УДК 346:341(477) DOI: 10.31359/2311-4894-2018-22-2-103

ANISIMOV K. G.,
1st year student of Master in Law program of
Yaroslav Mudryi National Law University
International Law Faculty

GENERAL DATA PROTECTION REGULATION: PERSPECTIVE WAYS FOR UKRAINIAN LEGISLATION AND BUSINESS DEVELOPMENT

In the Article modern standards and requirements to processing of personal data, which are proposed by the General Data Protection Regulation, as well as nowadays Ukrainian legislation on personal data protection are analysed. At the same time, in this Article examples, when thenfulfilment of obligations is mandatory for Ukrainian companies, are represented. The author proposed some changes into a range of Ukrainian legislative acts and defined further ways of Ukrainian legislation modernisation in order to reach European standards and effective use of right on personal data protection. In addition, the author described steps, which Ukrainian companies need to make for compliance with requirements of the Regulation and proper protection of data subjects rights.

Keywords: personal data, data protection, processing of personal data, business compliance, GDPR.

I. Introduction. Within the challenges which personal data and privacy protection faces today it comes to be obvious the fact that national legislation all over the world is not able to cope with them. It worth only to remember the latest Facebook data scandal, where was revealed that Cambridge Analytica collected and used personal data of more than 50 million Facebook users without their permission in Trump's presidential campaign [1]. On this background, it seems to be very urgent the adoption and implementation of new laws in the sphere of personal data and privacy protection field.

In the European Union the role of such a piece of legislation is entrusted to 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, which is nowadays is well-known as the General Data Protection Regulation (here and after – GDPR). Basically, it is necessary to highlight that the GDPR became a legal basis for Article 8 of Charter of Fundamental Rights of the European Union realization, which declares: "Everyone has the right to the protection of personal data concerning him or her" [2].

Under the Law of Ukraine on 01.07.2010 № 2411-VI "On the Principles of Domestic and Foreign Policy" basic principles of foreign policy of Ukraine as a European state are entrenched. Therefore, in the Article 11 (2) the provision of ensuring integration of the country into the European political, economic, legal space for the purpose of membership in the European Union is provided [3]. Thus, the task of harmonization of national data protection legislation with new data protection rules and standards described by the GDPR shall be one of the vitally important goals for Ukrainian legislators.

At the same time, establishing of the GDPR rules is extremely important for Ukrainian companies due to the nature of application of Regulation. Therethrough, the Regulation has an extra-territorial scope of application, which means that it takes into account the location of the individual, whose personal data is processing, as well the location of the processing. At the same time, under the GDPR companies can be brought to responsibility for not establishing its standards and can be obliged to pay fines respectively. However, it also brings elements of unification of business activity process between Ukrainian companies and their EU counteragents, and what is more it makes Ukrainian market far more interesting and safe for further investments from the European Union.

II. Topical GDPR outlines. As it was stated by Steve Wood, ICO Deputy Commissioner: "GDPR is an evolution in data protection, not a burdensome revolution" [4]. Basically, the new EU Regulation was adopted on 27 April 2016 by European Parliament and Council of the European Union, entered into force on 24 May 2016 and will apply from 25 May 2018. By this, it repealed Directive 95/46/EC, which was the previous EU legislative act on personal data and privacy protection.

Paying attention to this fact, M. Goddard said: "One of the major changes with the new framework is that, as a Regulation, it is directly applicable, with limited scope for Member States to impose their own rules" [5].

He also mentioned, that "GDPR goes beyond current law in demanding higher standards for organisations processing data – but these higher standards are philosophically in line with best practice and ethical approaches that are practised by research practitioners" [5]. T. Erridge shares such an opinion and says: "Being a cyber-security advocate and practitioner, I think the spirit of the GDPR is genuine and it should be seen as a driver for better behaviour and best practice" [6].

