УДК 342.721(045)

Kh. V. Kmetyk,
PhD (Law)

DATA PROTECTION IN THE EU

National Aviation University
Kosmonavta Komarova Avenue, 1, 03680, Kyiv, Ukraine
E-mail: khkmetyk@gmail.com

***Purpose**: to research the processing by an individual, a company or an organization of personal data relating to individuals in the EU. **Methods**: documentary analysis and synthesis, comparative analysis, objective truth, cognitive-analytical, etc. **Results**: an author made a conclusion that the EU General Data Protection Regulation is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market. A single law will also do away with the current fragmentation in different national systems and unnecessary administrative burdens. **Discussion**: clarified main rules of the EU General Data Protection Regulation as an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business.*

***Keywords**: an individual; processing; data; the GDPR; EU.*

Introduction. After a long and intense reform, the EU adopted the new 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) [1; 2].

According to the Article 4 of the General Data Protection Regulation (GDPR), "processing" means any operation or a set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. And "personal data" means 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 [1].

With the GDPR, the EU reaffirms its attachment to the protection of fundamental rights and freedoms of individuals, notably those related to the protection of individuals' privacy including the specific fundamental right to personal data protection enshrined within the Charter of the Fundamental Rights of the EU [3] and within the primary EU law Treaty on the Functioning of the EU [4], as well as its willingness to accelerate the achievement of the internal market for which the free flow of personal data is essential, for commercial and non-commercial relationships. The GDPR aims to harmonise the rules for all the Member States in order to reduce the legal fragmentation, complexities and uncertainties that existed between Member States under the Data Protection Directive. The ultimate goal of the GDPR is to create legal certainty and sustainability of the data protection measures in a technological neutral approach. Without fundamentally changing the approach to the field compared to what existed previously with the Directive of 1995, the GDPR performs several updates and introduces some new individual rights and procedures of importance.

Analysis of the latest research and publications. The problem of personal data protection in EU is not-enough researched in the Ukrainian sci-

entific literature. However, some authors considered some aspects of such issue, among them we can point K.S. Melnyk [5; 6], O.G. Rogova [7], V.M. Bryzhko [8], etc.

Purpose of a research is to research the processing by an individual, a company or an organization of personal data relating to individuals in the EU.

Presenting main material. Regulation (EU) 2016/679 of the European Parliament and of the Council, the European Union's (EU) new General Data Protection Regulation (GDPR), regulates the processing by an individual, a company or an organization of personal data relating to individuals in the EU. The GDPR entered into force on 24 May 2016 and applies since 25 May 2018 [1].

The GDPR does not apply to the processing of personal data of deceased persons or of legal persons. The rules do not apply to data processed by an individual for purely personal reasons or for activities carried out in one's home, provided there is no connection to a professional or commercial activity. When an individual uses personal data outside the personal sphere, for socio-cultural or financial activities, for example, then the data protection law has to be respected.

Any information that relates to an individual, as an identified or identifiable, living individual, falls under the GDPR. This includes for example an individual's name, home address, ID card number, Internet Protocol (IP) code and information on his/her health. Some sensitive data, such as data concerning an individual's health, racial or ethnic origin, political opinions and sexual orientation, has special protection.

The GDPR only apply to personal data about individuals, they do not govern data about companies or any other legal entities. However, information in relation to one-person companies may constitute personal data where it allows the identification of a natural person. The GDPR also apply to all personal data relating to individuals in the course of a professional activity

The GDPR apply when an individual's data is collected, used and stored digitally or in a structured filing system on paper. There is one set of rules for the whole of the EU, which can be complemented in some areas by national legislation. This means that an individual have the same rights whomever in the EU he/she give your data to. And companies from outside the EU are not exempt. If they offer goods and services in the EU or if they monitor an individual's behaviour in the EU then they have to give him/her the same level of data protection.

