of Ukraine, but only analysed.

Polish law provides for more detailed regulation of the legal status of the database administrator. Among the experience of Poland, which should be useful for Ukraine, the first provision on the peculiarities of the legal status of an administrator who performs a public task (for example, when maintaining a state register of court decisions). Also, provisions on the features of the administrator's powers, in particular, regarding the prevention of crimes, disclosure or prosecution of prohibited acts or execution of punishments, conducting inspections, etc.

In Poland, the Administrator must in some cases appoint a data protection officer, hereinafter referred to as the "inspector". Some authorities must

also appoint such an inspector: 1) subdivisions of the public finance sector; 2) research institutes; 3) National Bank of Poland. The entity that appointed the inspector must notify the President of the Office about his or her appointment within 14 days from the date of appointment, indicating information about such an inspector and issuing an indorsement. About dismissal, change of data, etc. the inspector also informs the President of the office. The inspector's data is also indicated on the website. In practice, the training of such inspectors is a separate specialty of postgraduate training in the field of administration [39].

Polish legislation provides for a number of specifics rights regarding to an administrator who performs a public task. There are a number of provisions when the administrator has fewer responsibilities. However, even in these cases, it is necessary to ensure data protection and establish that the right to privacy does not outweigh the public interest [39].

Clauses 32, 40, 42, 43, 50,54 of the preamble of the GDPR deal with issues of consent. In certain cases, for example, for reasons of public interest, processing without consent is possible. Consent must be provided by a clear affirmative act that establishes a freely given, specific, informed and unambiguous indication of the data subject's consent to the processing of personal data. Silence, pre-checked boxes or inaction shall not be construed as consent. Consent must cover all processing activities carried out for the same purpose or purposes. In addition to consent, processing is also possible on other legal grounds. The declaration of consent must be provided in an understandable and easily accessible form, using clear and simple language and must not contain unfair terms. For consent to be informed, the data subject must at least know the identity of the controller and the purposes of the processing. Consent is considered non-free if it does not allow giving separate consent for various personal data processing operations. Specific features are established when the purpose of processing is changed [14].

Clauses 65 and 68 of the GDPR provide for the rights of the data subject, including the right to rectification, the right to be forgotten, the right to control one's own data and the right to data portability [14]. Clauses 111-112 GDPR indicate the possibility of data transfer, including transfer without consent. In accordance with clause 155 of the Preamble of the GDPR, a number of features of the protection of employee data are provided for [14].

According to Art. 4 of GDPR, 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her [14].

According to Art. 6 of the GDPR, 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) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) 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) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child [14].

According to Art. 7 of the GDPR, the controller must be able to confirm consent. The consent itself must be clearly, comprehensibly and accessible. Before giving consent, the data subject must be informed about it. Withdrawing consent will be as easy as giving consent. In order to assess the voluntariness of the consent, first of all it is assessed whether such consent is necessary for the performance of the contract. Features of sensitive data processing and consent to their processing are regulated by Art. 9 of the GDPR. In Art. 49 of the GDPR regulates the subject's right to consent to the processing of his or her data in a third country [14].

As can be seen from the comparison of the EU Regulation, the Law of Ukraine and the Law of Poland, the Ukrainian model of personal data protection generally corresponds to the approach proposed by the EU, but needs to be refined. The definition of consent to data processing, the conditions for granting and confirming such consent and the rights of the person who gave consent in all cases has a similar theoretical basis.

According to Art. 42-43 of GDPR [14], states should promote certification in the field of personal data. At the same time, the certification bodies themselves need to go through the accreditation procedure. Such procedures have significant national specificity, so consider the mechanism provided for by the Law of Poland.

Articles 12-14 of the Law of Poland [39] provide for the accreditation of certification bodies through the Polish Accreditation Center according to the criteria determined by the President of the Office. The Polish Accreditation Center informs the President of the Office about the granted and cancelled accreditations.

The certification procedure is defined by Art. 15-26 of the Law of Poland [39]. Certification is carried out by the President of the Office or the certification body, at a request from a controller, processor, manufacturer or organization that brings a service or product to market. The list of valid and revoked certificates is published on the website of the Office of the President. The President of the Office during the specified period has the right to evaluate the subject's compliance with the certification criteria for conducting verification activities at the controller, processor, manufacturer or organization that carries out the introduction of the service or product to the market.

The Law of Poland [39, art. 27-33] regulates issue of codes of conduct in sufficient detail. Regarding the understanding of the essence of such codes, reference is made to the provisions of the Directive.

