The Personal Data Protection Mechanism in the European Union

Tetiana L. Syroid[1†], Tetiana Y. Kaganovska[1††], Valentyna M. Shamraieva[1†††], Olexander S. Perederii[1††††], Ievgen B. Titov[1†††††], Larysa D. Varunts[2††††††]

[1]V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
[2]Kharkiv National University of Internal Affairs, Kharkiv, Ukraine

Summary
The adoption of the General Data Protection Regulation (EU) 2016/679 transformed approaches and concepts to the implementation of the personal data protection mechanism in the European Union. Within the EU, almost all countries have adapted a new protection mechanism, which requires a study of the specifics of its use. The article intends to assess the legal provisions of the current mechanism of personal data protection in the EU. The author studied the mechanism of personal data protection under the General Data Protection Regulation (EU) 2016/679 (GDPR) based on the concept of contextual integrity and analysis of EU legislation on personal data protection. The scientific publications for 2016-2020 were reviewed for the formation of ideas of a new personal data protection mechanism in the EU, informative and transparent analysis of legal provisions. The article notes that the personal data privacy and protection is increasing, there is an ongoing unification of the legal status of personal data protection and the formation of a digital market for dissemination, exchange, control, and supervision of data. Cross-border cooperation is part of the personal data protection mechanism. The author proved that the GDPR has changed approach to personal data protection: the emphasis is now shifting to the formation of a digital market, where the EU's role in ensuring regulation is crucial. The article identifies the emergence of a new protectionist legal system and strengthening of legal provisions regarding privacy. This legal system needs unification and harmonization in accordance with national legislation, is territorially fragmented and differentiated within the EU.

Key words:
Personal data, personal data protection, GDPR, data protection authorities in EU, GDPR implementation in EU.

1. Introduction

From The fundamental right to the personal data protection is enshrined in the Charter of Fundamental Rights of the European Union (Article 8) and in the Treaties (Article 16 of the Treaty on the Functioning of the European Union, TFEU) [1,2]. Improved methods of data mining, increasing volume of publicly available data have expanded the scope of the EU Data Protection Directive [3]. "Data have become part and parcel of contemporary capitalism" [4]. At the same time, the legislation on personal data protection remains underdeveloped, which requires a revision of the concept of personal data protection [3]. Individuals should acquire the right to use their own personal data, which will ensure a more active role in personal data management and sustainable development. Determining the line between legal and illegal personal data processing causes a number of problems [5].

The data strategy calls for the formation of a personal data market, a "single European data space" [2], which necessitates the development of a mechanism and a clear structure for secure data exchange and increased accessibility. The importance of the research sector's access to data, which requires the functioning of the European Cloud Federation to monitor the personal data market, is increasing [2].

In fact, personal data is transferred from the object of protection to the object of management, control and sale for the necessary purposes and in required volumes. The data market is emerging in the EU, its control and supervision is based on the EU legislation and initiatives. Public awareness of the need for data privacy and security is growing through an understanding of the impact on decision-making and people's behaviour on the Internet. Companies encourage the initiative to form a data market through the possibility of creating competitive advantages, providing certain rights and guarantees to their customers in accordance with the GDPR.

The Regulation (EU) 2016/679 (General Data Protection Regulation), the EU's new data privacy law, aims to strike a balance between personal data protection rights and data processing needs of business and the research sector [6]. The adoption of the updated GDPR in May 2018 strengthened data protection guarantees, powers and additional rights of data subjects, increased transparency, created a new management system, and gave authorized bodies stronger enforcement powers [2]. As a result, a new concept of personal data protection based on a human-cantered approach is being formed in the EU. This raises the issue of the effectiveness of the personal data protection mechanism in the EU. Given that the studies mostly cover the mechanisms of action of the EU Data Protection Directive (DPD) [5, 7, 8], it is important to identify the features of the new innovative mechanism for personal data protection management in the EU.

Manuscript received May 5, 2021
Manuscript revised May 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.5.17

The article is intended to assess the legal provisions of the current personal data protection mechanism in the EU.
This article answers the following questions:

1. How flexible is the EU's personal data protection mechanism?
2. What are the differences within the EU regarding the implementation of the personal data protection mechanism in the EU?
3. What concepts does the EU data protection mechanism correspond to?