At the same time, B.-J. Koops is arguing, that "the current data protection reform is on the wrong track, since it disregards the problems underlying the current lack of actual data protection in practice" [7]. Furthermore, he points: "Too much is expected from informational self-determination, which is impossible in the 21st century. Too much is expected from controllers, for whom compliance is too complex even if they want to follow the law. And too much is expected from regulating everything within a single framework of law in the books" [7].

Nevertheless, as it was already mentioned that the GDPR is applicable from 25 May 2018. Under Article 3(1) of the Regulation, it applies to "the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not" [8]. Moreover, the fact that has direct link to the Ukrainian companies is that under Article 3(2) the GDPR rules apply to the processing of personal data of data subjects, who are in the Union, by a controller or processor, which is not established in the Union in two cases: 1) 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*** 2) the monitoring of their behaviour as far as their behaviour takes place within the Union" [8]. Hopefully, the explanation of both of these situations is partly provided in recitals 23 and 24 of the GDPR respectively. Thus, to determine whereas the offering of goods or services to EU data subjects exists "it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union" [8]. It also adds: "Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention…" [8]. At the same time, recital 24 establishes monitoring the behaviour of data subjects as a process, when "natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes" [8]. As an example, usage of cookies or IP addresses to obtain information about behaviour of EU data subjects will be determined as a monitoring. However, for Ukrainian companies is necessary to understand that "behavior monitoring does not have to be aimed at individuals in the EU, but the monitored behavior must take place in the Union" [9].

III. Ways to improve legislation. As it was already mentioned in paragraph I of this article, national data protection legislation harmonization to the GDPR standards should become the prior task of Ukrainian legislator. Thus, the Constitution of Ukraine on June 28, 1996 № 254к/96-ВР (here and after – the Constitution of Ukraine) and the Law of Ukraine on June 1, 2010 № 2297-VI "On Protection of Personal Data" (here and after – the Law of Ukraine "On Protection of Personal Data") require further modernisation in the sphere of data protection. Firstly, taking into account European ambitions of Ukraine these changes shall be implemented as quickly and precise, as it possible. Secondly, establishment of effective functioning of the GDPR rules and standards on the level of national legislation will definitely raise up overall impression of Ukrainian data protection legislation among EU Member States and attract new investments from EU zone. For these purposes, it is necessary to pay attention to implementation to national legislation next provisions: 1) fundamental right on protection of personal data; 2) harmonization 'personal data' definition to the GDPR standard; 3) new general principles relating to processing of personal data; 4) establishing breach notifications.

III.1. Protection of personal data as a fundamental right

To begin with, recital 1 of the GDPR declares: "The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her" [8]. Further, in recital 4 mentioned that "the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality" [8]. However, if to refer to Chapter II of the Constitution of Ukraine, it will be impossible to define something similar to the right of protection of personal data. Thus, the Constitution guarantees to each person privacy of mail, telephone conversations, telegraph and other communication;

non-interference in personal and family life, etc. Constitutional rights and freedoms are guaranteed and cannot be abolished [10], so there is a pressing need for the right of personal data protection to be established in the Constitution of Ukraine among other fundamental rights and freedoms. At the same time, it is necessary to underline, that constitutional norms are the norms, which have direct effect [10]. So, integrating the right of person for protection of his or her personal data into the Constitution of Ukraine will have positive consequences which lead to ensuring higher standards of data protection in Ukraine, creating a legislative basis for implementing best examples of European data protection practices, etc.

III.2. 'Personal data': how to define?

The definition of 'personal data' in national legislation can be found in the Law of Ukraine "On Protection of Personal Data". It is considered to be information or a set of information about natural person that is identified or can be directly identified [11]. However, this definition in comparison to the one established in the GDPR is too narrow, so is not able to protect personal data of citizens within the European standards and needs urgent harmonization. Thus, under the GDPR personal data definition covers "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" [8]. Further examples of what is considered to be 'personal data' provided: a name and surname; a home address; an email address such as name.surname@company.com; an identification card number; location data (for example the location data function on a mobile phone); an Internet Protocol (IP) address; a cookie ID; the advertising identifier on data subject's phone; data held by a hospital or doctor, which could be a symbol that uniquely identifies a person [12]. So, it is necessary to agree with J. Krystlik on the fact that "the scope of 'personal data' has broadened considerably and now includes any information relating to a person" [13]. Implementation of 'personal data' definition under the GDPR into the Law of Ukraine "On Protection of Personal Data" is important to fulfill due to the fact that modern one is not all the aspects, so a lot of information, e.g. information, by which is possible indirectly identify person, is not a 'personal data', which leads to the ineffective protection of data subjects and making them vulnerable to nowadays cyber-threats.