Accreditation of the subject is carried out at his or her request, subject to compliance with the criteria specified in Art. 41 GDPR [14]. After submitting the application, the President of the Office will consider such an application within 3 months and, if appropriate, will issue an accreditation certificate. The president of the office enters information about accredited entities into the register and posts it on the official website. In theory, such accreditation can also be revoked.

After analysing the specified provisions (compared to the certification procedure), it becomes clear that currently the Law of Poland does not prescribe the rights of accredited entities in sufficient detail when monitoring compliance with codes of conduct. However, in general, such a concept can also be borrowed by Ukraine after the implementation of provisions regarding the possibility of approving codes of conduct.

Chapter 9 of the Law of Poland [39, art. 78-91] regulates the issue of inspections on the protection of personal data in great detail. The documents for the inspection, authorizations, procedures for imposing fines, etc., are written out in detail.

First of all, the Law of Poland contains a reference to Articles 83-84 [39] of the GDPR [14]. Many factors must be taken into account. Fines are also significant. The culprit may be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

According to the Law of Poland [39, art. 101-106], the Head of the Office can impose the fines specified in the Directive by his or her decision (lower fines are provided only for certain subjects), postpone and remit such fines. The procedure for transferring fines in different currencies has also been regulated, and there are provisions on transferring them to the budget.

In Poland, two main criminal offenses in the field of personal data protection are included directly in the law on personal data protection. The processing of data without a legal basis is punished (increased liability is established for such actions regarding sensitive data) and for failure to comply with the inspector's instructions [39, art. 107-108].

According to GDPR [14], in order to ensure that natural persons are not deprived of the protection to which they are entitled under this regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as it takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of

natural persons, taking into account the 4.5.2016 EN Official Journal of the European Union L 119/15 nature, context, scope and purposes of the processing or if the controller is a public authority or body.

In Poland, great attention is paid to the education of persons responsible for the protection of personal data. We will give two examples of such programs.

The first example is a two-semester post diploma study, which is held at the Institute of Legal Sciences of the Polish Academy of Sciences [17]. Classes include 176 hours of lectures and practical sessions. Training is conducted in two specializations: "Inspector for data protection in state authorities and organizations" and "Private Sector Data Protection Officer". The postgraduate study program was divided into 4 thematic blocks, common to specialization, concerning: basic issues of personal data protection, specific obligations in the field of personal data protection, performance of tasks of the data protection officer and personal data security management.

An alternative is, for example, the Course for data protection specialists and individuals responsible for the protection of personal data in organizations, preparation for obtaining CIPP/E (Certified Information Privacy Professional/ Europe) and CIPM (Certified Information Privacy Manager) certificates, accredited according to ISO 17024: 2012. The course lasts two or four days and consists of two independent modules: CIPP/E and CIPM [11].

The IAPP's (International Association of Privacy Professionals) CIPP/E, CIPM credentials are the premier privacy certifications accredited by the American National Standards Institute in compliance with ISO/ IAF standards (Accreditation, n.d.). ANAB (ANSI National Accreditation Board) is a wholly-owned subsidiary of the American National Standards Institute (ANSI) and a recognized leader in personnel credentialing. Currently, ANAB is also the only personnel certification body in the United States to meet nationally accepted practices for accreditation.

That is, the company that provides the certification is based in the USA, which is not a party to the GDPR system and has certain problems with the protection of personal data. However, this certification is an example of a voluntary certification, although it has a high cost of up to $550 USD. It is also impossible to talk about any formal advantages after certification.

The main issues to which attention is drawn are the rules of personal data protection; definition and distinction of categories of personal data,

definition of controllers and processors, processing of personal data, information obligations, rights of subjects of personal data, security of data processing, reporting and supervision, international data transfer.

Therefore, in order to ensure the proper level of interaction with the EU and subsequent accession to Ukraine, it is also necessary to conduct courses for personal data protection inspectors at the state level, taking into account the requirements of the GDPR, the national legislation of Ukraine and one of the EU countries, where a representative in the EU will work for quality cooperation. From the basis of Ukraine, take the Polish program and include, first of all, questions about basic issues of personal data protection, specific obligations in the field of personal data protection, performance of tasks of the data protection officer and personal data security management.