2. Literature Review

Personal data is any information relating to a particular individual (personal data subject), including his last name, first name, patronymic, year, month, date and place of birth, address, family, social, property status, education, profession, income, other information. Legal remedies for personal data protection include administrative and judicial tools to restore the violated right to personal data protection [9-11]. Administrative means are used in case the entity decides to file a complaint to the supervisory authorities. Judicial remedies are used in case of opposition to the bodies of supervision and control on the basis of individual rights [12]. The latest innovative mechanism for personal data protection is the GDPR, which aims to facilitate administrative protection procedures and reduce the use of judicial data protection procedures.

Under the new regulation, personal data can be considered to be any personal information that may identify individuals, such as audio, address, video, texts, but also online identifies, such as IP addresses. The new EU law also introduces and discusses the idea of pseudonymous data, which is data attempting to identify the subject. The law also covers profiling. So, if genuine efforts have been made to pseudonymize personal data, the law looks favourably at these efforts in legal cases. Effectively, GDPR will apply to all types of data collected, whether it is directly identifiable or quantitative and technical data from or about any EU resident In Europe, the current law that covers personal data protection was approved by Parliament in April 2016 and after a two-year grace period, allowing national governments and regulators to get ready, was finally put into practice on 25 May 2018. The General Data Protection Regulation (GDPR) was enacted in order to enable EU citizens and institutions to get better control of their personal data. GDPR is the latest legal instrument for personal data protection, which will ensure the introduction of a new generation of communication infrastructure in many urban areas of Europe, Northeast Asia, North America and other regions of the world through an innovative mechanism for managing personal data protection [13]. One of the focus of the law is to ensure transparency and accountability in order to minimize risks of individuals' data from being misused. Organizations, whether European or foreign, operating in the EU are now required to abide by this legislation and this presents a challenge as some global institutions, such as NGOs and multinational corporations, will have to comply with several regulatory bodies.

"The new GDPR provides a common framework more consistent with technological advances and globalisation, providing legal security to the personal data processing" [14]. GDPR applies in cases where the data may be processed outside the EU, but the law of a Member State will be applied to that jurisdiction through the use of an instrument of public international law. The "territorial" provisions of the GDPR are the "long arm" of the law, ensuring that the GDPR applies beyond the EU. Under the GDPR, data processing is any set of operations with personal data or their processing, regardless of the processing methods (manual or automated). The GDPR sets out complex and stringent requirements for organizations or individuals doing business in the European Union (EU) and the European Economic Space, while dealing with the export of personal data outside the country [15, p. 45-57]. The GDPR allows for fines of up to 5% of income for breaches of privacy and data protection.

3. Materials and Methods

This article uses contextual integrity due to changes in the mechanism of personal data protection in accordance with the General Data Protection Regulation (EU) 2016/679 [1]. Contextual integrity, developed by Helen Nissenbaum, was the basis of the analysis, which provides a study of EU legislation on personal data protection. The concept is used to provide a systemic method of study and interpretation, which contributes to a more informative and transparent analysis of legal norms. Contextual integrity is ensured by reviewing scientific publications on research issues, that take into account various expert opinions on the new personal data protection mechanism under the GDPR.

The study is based on the review of scientific publications for 2016-2020, as a new personal data protection mechanism in the EU has been implemented since the adoption of the General Data Protection Regulation (EU) 2016/679. For analysis, the study used a search in Tandfonline and Wiley Online Library databases, which contains research on the features of the implementation of the mechanism of personal data protection, advantages and disadvantages. The following keywords were used to search for scientific publications: GDPR in EU, Data protection GDPR in EU, Data protection authorities in EU, GDPR implementation in EU,

Data protection in EU, Personal Data protection in EU, Protection of personal data in the EU.

The search for studies allowed identifying journals that have a high Impact Factor (Table 1) according to 2019 Journal Citation Reports. The journals belong to the categories of Communication, Political Science, Law. During the period of 2016-2020, 19 studies were published on the implementation of the mechanism of personal data protection in connection with the adoption of the GDPR.