III.3. Implementation of new principles

Under the Law of Ukraine "On Protection of Personal Data" such principles relating to processing of personal data as 'lawfulness, fairness and transparency', 'purpose limitation', 'accuracy' and 'storage limitation' are already ensured [11]. However, in this case the GDPR also represents a few new principles for Ukrainian data protection legislation, which broaden legislation in this sphere and deepen protection respectively. So, it is necessary to pay the attention to the principle of 'integrity and confidentiality' of data processing and the general principle of 'accountability' implementation.

Firstly, Article 5 (1(f)) defines 'integrity and confidentiality' as a data processing "in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures" [8]. Basically, this principle represent one of the main ideas of the GDPR, as it was formulated by … "motivating companies to secure their systems to avoid data breaches where possible and effectively reporting on them when mitigation has failed" [14]. So, on the background of rapid technological changes this idea seems to be effective and appropriate to data processing. Of course, it obliges data controllers and processors to specific rules of processing, however, it is adequate measures for such a sensitive information as personal data they are working with.

Secondly, under Article 5 (2) "the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1" [8], what is also known as a principle of 'accountability'. Consequently, it leads to the obligation of data controllers to establish and represent compliance programs and strategies. At the same time, this principle is important for implementation, because it can bring to Ukrainian legislation concept of privacy by design and by default [8] and make to rethink the deepness of the responsibility of companies for the safety of personal data of data subjects in national legislation and doctrine.

III.4. Breach notification

Article 33 of the GDPR represents personal data breach notification requirement, which means that "in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" [8]. C. Tankard highlights the fact that "prior to the GDPR, there has been no uniform legislation regarding breach notification… the GDPR introduces mandatory breach notification unless the breach is unlikely to result in a risk to the rights and freedoms of the data subjects concerned" [15]. It is impossible to miss such a serious concept, because without establishing such rules Ukrainian legislation will be not considered to be as the one, which "ensures an

adequate level of protection" [8]. Thus, it will require expenses from data controllers for the compliance, however, it provides better level of personal data and privacy protection regarding to the fact the governmental bodies will take part in prevention of possible breaches in short terms and data subjects will not stay alone in such a situation.

IV. Recommendations for Ukrainian companies

In the part II of this article were already mentioned situations, when Ukrainian companies can fall under the scope of GDPR. For non-compliance with new rules or for their infringement, they will be liable under Article 83 of the GDPR, which represents a system of administrative fines. However, in the nearest future all Ukrainian companies, who are controlling or processing any kind of personal data, shall adopt GDPR practices. And it is not a question of possible fines, but of companies' comfortable existence on the market. Thus, S. Hooson states: "The GDPR aims to clarify the responsibilities of organisations relating to the data they handle and store, thus making it easier for both European and non-European companies to comply and avoid penalties" [16]. So, the GDPR goes by the way of unification rules, by creating general standards, clarification rights and obligations of data processing relations subjects and establishing unified fines policy as well. Ukrainian companies in this issue shall pay attention for compliance with next requirements of the Regulation, which are the most essential in nowadays data protection: 1) establishing representative in the European Union; 2) creating a Data Protection Officer; 3) composing a code of conduct.