The GDPR helps an individual to take control of this information through several key rights, giving him/her greater power to protect himself/herself, in particular:

– the right on information about the processing of his/her personal data;

– the right to access his/her data. It means that an individual has the right to request access to the personal data an organization has about his/her, free of charge, and obtain a copy in an accessible format. For example, an individual bought a fitness tracker and subscribed to a health app that monitors his/her activity, and he/she can ask the app operator for all the information processed on him/her. This includes all subscription data (such as his/her name and contact details where relevant) and all information collected about him/her through the tracker (such as heart rate, performance, etc.);

– the right to object to the processing of an individual's personal data for marketing purposes or on grounds relating to his/her particular situation. It means that if an organization is processing an individual's personal data he/she may have the right to object. However, in some circumstances, public interest may prevail. This could be the case for scientific or historical research. An individual also has the right to object at any time to receiving direct marketing. For example, an individual bought two tickets online to see his/her favourite band play live. Afterwards, he/she is bombarded with adverts for concerts and events that he/she are not interested in. An individual informs the online ticketing company that he/she does not want to receive further advertising material. The company should stop processing him/her data for direct marketing and, shortly afterwards, he/she should no longer receive emails from them. They should not charge he/she for this;

– the right to correct his/her incorrect, inaccurate or incomplete personal data. Errors in an individual's personal data can have a significant impact on

his/her life, particularly when applying for loans, insurance, credit and so on. If an individual believes that personal data held by an organization might be incorrect, incomplete or inaccurate he/she can ask for it to be corrected. This should be done without undue delay. For example, and individual applies for a new insurance policy but notice the company mistakenly records him/her as a smoker, increasing his/her life insurance payments. In such case an individual has the right to contact them and get this corrected;

– the right to have data deleted and to be forgotten. It means that where an individual's consent has been requested to process his/her data, he/she can ask the organization to stop processing it by withdrawing his/her consent. They should do so if they have not relied on any other legal grounds for processing his/her data. It should be as easy to withdraw consent as it is to give it. If an individual's data is no longer needed or is being processed unlawfully then he/she can ask for the data to be erased. However, other EU rights, like freedom of expression, should also be safeguarded. Controversial statements made by people in the public eye, for example, may not automatically be deleted if the public interest is best served by keeping them online. Organizations should delete personal data collected from a child that is processed through an app or a website on request. For example, when an individual types his/her name into an online search engine, the results include links to an old newspaper article about a debt he/she paid long ago. If an individual is not a public figure and his/her interest in removing the article outweighs the general public's interest in accessing the information, the search engine is obliged to delete the links;

– the right to have a say when decisions are automated. In this case, an individual also has the right to express his/her point of view and to contest the decision. Some organizations, such as banks, tax offices and hospitals, use algorithms to make decisions about an individual using his/her personal data. It is efficient for them, but not always transparent and these decisions may affect an individual legally or have another significant impact on his/her life. In those cases, organizations should: tell an individual if their decision is automated; give an individual the right to have the automated decision reviewed by a person; let an individual contests the automated decision. Automated decisions are allowed in some circumstances, for example, when a particular law allows it. For example, an individual applies for a loan with an online bank. He/she are asked to insert his/her data and the bank's algorithm tells him/her whether the bank will grant him/her the loan and gives the suggested interest rate. An individual should be informed that he/she may: express his/her opinion; contest the decision; and ask for a person's input in the process to review the algorithm's decision;

– the right to move an individual's data. It means to receive an individual's personal data in a machine-readable format and send it to another controller. If an individual's data are used by a company after he/she gave his/her consent or signed a contract, then he/she can ask for it to be returned to him/her or transmitted to another company whose services he/she would like to use – this is called the right to "data portability". The original supplier, such as a social media company, bank or even healthcare provider, has to transmit the data to the new supplier. Moving data should help an individual to access other markets and suppliers more easily, and so give him/her more choice. For example, an individual has to found a cheaper electricity supplier. He/she can ask his/her existing supplier to transmit his/her data directly to the new supplier, if it is technically feasible. In any case, they should return individual's data to him/her in a commonly used and machine readable format so that it can be used on other systems.