Table 1: Description of research sources

Journal	Impact factor	ISI Journal Citation Reports, 2019		
		Communication	Political Science	Law
Policy & Internet (P&I)	2.763	16 / 92	27 / 180	-
European Law Journal	1.589	-	-	43 / 154
Government Information Quarterly	6,430	-	-	-
Journal of data protection & privacy	4.162	-	-	-
Biometric Security and Privacy	2.092	-	-	-

The main criteria for selecting publications were the subjects of research: the mechanism of personal data protection, tools for personal data protection, the implementation of the mechanism of personal data protection, the state of implementation of legislation on personal data protection. We made a search by keywords using filters in Wiley Online Library databases: the period of 2016-2020, keywords or key phrases, journal. The search results repeated, i.e. contained the same studies by different keywords (Figure 1-2). The search results were an intermediate step. Qualitative analysis was conducted to select publications that corresponded to the main objective of the study – assessing the current mechanism of personal data protection in the EU. As a result, publications were selected, which partially or fully reveal the results of the study of the legal provisions of implementation of the personal data protection mechanism in the EU.

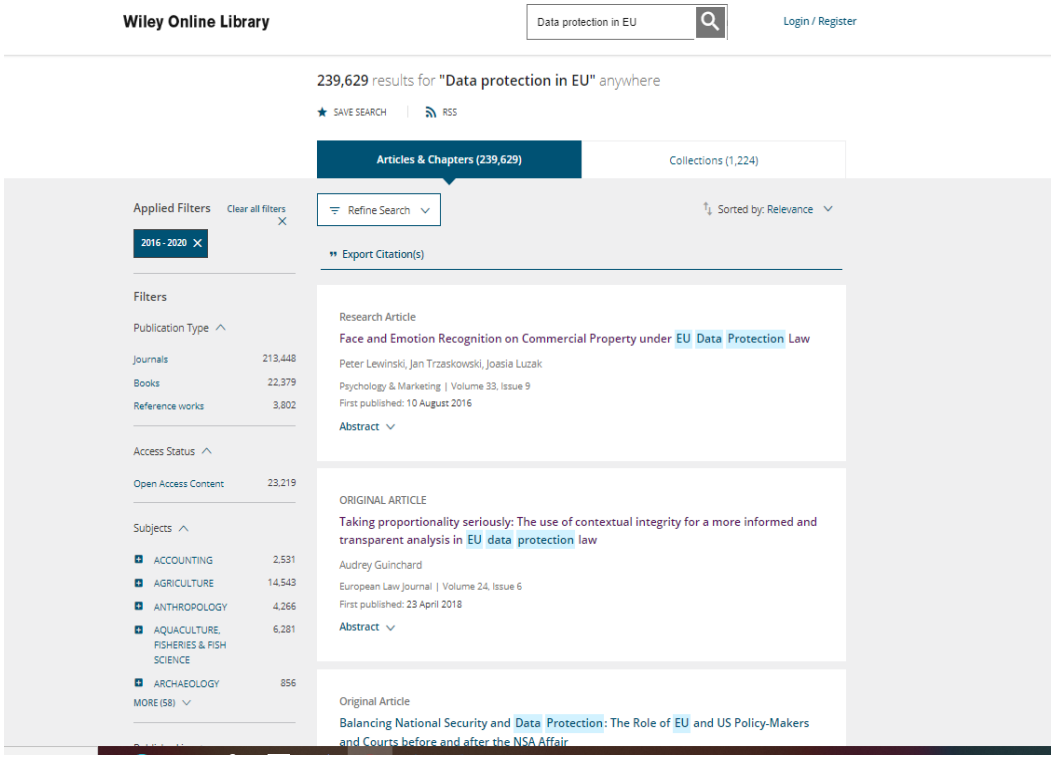

Fig. 1. Search results for publications by keywords "Data protection in EU"