IV.1. A representative in the EU

Article 27 of the GDPR directly poses the requirement of setting up representatives of controllers or processors not established in the Union. Thus, Article 27(3) requires: "The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are" [8]. However, the GDPR does not determine in which for shall the representative exist, shall it be natural person or legal entity. Article 27(1) only mentions that such a representative shall be designated in writing. Basically, the best solutions for Ukrainian companies is to join their forces to create legal entities, which can professionally and highly qualified represent them in the EU Member States. It can save the money and efforts of companies, but at the same time the GDPR requirements will be met.

IV.2. Data Protection Officer

Data Protection Officer (here and after – DPO) shall be designated under section 5 of the GDPR. It is obligatory in next situations: "(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10" [8]. Furthermore, it is suggested in Article 37(2) to companies to designate one DPO from these companies, if a DPO in this case will be "easily accessible from each establishment" [8]. S. Hooson points that the DPO, basically, "will act as an internal data protection compliance auditor" [16]. At the same time, he adds, that nowadays is an extremely important for businesses "to invest in training up an individual to act as its DPO" [16]. It is necessary to agree with this fact, because the GDPR requires from the DPO to be designated "on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39" [8]. Nevertheless, companies, which are data controllers or processors, are free to decide whether the DPO will be their staff member or it is better for them to make a service contract for the DPO tasks provision [8]. In addition, Article 39(1) requires from the DPO minimum of tasks, which he or she shall be ready to cope with, however, which can be extended be controller or processor company. This Article includes next obligatory tasks: "(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; (d) to cooperate with the supervisory authority; (e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter" [8]. So, establishment the position of the DPO in companies will take some efforts and investment, however, for some companies, as it was already mentioned above, it is obligatory steps, but others can by such measures deepen security of own system and provide better protection for theirs data subjects, which is the best way of overall improvement data protection in Ukraine.

IV.3. Code of conduct

Under Article 40 of the GDPR it is important to encourage the drawing up of codes of conduct, due to the fact that it ensures proper application of the Regulation [8]. J. Krystlik supports this idea of proper application and mentions that code of conduct shall uphold "the collection of personal data and information communicated to the public and concerned individuals" [13]. Moreover, the GDPR provides controllers and processors with a list of what is possible and adequate to include to theirs codes of conduct: "(a) fair and transparent processing; (b) the legitimate interests pursued by controllers in specific contexts; (c) the collection of personal data; (d) the pseudonymisation of personal data; (e) the information provided to the public and to data subjects; (f) the exercise of the rights of data subjects; (g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained; (h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32; (i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects; (j) the transfer of personal data to third countries or international organisations; or (k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79" [8]. So, the list is quite long and covers the most important spheres of data protection. However, it is appropriate for companies, because it simply encourages company to establish their policy in a clear manner, which will be easy to follow. Moreover, the companies will not stay along facing composing such a code, but will be provided with help and advices by EU bodies, due to the fact, that Member States are also interested in deep realisation of GDPR principles.

V. Conclusion. The General Data Protection regulation became one of the major changes in personal data and privacy protection nowadays. Created to establish 'privacy by design' and 'privacy by default', it directly touches not only Ukrainian business, but Ukrainian legislation as well. However, representing challenges for compliance with its rules and principles, it represents new ways for Ukrainian society development in the sphere of data protection. Thus, there is a vital need of the implementation of such general concept into the Constitution of Ukraine, as 'right to protection of personal data' as a fundamental right, in order to guarantee proper data protection and create a direction for further its improvement in national legislation. Nevertheless, Law of Ukraine "On Protection of Personal Data" also needs improvement of general provisions to be adequate to European level of data protection. As it was mentioned in this article, primarily the definition of 'personal data' and principles of data processing shall be modernised and reach to the GDPR standards. Furthermore, national legislator shall pay an attention to the creation 'breach notification' as a new institution of law, which is considered to become an effective way to avoid a breach of rights and freedoms of data subjects and opens ways for international cooperation and legal help, if such a breach will take place. At the same time, some Ukrainian companies shall be ready to represent compliance with the GDPR requirements, which basically includes designation of the representative in the EU Member States, the Data Protection Officer and elaboration Codes of conduct. To conclude, integral and deep modernisation of national data protection legislation in above-mentioned directions with implementation latest standards, represented by the GDPR, ensure the development of Ukraine as a safe and law-bound state, proper protection of the rights and freedoms of data subjects, as well as make a huge step for further European integration.