5. Legislative proposals

As a result of studying the issue, a number of conclusions were formed. It can be submitted primarily in the form of legislative proposals. Since the current version of the Law of Ukraine "On the Protection of Personal Data" does not correspond to the realities. It is necessary to adopt a new document on the protection of personal data, which will include the following provisions:

1. As part of its regulation, this Law implements the GDPR as part of the national legislation of Ukraine. All terms and concepts used in the GDPR have priority in application in case of discrepancies with other regulatory acts.

This law must define the status of Personal data protection Commissioner, the conditions and procedure for accreditation of the entity authorized to carry out certification in the field of personal data protection, hereinafter referred to as the "certifying body", code of conduct, monitoring and certification; proceedings regarding violation of personal data protection rules; European administrative cooperation regime; control over compliance with provisions on personal data protection; civil liability for violation of information protection rules, personal and legal proceedings and other issues.

2. Appointment of a data protection officer. The administrator and the processor are obliged to appoint a data protection officer, hereinafter

referred to as the "inspector", in the cases and under the conditions specified in Art. 37 of GDPR.

State authorities, local self-government bodies, as well as owners or managers of personal data, who process personal data subject to notification in accordance with this Law, appoint a responsible person who organizes work on the protection of personal data during their processing. Such a person should have knowledge about the peculiarities of personal data protection in Ukraine, GDPR and have sufficient knowledge of foreign languages for constant contact with a representative in the EU. Information about the specified structural unit or the responsible person is reported to the Commissioner who ensures its publication.

3. Personal data protection Commissioner is a supervisory authority within the meaning of GDPR. Commissioner is appointed by the Verkhovna Rada of Ukraine by secret ballot. A citizen of Ukraine who has a higher education and experience in the field of personal data protection, has no criminal record for committing an intentional offense, speaks the state language in accordance with the level determined by the National Commission for State Language Standards, and has high moral qualities can be appointed as a Commissioner. After appointment, the Commissioner takes an oath. The Commissioner cannot belong to a party or a trade union. The Commissioner may have a first deputy and up to three deputies.

4. Also, the new law should pay attention to such issues as: peculiarities of regulating the powers of an administrator performing a public task; issues of personal data protection and national security; accreditation of entities applying for certification in the field of personal data protection; conditions and certification procedure; codes of conduct; the status of the Commissioner and the procedure for his or her appointment; guarantees of independence of the Commissioner; report of the Commissioner; official requests of the Commissioner; procedure for dismissal of the Commissioner; powers of the Commissioner; Data Protection Office; official bulletin and website; the procedure for imposing fines by the Commissioner; peculiarities of appealing decisions of the commissioner in courts; European administrative cooperation and data transfer to third countries; inspections by the Commissioner's office; civil liability; final and transitional provisions.

References:

1. About personal data protection, Law of Ukraine (1 June 2010). Available at: https://zakon.rada.gov.ua/laws/show/en/2297-17#Text

2. Accreditation (n.d.). International Association of Privacy Professionals. Available at: https://iapp.org/certify/accreditation/

3. Adamczewski, P. (2018). Intelligent organizations in development of information civilization. *Ekonomiczne Problemy Usług*, 131, 9–17. DOI: https://doi.org/10.18276/epu.2018.131/1-01

4. Alama-Maruta, K. (2022). Cyfrowe samostanowienie w kontekście algorytmicznych systemów rekomendacji treści o charakterze informacyjnym. Cz. 1. *Prawo Nowych Technologii,* 1, 10–19.

5. Cieślik, A., Karwala, D., Lubasz, D., Palka-Bartoszek, K., Czaplińska, M., Więckowska, M., Jagielski, M., Sakowska-Baryła, M., Otto, M., Komorowska, P., Fajgielski, P., Tobiczyk, P., & Piszewski, W. (2022). *Dokumentacja ochrony danych osobowych ze wzorami* (2nd ed.). Wolters Kluwer Polska SA.

6. Choluj, M., & Kowalczuk- Pakula, I. (2021). Przekazywanie danych do państwa trzeciego – w poszukiwaniu definicji. *Prawo Nowych Technologii,* 1, 19–23.