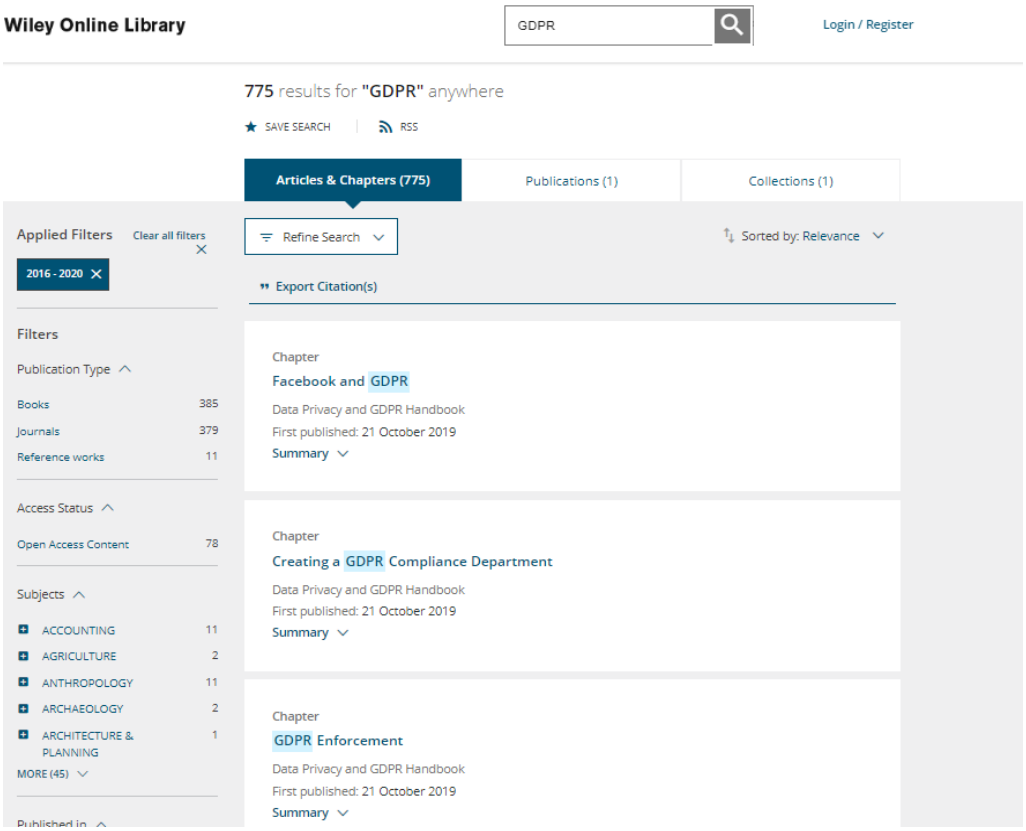

Fig. 2. Search results for publications by keywords "GDPR"

4. Results

The GDPR's entry into force provided a legal basis for the implementation of a culture of personal data privacy and protection in companies in accordance with EU standards for the first time [9]. The legal status of personal data protection is being unified, and a digital market for dissemination, exchange, control, supervision is being formed. "The development of the digital market deepened an imbalance in the relationship(s) between traders and consumers, leading to new questions as to the ethical boundaries of marketing and retailing" [8].

In June 2020, the European Commission published a report on the evaluation of the GDPR, which in particular assesses the GDPR's effectiveness in terms of functioning of the rules for the transfer of personal data to third countries and international organizations.

On May 5, 2017, the Federal Council of Germany approved the Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 and zur Umsetzung der Richtlinie (EU) 2016/680 o Bundesdatenschutzgesetz-BDSG (Federal Data Protection Act). This is the first national standard adapted to the GDPR's provisions. At the same time, in Spain, the new draft Law on Data Protection, presented in the report of the Council of Ministers on July 7, 2017, contained 78 articles on the adaptation and development of the GDPR.

The GDPR has changed approaches to personal data protection: from now on, the emphasis shifts from corporate sector data protection to personal data protection, the creation of a digital market, where the EU's role in ensuring regulation is crucial. Personal data became a new factor of production, "a new currency of change", a new protectionist legal system to strengthen the law on privacy. This legal system needs unification and harmonization in accordance with national legislation, is territorially fragmented and differentiated within the EU. The GDPR ensured the formation of a protection mechanism based on a culture of prevention and compliance with regulatory requirements in order to ensure privacy. The GDPR is the basis for the formation of personal data protection management systems, and national agencies will be responsible for the effectiveness of the protection mechanism [14].