SOURCES

1. Rosenberg M., Confessore N., Cadwalladr C., Dance G., Hakim D. How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*: March 18, 2018. URL: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html#click=https://t.co/UAg1Q5t1BG (Last accessed: 10.06.2018).
2. Charter of Fundamental Rights of the European Union. 2012/C, 326/02. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN (Last accessed: 10.06.2018).
3. Про засади внутрішньої та зовнішньої політики : Закон від 01.07.2010 р. № 2411-VI. URL: http://zakon3.rada.gov.ua/laws/show/2411-17 (дата звернення: 10.06.2018).
4. Wood S. GDPR is an evolution in data protection, not a burdensome revolution (legal blog by ICO Deputy Commissioner). URL: https://www.hampshirechamber.co.uk/ICO%2025.8.pdf (Last accessed: 10.06.2018).
5. Goddard M. The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research 2017*: November 1, 2017. Vol. 59, Issue 6. URL: http://journals.sagepub.com/doi/pdf/10.2501/IJMR-2017-050 (Last accessed: 12.06.2018).

6. Mansfield-Devine S. Data protection: prepare now or risk disaster. *Computer Fraud & Security 2016:* December 2016. Vol. 2016, Issue 12. P. 5–12. URL: https://www.sciencedirect.com/science/article/pii/S1361372316300987#cesec110 (Last accessed: 12.06.2018).
7. Koops B.-J. The trouble with European data protection law. *International Data Privacy Law 2014*: November 11, 2014. Vol. 4, No. 4. P. 250–261. URL: https://is.muni.cz/auth/el/1422/jaro2018/SOC022/um/59943709/International_Data_Privacy_Law-2014-Koops-250-61.pdf (Last accessed: 12.06.2018).
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN (Last accessible: 13.06.2018).
9. Schonhofen S., Detmering F. Territorial applicability of the GDPR. *Business Law Magazine 2018*: March 1, 2018. No. 1. P. 3–5. URL: https://www.businesslaw-magazine.com/2018/02/28/territorial-applicability-of-the-gdpr/ (Last accessed: 13.06.2018).
10. Конституція України: Закон від 28.06.1996 р. № 254к/96-ВР. URL: http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 10.06.2018).
11. Про захист персональних даних: Закон від 01.06.2010 р. № 2297-VI. URL: http://zakon0.rada.gov.ua/laws/show/2297-17 (дата звернення: 10.06.2018).
12. What is personal data? (European Commission answers). URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (Last accessed: 10.06.2018).
13. Krystlik J. With GDPR, preparation is everything. *Computer Fraud & Security 2017*: 21 June, 2017. Vol. 2017, Issue 6. P. 5–8. URL: https://www.sciencedirect.com/science/article/pii/S1361372317300507 (Last accessed: 10.06.2018).
14. Zerlang J. GDPR: a milestone in convergence for cyber-security and compliance. N*etwork Security 2017*: 21 June 2017. Vol. 2017, Issue 6. P. 8–11. URL: https://www.sciencedirect.com/science/article/pii/S1353485817300600 (Last accessed: 12.06.2018).
15. Tankard C. What the GDPR means for businesses. *Network Security 2016:* 29 June, 2016. Vol. 2016, Issue 6. P. 5–8. URL: https://www.sciencedirect.com/science/article/pii/S1353485816300563 (Last accessed: 11.06.2018).
16. Hooson S. Smarten your data security before new EU legislation or risk corporate loss. *Network Security 2015*: 12 June, 2015. Vol. 2015, Issue 6. P. 8–10. URL: https://www.sciencedirect.com/science/article/pii/S1353485815300489?via%3Dihub (Last accessible: 12.06.2018).