7. Code of Ukraine on Administrative Offenses (1984). Available at: https://zakon.rada.gov.ua/laws/show/80731-10#Text

8. Criminal Code of Ukraine, The law of Ukraine (2002). Available at: https://zakon.rada.gov.ua/laws/show/en/2341-14#Text

9. Criminal Procedural Code of Ukraine, The law of Ukraine (2013). Available at: https://zakon.rada.gov.ua/laws/show/en/4651-17#Text

10. Cyberbezpieczeństwo. Zarys wykładu (2018). Wolters Kluwer.

11. Deloitte Deutschland. Available at: https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Brochures/pl-Kurs-Inspektor-Ochrony-Danych-IAPP-2021_MA.pdf

12. Eva, G., Liese, G., Stephanie, B., Petr, H., Leslie, M., Roel, V., Martine, V., Sergi, B., Mette, H., Sarah, J., Martin Laura, R., Arnout, S., Morris, S. A., Jan, T., Xenia, T., Nina, V., Espen Koert, V., Sylvie, R., & Greet, S. (2022). Position paper on management of personal data in environment and health research in Europe. *Environment International*, 107334. DOI: https://doi.org/10.1016/j.envint.2022.107334

13. European judicial systems CEPEJ Evaluation Report 2022 Evaluation cycle (2020 data). Available at: https://rm.coe.int/cepej-report-2020-22-e-web/1680a86279

14. General Data Protection Regulation, Directive (2016) (Regulation (EU) 2016/679 of the European Parliament and of the Council). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

15. Greser, J. (2018). Obowiązki organizacji pozarządowych jako administratorów danych osobowych w świetle RODO. *Kwartalnik trzeci sektor*, 42 (2), 21–36.

16. Gnatowska, A., & Szeliga, A. (2022). Relacja Administratora z podmiotem przetwarzającym. *Prawo Nowych Technologii,* 2, 21–26.

17. Inspektor Ochrony Danych – Instytut Nauk Prawnych PAN (n.d.). Instytut Nauk Prawnych PAN. Available at: https://inp.pan.pl/studia-podyplomowe/wykonywanie-funkcji-inspektora-ochrony-danych/

18. Jasmontaitė-Zaniewicz, L., Calvi, A., Nagy, R., & Barnard-Wills, D. (Eds.). (2021). *The GDPR made simpl(er) for SMEs*. Academic & Scientific Publishers. DOI: https://doi.org/10.46944/9789461171092

19. Kępa, L. (2014). *Ochrona danych osobowych w praktyce*. Difin.

20. Kogut-Czarkowska, M. (2021). Pseuwdonimisazja i anonomizacja danych osobowych w badaniach naukowych. *Prawo Nowych Technologii,* 1, 10–18.

21. Kurek, J. (2020). *Ochrona danych osobowych jako realizacja zadań w obszarze bezpieczeństwa państwa*. Wydawnictwo C.H.Beck Sp. z o.o.

22. Kurowska-Tober, E., & Czulak, P. (2022). Metaverse a ochrona danych osobowych- problemy prawne, ryzyka i możliwe podejścia. Prawo Nowych Technologii, 4, 32–38.

23. Labuś, M. (2020). Ochrona danych osobowych po rozpoczęciu obowiązywania rozporządzenia RODO: analiza przypadku Banków Spółdzielczych. *Finanse i Prawo Finansowe*, 1(25), 65–80. DOI: https://doi.org/10.18778/2391-6478.1.25.05

24. Łukańko, B. (2020). Stosunek kościelnej ochrony danych osobowych do RODO – uwagi na marginesie postanowienia Krajowego Sądu Pracy w Norymberdze z dnia 29 maja 2020 roku, 8 Ta 36/20. Studia z Prawa Wyznaniowego, 23, 153–176. DOI: https://doi.org/10.31743/spw.10186

25. Mănescu, D. M. (2021). Brief explanations on EU Directive no. 68027.04.2016 in the field of personal data processing. *Technium Social Sciences Journal*, 26, 424–429.

26. Marciniak, B., Piotr, T., & Strapagiel, D. (2018). Anonimizacja w dobie wielkich danych – sytuacja biobanków w kontekście RODO. *Studia Iuridica*, (73), 73–85.

27. Mednis, A. (2019). Prawo ochrony danych osobowych wobec profilowaina osób fizycznych. Presscom.

28. Miernik, M. U. (2022). Wizerunek a nowe technologie. Wizerunek jako dana biometryczna. *Prawo Nowych Technologii*, 3, 12–14.

29. Md. Toriqul Islam & Mohammad Ershadul Karim. (2021). Extraterritorial application of the eu general data protection regulation: an international law perspective. *IIUM Law Journal*, 28(2), 531–565. DOI: https://doi.org/10.31436/iiumlj.v28i2.495

30. Modzelewska-Stalmach, A., & Popiołek, M. (2018). Opinie pracowników administracji na temat rozporządzenia o ochronie danych osobowych (RODO) w świetle pilotażowych badań jakościowych. *Zarządzanie i Finanse*, 16(4/2), 153–165.