The GDPR provides for the implementation of two new personal data protection mechanisms: the mechanism of cooperation and the mechanism of consistency and

logic [2]. GDPR and the functioning of cooperation mechanisms created an innovative management system based on independent bodies of personal data protection, their cooperation at the international level. National authorities have the right to use their powers for prevention purposes, imposing penalties, imposing time limits on the use and processing of data. The severity of the violations determines the size of the fines: from several thousand euros to millions. There is a possibility of a ban on data processing.

The new personal data protection mechanism cannot be assessed at the current initial stage of implementation in the EU. The protection authorities have, however, established cooperation based on a "single-window" mechanism and the use of mutual assistance, in particular in cross-border cooperation. "Data protection authorities developed their cooperation through the one-stop-shop mechanism and through a large use of mutual assistance. The one-stop-shop mechanism, which is a key asset of the internal market, is used to decide many cross-border cases". EU data protection authorities need human, financial and technical resources to make the mechanisms work more effectively. The situation with the development of personal data protection mechanisms is uneven, in particular due to the reason for the operation of large multinational companies in certain countries (Ireland, Luxembourg). Personal data protection authorities are the most influential, they need much more resources for the effectiveness of data protection mechanisms. In Ireland, the Netherlands, Finland, and Luxembourg, the number of employees in the field of personal data protection increased in 2016-2019 [2].

At the time of report generation all EU Member States, except Slovenia, have implemented GDPR into national law. The GDPR provides a sequence of formation of the personal data protection mechanism. This determines the fragmentary nature of the implementation of legal provisions. As a result, businesses (including multinational companies) face problems of introducing innovation, new technological developments, solving problems in the field of cybersecurity.

Another problem with the personal data protection concerns the level of harmonization of the right to protection and freedom of expression and information. Some countries determine the priority of freedom of expression, the others – the priority of data protection, exempting from this priority in certain situations (publicity of the person). In some countries, rights are balanced and assessed in specific situations. Data protection rules should not affect freedom of expression, especially in certain areas of activity (journalists, media).

The EU countries use different legal norms and approaches to regulate the right to evade the legal norms for the personal data processing. This applies, for example, to the areas of healthcare and research. This requires the implementation of a code of conduct in different areas of activity.

According to the report, "69% of the EU population above the age of 16 have heard about the GDPR and 71% of people in the EU know about their national data protection authority" [2]. This indicates an increase in public awareness of the right to access, correct, delete and other actions with personal data, increased level of transparency of use. The GDPR improved protection processes and procedures, such as the right to complain, in particular through representation, rather than litigation.

The personal data protection mechanism needs to be improved in the context of facilitating people's access to personal data, making collective decisions and reducing costs of cross-checks and customs operations. The potential for the development of the mechanism is in the personal data transfer. Thus, a person will be at the center of the digital market, will be able to choose a service provider, combining different services, choose innovative services. This will indirectly affect competition between service providers. The mobility of personal data (for example, through the technology of data transfer on printed media in real time in a virtual environment) will simplify the mechanism of data transfer. Mobility of personal data is especially relevant in the field of medicine and research.

The GDPR and the Regulation on the Free Flow of Personal Data [2] provide companies with opportunities, through competition and innovation, to ensure the free flow of data within the EU and to create a level playing field for companies established outside the EU. Personal data protection authorities provided small and medium-sized enterprises with templates for processing contracts, processing records, and hotlines for consultations in the field of data protection. Codes of conduct, certification mechanisms and standard contractual terms are tools to support small and medium-sized businesses in implementing a new personal data protection mechanism.

5. Discussion

The GDPR is becoming the global standard for how privacy and privacy protection laws should be shaped. In essence, it sets the rules which guide companies in personal data processing. Legislators cherished the idea of consent, which means companies often have to ask users for permission to use their data. The law also stipulates that third party data sharing will be more restricted since they will have to offer a reasonable explanation for why and how long they need the data and EU residents now have the right to request their personal data from companies (see Table 2).