REFERENCES

1. Rosenberg, M., Confessore, N., Cadwalladr, C., Dance, G., Hakim, D. (March 18, 2018). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*. URL: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html#click=https://t.co/UAg1Q5t1BG (Last accessed: 10.06.2018).
2. Charter of Fundamental Rights of the European Union. 2012/C, 326/02. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN (Last accessed: 10.06.2018).
3. Pro zasady vnutrishnoi ta zovnishnoi polityky: Zakon vid 01.07.2010 r. № 2411-VI. URL: http://zakon3.rada.gov.ua/laws/show/2411-17 (data zvernennia: 10.06.2018).
4. Wood, S. GDPR is an evolution in data protection, not a burdensome revolution (legal blog by ICO Deputy Commissioner). URL: https://www.hampshirechamber.co.uk/ICO%2025.8.pdf (Last accessed: 10.06.2018).
5. Goddard, M. (November 1, 2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research 2017*, Vol. 59, Issue 6. URL: http://journals.sagepub.com/doi/pdf/10.2501/IJMR-2017-050 (Last accessed: 12.06.2018).
6. Mansfield-Devine, S. (December 2016). Data protection: prepare now or risk disaster. *Computer Fraud & Security 2016,* Vol. 2016, Issue 12, 5–12. URL: https://www.sciencedirect.com/science/article/pii/S1361372316300987#cesec110 (Last accessed: 12.06.2018).
7. Koops, B.-J. (November 11, 2014). The trouble with European data protection law. *International Data Privacy Law 2014*, Vol. 4, No. 4, 250–261. URL: https://is.muni.cz/auth/el/1422/jaro2018/SOC022/um/59943709/International_Data_Privacy_Law-2014-Koops-250-61.pdf (Last accessed: 12.06.2018).
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive

95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN (Last accessible: 13.06.2018).
9. Schonhofen, S., Detmering, F. (March 1, 2018). Territorial applicability of the GDPR. *Business Law Magazine 2018*, No. 1, 3–5. URL: https://www.businesslaw-magazine.com/2018/02/28/territorial-applicability-of-the-gdpr/ (Last accessed: 13.06.2018).
10. Konstytutsiia Ukrainy: Zakon vid 28.06.1996 r. № 254k/96-VR. URL: http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (data zvernennia: 10.06.2018).
11. Pro zakhyst personalnykh danykh: Zakon vid 01.06.2010 r. № 2297-VI. URL: http://zakon0.rada.gov.ua/laws/show/2297-17 (data zvernennia: 10.06.2018).
12. What is personal data? (European Commission answers). URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (Last accessed: 10.06.2018).
13. Krystlik, J. (21 June, 2017). With GDPR, preparation is everything. *Computer Fraud & Security 2017*, Vol. 2017, Issue 6, 5–8. URL: https://www.sciencedirect.com/science/article/pii/S1361372317300507 (Last accessed: 10.06.2018).
14. Zerlang, J. (21 June 2017). GDPR: a milestone in convergence for cyber-security and compliance. N*etwork Security 2017*, Vol. 2017, Issue 6, 8–11. URL: https://www.sciencedirect.com/science/article/pii/S1353485817300600 (Last accessed: 12.06.2018).
15. Tankard, C. (29 June, 2016). What the GDPR means for businesses. *Network Security 2016,* Vol. 2016, Issue 6, 5–8. URL: https://www.sciencedirect.com/science/article/pii/S1353485816300563 (Last accessed: 11.06.2018).
16. Hooson, S. (12 June, 2015). Smarten your data security before new EU legislation or risk corporate loss. *Network Security 2015*, Vol. 2015, Issue 6, 8–10. URL: https://www.sciencedirect.com/science/article/pii/S1353485815300489?via%3Dihub (Last accessible: 12.06.2018).