31. Negri-Ribalta, C., Noel, R., Herbaut, N., Pastor, O., & Salinesi, C. (n.d.). Socio-Technical modelling for GDPR principles: An extension for the sts-ml. In *2022 IEEE 30th international requirements engineering conference workshops (REW)*.

32. On Access to Public Information, The law of Ukraine (2011). Available at: https://zakon.rada.gov.ua/laws/show/en/2939-17#Text

33. On the approval of documents in the field of personal data protection, Order (2014). Available at: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

34. On the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act (notified under document C(2021) 9316), Commission Implementing Decision (EU) (б. д.) (European Union). Available at: http://data.europa.eu/eli/dec_impl/2022/254/oj

35. Olszewska, J. T., & Nowikowska, M. (2019). *Prawo do informacji publicznej. Informacje niejawne. Ochrona danych osobowych*. Wolters Kluwer.

36. Piechocki, A., & Gorzkowcka, K. (2022). Wybrane wyzwania dla ochrony prywatności w metawerse. *Prawo Nowych Technologii*, 3, 15–20.

37. Pikulík, T., & Štarchoň, P. (2020). Public registers with personal data under scrutiny of DPA regulators. *Procedia Computer Science*, 170, 1174–1179. DOI: https://doi.org/10.1016/j.procs.2020.03.033

38. Polański, P. (2021). O efektyvnym wdrożeniu domyślniej ochrony danych osobowych w systemach informatycznych. *Prawo Nowych Technologii,* 2, 12–18.

39. Polish personal data protection act, Law of Poland (2018) (Poland). Available at: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000

40. Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, 4(1). DOI: https://doi.org/10.1093/cybsec/tyy001

41. Romansky, R. (2021). Privacy and data protection in the contemporary digital age. *International Journal on Information Technologies & Security*, 4 (vol. 13), 99–110.

42. Sakowska-Baryła, M., & Wyporska-Frankiewicz, J. (2022). Postępowanie po wydaniu decyzji administracyjnej przez Prezesa Urzędu Ochrony Danych Osobowych. *Roczniki Nauk Prawnych*, 32(2), 91–111. DOI: https://doi.org/10.18290/rnp22322.6

43. Sybilski, D. (2022). Nowe modele dzielenia się danymi według przepisów aktu w sprawie zarządzenia danymi (DGA). Cz 2 Dostawca usług pośrednictwa danych i spłodzenie danych. *Prawo Nowych Technologii,* 3, 24–30.

44. Todorova – Ekmekci, M. (2021). GDPR – General Data Protection Regulation on Sites Requiring Accessibility. *Complex Control Systems*, 3(1), 30–40. Available at: http://ir.bas.bg/ccs/2021/4_todorova.pdf

45. Toum, M. (2019). Nowe obowiązki administratorów danych osobowych. *Teka Komisji Prawniczej PAN Oddział w Lublinie*, 12 (2), 377–391.

46. Walczak, K. (2021). Problem przetwarzania danych osobowych w sferze działalności socjalnej pracodawcy. *Krytyka Prawa*, 13 (1), 39–50.

47. Wyka, T. (2021). Ochrona danych osobowych w działalności społecznej inspekcji pracy. *Krytyka Prawa*, 13(1), 25–38. DOI: https://doi.org/10.7206/kp.2080-1084.426

48. Zhang, J., Gisca, O., Koivumäki, T., & Ahokangas, P. (n.d.). 1. Legitimacy challenges in the healthcare ecosystem: data management in the era of GDPR. In *15th Annual Conference of the EuroMed Academy of Business*.

49. Zichichi, M., Contu, M., Ferretti, S., & Rodr´ıguez-Doncel, V. (2020). Ensuring Personal Data Anonymity in Data Marketplaces through Sensing-as-a-Service and Distributed Ledger Technologies. In *3rd Distributed Ledger Technology Workshop Co-located with ITASEC 2020*. Available at: https://ceur-ws.org/Vol-2580/DLT_2020_paper_5.pdf

50. WJP Rule of Law Index (n.d.). https://worldjusticeproject.org/rule-of-law-index/global. Available at: https://worldjusticeproject.org/rule-of-law-index/global