Table 2: Summary of Data Protection Regulation in Europe

	Data Protection Regulation in Europe
Finland	New privacy regulation approved by the Finnish government in 2018 goes a step further than the GDPR protecting. The new legislation also increases the power of regulators to administer steep fines on individuals and institutions that breach the law. Based on the new law, children's date and age of consent states that public and private institutions, including individuals, will no longer be able to retrieve data of minors younger than 13 years old
Germany	Germany has historically had some of the most comprehensive data protection laws in Europe. The German Federal Data Protection Act (Bundesdatenschutzgesetz) was adopted in 1970. In the following decade, Constitutional Court drew a distinction between the right to information self-determination from the right to respect for personality. In 2001, the parliament amended the Federal Data Protection Act by creating a provision, which incorporated the recommendations of EU Directive 94/46/EC. Since 2009, Germany has had some of the strictest data protection laws in Europe. However, as the GDPR supersedes national law, German regulators are required to apply GDPR standards when necessary
France	The French Data Protection Bill was introduced by the Ministry of Justice in December of 2017. The new proposed legislation revises the previous 1978 French Date Protection Act. The new bill attempts to balance the increased need for access to personal data with the necessity to protect the privacy of some critical data, such as medical records, criminal records, data of underage citizens, genetic data, etc. In 2017, France passed a data protection law which called for the lowering of the age of consent from 16 to 15 years old. In addition, in 2018, France adopted a law that imposes hefty fines, up to 125 000 euros, on operators that fail to provide adequate data protection to users
Italy	Rather than passing new a legislation, a decree was signed in 2018 that requires data operators to comply with the GDPR by introducing new code of conducts and guidelines. The decree maintained GARANTE as the national data protection agency in charge of guaranteeing compliance with the new EU legislation. The decree also stipulates that the age of consent was reduced to 14 years old and data controllers are required to design simple, clear, concise, and objective consent forms for children
Spain	The privacy and data protection law was enacted in December of 2018. The Protection of Personal Data and the Guarantee of Digital Rights targets five specific issues: political parties and personal data processing, digital rights at work, object of the law, data subject rights, and data protection officers. The Spanish legislation goes a step beyond the EU law by offering increased personal data protection. The expansion of data rights is stipulated in the law by addressing the right of parents to access, modify, suppress, and oppose on behalf of their children
Portugal	In June of 2018, Portugal passed the Execution Law of the General Data Protection Regulation. A regulation approved by the Portuguese Data Protection National Commission lists the types of activities to be covered by the Data Protection Impact Assessment (DPIA). The purpose is to mitigate the threats posed by unnecessary exposing of personal data during the implementation of projects, systems, protocols, strategies, and policies. The types of data included are health data electronic devices, large scale profiling data, locators and trackers of individual subjects by organizations, biometric data for identification and genetic data
Netherlands	In case of the Netherlands, the GDPR replaced the Dutch Data Protection Act. The Dutch Data Protection Authority (DPA) proactively instituted rules and compliance obligations to GDPR ahead of its EU counterparts. The new rules determine that failure to comply may result in the incurrence of fines up to 1 million Euros, depending on the type and severity of the infraction. Dutch authorities also streamlined the process for individuals or companies to report data breach or misuse of data by contacting the DPA website and reporting the violation
Poland	The Polish Data Protection Act (PDPA) was passed in order to facilitate the implementation of the EU's GDPR. However, the PDPA lacks enforcement mechanisms as authorities are not allowed to institute fines when an infraction has been detected. In addition, Poland is in the process of adjusting other laws, such as telecommunications, commerce, and copyright in order to comply with GDPR. This work falls under the jurisdiction of the Ministry of Digitization. One of the concerns brought forth is the low fines instituted for public agencies, which is capped at 25 000 Euros
Denmark	In 2000, the Danish government enacted the Danish Act on Process of Personal Information in which it stated that personal data should be collected only for specific, legal and explicit reasons. It also stated that it should be accurate and not be excessive. The Danish Data Protection Act was passed in 2018 and it adopts and amends the GDPR by including in the regulation sections that were specifically designed to be interpreted by nation states

Source: [13].

Despite the huge potential for large fines imposed by regulators, there is a high level of ignorance of the GDPR provisions in the business environment. A recent survey conducted in the UK shows that only 40% of firms are aware of the new law and their own responsibilities to ensure compliance with GDPR [15, p. 45-57]. Guidelines

on data privacy and GDPR help organizations strictly adhere to legislation within the EU, the US and other countries [16].