АНИСИМОВ К. Г.,
студент 1-ого курса магистратуры Международно-правового факультета
Национального юридического университета Украины имени Ярослава Мудрого

ОБЩИЙ РЕГЛАМЕНТ ПО ЗАЩИТЕ ДАННЫХ: ПЕРСПЕКТИВНЫЕ ПУТИ РАЗВИТИЯ ДЛЯ УКРАИНСКОГО ЗАКОНОДАТЕЛЬСТВА И БИЗНЕСА

В статье проанализированы современные стандарты обработки персональных данных и требования к ним, которые предложены Общим регламентом про защиту данных и введены в действие в Европейском Союзе, а также современное состояние законодательства Украины относительно защиты персональных данных. В то же время, приведены примеры, когда исполнение требований Регламента является обязательным для украинских компаний. Автором статьи предложены изменения в ряд нормативно-правовых актов Украины и намечены пути дальнейшей модернизации законодательства с целью достижения европейских стандартов и эффективного использования права на защиту данных лица. Определены шаги, которые необходимо осуществить для достижения комплаенса с требованиями Регламента и надлежащей защиты субъектов персональных данных.

Ключевые слова: персональные данные, защита данных, обработка персональных данных, комплаенс бизнеса, ОРЗД.

АНІСІМОВ К. Г.,
студент 1-ого курсу магістратури Міжнародно-правового факультету Національного юридичного університету імені Ярослава Мудрого

ЗАГАЛЬНИЙ РЕГЛАМЕНТ ІЗ ЗАХИСТУ ДАНИХ: ПЕРСПЕКТИВНІ ШЛЯХИ РОЗВИТКУ ДЛЯ УКРАЇНСЬКОГО ЗАКОНОДАВСТВА ТА БІЗНЕСУ

Постановка проблеми. Набрання чинності Загальним регламентом із захисту даних впливає не лише на країни-члени Європейського Союзу та їхнє законодавство, а й на Україну. На тлі євроінтеграційних процесів стає необхідним запровадження новітніх європейських стандартів захисту персональних даних, запровадження додаткових вимог до їх обробки та переосмислення місця володільців і розпорядників персональних даних щодо

обов'язків з приводу належного захисту прав суб'єктів персональних даних.

Метою дослідження є теоретичне опрацювання законодавства ЄС щодо обробки персональних даних, зокрема, детальний розгляд ЗРЗД у контексті його впливу на українське законодавство та українські компанії-володільці та компанії-розпорядники персональних даних, та вироблення практичних порад і рекомендацій щодо імплементації нових стандартів в українське законодавство, пропозицій до українських компаній задля забезпечення комплаєнсу із нормами ЗРЗД.

Аналіз останніх досліджень. У статті проаналізовані праці європейських вчених-юристів, а також правників-практиків, що стосуються аналізу положень ЗРЗД та їхнього впливу на законодавство. Так, були проаналізовані роботи Goddard M., Tankard C., Hooson S., Krystlik J., Koops B.-J. та інших.

Виклад основного матеріалу. Проаналізовано загальну структуру ЗРЗД та звернена увага на новели, що були запропоновані у Регламенті. Викладено детальний аналіз нововведень щодо принципів обробки персональних даних, закріплення інституту 'повідомлень про порушення' та наведені можливості їх подальшої імплементації у законодавство України. Запропоновано гармонізацію національної термінології з європейською, зокрема, підкреслена необхідність модернізації визначення персональних даних. Далі, автором проаналізовані шляхи досягнення комплаєнсу українських компаній до вимог ЗРЗД та окреслені конкретні дії, які повинні бути виконані, як наприклад створення посади Офіцера із захисту даних, забезпечення представництва компанії у ЄС тощо.

Висновки. Українське законодавство та бізнес мають рухатися у подальшому напрямку європейської інтеграції та забезпечувати новітні стандарти обробки персональних даних. З цією метою необхідними є ретельна гармонізація термінології та загальних принципів, утвердження на території України права на захист персональних даних як фундаментального права людини, імплементація прогресивних правових інститутів, що забезпечують належний захист суб'єктів персональних даних.

Ключові слова: персональні дані, захист даних, обробка персональних даних, комплаєнс бізнесу, ЗРЗД.