The GDPR impose numerous restrictions and sets rules for daily data processing, external interaction with consumers and foreign countries. Elements of the GDPR are subjective [15, p. 125-192]. and may lead to the inability of some foreign countries to interact with EU countries because of data processing rules [17]. The processing of data and information under the GDPR requires a legal basis in accordance with regulation. The GDPR is centralized in the field of data collection, limiting the volume of collection, authorizing certain types of international data transfer, ensuring compliance with EU law [18]. On the one hand, the GDPR facilitate the exchange of data during intragroup processing, which requires organizations to take a more careful approach to compliance. On the other hand, the GDPR oblige for cooperation between countries, while limiting the possibility of applying foreign laws and court rulings if they do not comply with the EU's regulatory framework [15, p. 125-192].

Researchers criticize the European Court for shortcomings in identifying, at an early stage, various elements, that need to be balanced in assessing the proportionality of data processing interference with human rights for legitimate purposes pursued by data controllers. The European Court has not examined in detail the legitimate interests of data controllers in data processing or the rights of data subjects who violate such processing [19]. Thus, the weighing and discussion of these elements in the European Court was presented as inadequate and even as "impossible" [20], there was criticism of the proportionality in the constitutional court [21, 22].

As a result, the various participants who process personal data find themselves in a difficult position when it is necessary to effectively determine the line between legal and illegal data flows. The GDPR, which replaced the DPD on May 25, 2018, emphasizes the need to increase "legal and practical certainty" for all stakeholders in interpreting data protection rules, given the importance of building trust that will allow the digital economy to develop" [1]

6. Conclusion

The current personal data protection mechanism in the EU is characterized by a fundamentally new approach to data protection: human-centered and innovative in terms of personal data management. Protection authorities establish cooperation on the basis of a "single-window" mechanism and use mutual assistance, in particular, in cross-border cooperation on data protection. Given the need to implement the mechanism in all EU countries, with the exception of Slovenia, the level of flexibility and adaptability can be described as high. At the same time, the fragmentary nature of the implementation of legal provisions proves the need to increase the level of flexibility. A number of problems arise due to the peculiarities of the legislation of the EU countries, which are related to the rights to data protection and the right to freedom of expression. The priority of rights differs within the EU, which leads to differences regarding the implementation of the personal data protection mechanism. Another problem of the new mechanism concerns the problems of business (including multinational companies) in the implementation of innovations, new technological developments, solving problems in the field of cybersecurity. The current protection mechanism corresponds to the concepts of sustainable development and digital transformation, where a person is a partner of the state and has the right to dispose of their own data as a participant in the digital market and the owner of the resource in the form of personal data. The data became the new currency of exchange and the factor of production.

References

[1] European Commission: 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 (2016). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed: 20.04.2021).

[2] European Commission: Communication from the Commission to the European Parliament and the Council. Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition – Two Years of Application of the General Data Protection Regulation (2020). Available at: https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v6_1.pdf (accessed: 20.04.2021).

[3] Van Loenen, B., Kulk, S., Ploeger, H.: *Data Protection Legislation: A Very Hungry Caterpillar: The Case of Mapping Data in the European Union*. Government Information Quarterly 33(2), 338-345 (2016).

[4] Laurer, M., Seidl, T: *Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation*. Policy & Internet (2020). Available at: https://doi.org/10.1002/poi3.246 (accessed: 20.04.2021).

[5] Guinchard, A.: *Taking Proportionality Seriously: The Use of Contextual Integrity for a More Informed and Transparent Analysis in EU Data Protection Law*. European Law Journal 24(6), 434-457 (2018).

[6] Bentzen, H. B., Høstmælingen, N: *Balancing Protection and Free Movement of Personal Data: The New European Union General Data Protection Regulation.* Annals of Internal Medicine 170(5), 335-337 (2019).

[7] Ilina, E. L., Miloradov, K. A., Kovaltchuk, A. P.: 'Green Hotel': *Concepts and Implementation.* Journal of

Environmental Management and Tourism 10(2), 300-306 (2019).
[8] Lewinski, P., Trzaskowski, J., Luzak, J.: *Face and Emotion Recognition on Commercial Property under EU Data Protection Law*. Psychology & Marketing 33(9), 729-746 (2016).
[9] African Commission on Human and Peoples' Rights: Model Law on Access to Information for Africa (2013). Available at: https://www.achpr.org/legalinstruments/detail?id=32 (accessed: 20.04.2021).
[10] African Commission on Human and Peoples Rights: 362 Resolution on the Right to Freedom of Information and Expression on the Internet in Africa - ACHPR/Res. 362(LIX)2016 (2016). Available at: https://www.achpr.org/sessions/resolutions?id=374 (accessed: 20.04.2021).
[11] African Commission on Human and Peoples' Rights: Declaration of Principles on Freedom of Expression in Africa (2019). Available at: https://www.achpr.org/public/Document/file/English/draft_declaration_of_principles_on_freedom_of_expression_in_africa_eng.pdf (accessed: 20.04.2021).
[12] Ungureanu, C. T.: *Legal Remedies for Personal Data Protection in European Union.* Logos, Universality, Mentality, Education, Novelty. Section: Law 6(2), 26-47 (2018).
[13] Teatini, S. & Matinmikko-Blue, M.: *Privacy in the 5G World: The GDPR in a Datafied Society.* In: Tafazolli, R., Chatzimisios, P., Wang, C.-L. (eds.), Wiley 5G Ref: The Essential 5G Reference Online. Wiley, Hoboken (2020). Available at: https://doi.org/10.1002/9781119471509.w5GRef173 (accessed: 20.04.2021).
[14] Martínez-Martínez, D. F.: *Unification of Personal Data Protection in the European Union: Challenges and Implications*. El Profesional de la Información 27(1), 185-194 (2018).
[15] Sharma, S. (ed.): Data Privacy and GDPR Handbook. Wiley, Hoboken (2020).
[16] Kloza, D., van Dijk, N., Gellert, R., Böröcz, I., Tanas, A., Mantovani, E., Quinn, P.: Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework Towards a More Robust Protection of Individuals. Brussels Laboratory for Data Protection & Privacy Impact Assessments Policy Brief, Brussels (2017).
[17] Christou, G.: *European Union Privacy and Data Protection Policy*. In: N. Zahariadis, L. Buonanno (eds.) The Routledge Handbook of European Public Policy. pp. 179-187. Routledge, Abingdon (2017).
[18] Freitas, P. M., Moreira, T. C., Andrade, F.: *Data Protection and Biometric Data: European Union Legislation.* In: R. Jiang, S. Al-maadeed, A. Bouridane, D. Crookes, A. Beghdadi (eds.), Biometric Security and Privacy: Opportunities & Challenges in The Big Data Era. pp. 413-421. Springer, Cham (2017).
[19] Neves, A.: *Protection of Personal Data Regulation and Public Liberties: A Polyhedron with Unexpected Effects.* In: M. Tzanou (ed.) Personal Data Protection and Legal Developments in the European Union. pp. 1-18. IGI Global, Hershey (2020).
[20] Fontanelli, F.: *The Mythology of Proportionality in Judgments of the Court of Justice of the European Union on Internet and Fundamental Rights.* Oxford Journal of Legal Studies 36, 630-660 (2016).
[21] Niglia, L.: *Eclipse of the Constitution Europe Nouveau Siècle*. European Law Journal 22(2), 132-156 (2016).
[22] Tsakyrakis, S.: *Proportionality: An Assault on Human Rights?: A Rejoinder to Madhav Khosla.* International Journal of Constitutional Law 8(2), 307-310 (2010).

Tetiana L. Syroid is a Doctor of Law, Professor, Head of the Department of International and European Law, Faculty of Law, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.

Tetiana Y. Kaganovska is a Doctor of Law, Professor, Dean of the Faculty of Law, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.

Valentyna M. Shamraieva is a Doctor of Politics, Associate Professor at the Department of International and European Law, Faculty of Law, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.

Olexander S. Perederii is a PhD in Law, Associate Professor at the Department of International and European Law, Faculty of Law, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.

Ievgen B. Titov is a PhD in Law, Associate Professor at the Department of International and European Law, Faculty of Law, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.

Larysa D. Varunts is a PhD in Law, Associate Professor at the Department of Constitutional and International Law, Faculty № 4, Kharkiv National University of Internal Affairs, Kharkiv, Ukraine.