To exercise an individual's rights he/she should contact the company or organization processing his/her personal data, also known as the controller. If the company/organization has a Data Protection Officer (DPO) an individual may address his/her request to the DPO. The company/organization should respond to his/her requests without undue delay and at the latest within one month. If the company/organization does not intend to comply with his/her request they should state the reason why. An individual may be asked to provide information to confirm his/her identity (such as, clicking a verification link, entering a username or password) in order to exercise his/her rights.

The type and amount of personal data a company/organization may process depends on the reason for processing it (legal reason used) and the intended use. The company/organization should respect several key rules, including:

– personal data should be processed in a lawful and transparent manner, ensuring fairness towards the individuals whose personal data is being processed ("lawfulness, fairness and transparency");

– there should be specific purposes for processing the data and the company/organization should indicate those purposes to individuals when collecting their personal data. A company/organization can not simply collect personal data for undefined purposes ("purpose limitation");

– the company/organization should collect and process only the personal data that is necessary to fulfil that purpose ("data minimisation");

– the company/organization should ensure the personal data is accurate and up-to-date, having regard to the purposes for which it is processed, and correct it if not ("accuracy");

– the company/organization can not further use the personal data for other purposes that are not compatible with the original purpose;

– the company/organization should ensure that personal data is stored for no longer than necessary for the purposes for which it was collected ("storage limitation");

– the company/organization should install appropriate technical and organizational safeguards that ensure the security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technology ("integrity and confidentiality").

– If the consent provided by a person prior to the application of the GDPR is in line with the conditions of the GDPR, then there is no need to ask again for the individual's consent. The company/organization has to make sure that the consent given before the GDPR meets the conditions set out in the GDPR [9].

Data must be stored for the shortest time possible. That period should take into account the reasons why a company/organization needs to process the data, as well as any legal obligations to keep the data for a fixed period of time. For example, national labour, tax or anti-fraud laws requiring you to keep personal data about all employees for a defined period, product warranty duration, etc.

The company/organization should establish time limits to erase or review the data stored.

By way of an exception, personal data may be kept for a longer period for archiving purposes in the public interest or for reasons of scientific or historical research, provided that appropriate technical and organizational measures are put in place (such as anonymization, encryption, etc.).

The company/organization should also ensure that the data held is accurate and kept up-to-date.

At the time of collecting their data, an individual should be informed clearly about at least:

– who a company/organization is (its contact details, and those of its DPO if any);

– why a company/organization will be using his/her personal data (purposes);

– the categories of personal data concerned;

– the legal justification for processing his/her data;

– for how long the data will be kept;

– who else might receive it;

– whether their personal data will be transferred to a recipient outside the EU;

– that he/she have the right to a copy of the data (right to access personal data) and other basic rights in the field of data protection;

– his/her right to lodge a complaint with a Data Protection Authority (DPA);

– his/her right to withdraw consent at any time;

– where applicable, the existence of automated decision-making and the logic involved, including the consequences thereof.

The information may be provided in writing, orally at the request of an individual when identity of that person is proven by other means, or by electronic means where appropriate. A company/organization should do that in a concise, transparent, intelligible and easily accessible way, in clear and plain language and free of charge.

A company/organization is also required to inform the individual of the categories of data and the source from which it was obtained including if it was obtained from publicly accessible sources.

The DPA are independent public authorities that supervise, through investigative and corrective

powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints lodged against violations of the GDPR and the relevant national laws. There is one in each EU Member State [10].

The GDPR provides the DPA with different options in case of non-compliance with the data protection rules:

– likely infringement – a warning may be issued;

– infringement: the possibilities include a reprimand, a temporary or definitive ban on processing and a fine of up to €20 million or 4% of the business's total annual worldwide turnover.

It is worth noting that in the case of an infringement, the DPA may impose a monetary fine instead of, or in addition to, the reprimand and/or ban on processing.

The DPA should ensure that fines imposed in each individual case are effective, proportionate and dissuasive. It will take into account a number of factors such as the nature, gravity and duration of the infringement, its intentional or negligent character, any action taken to mitigate the damage suffered by individuals, the degree of cooperation of the organization, etc. [11]

Conclusions. The GRDP is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market. A single law will also do away with the current fragmentation in different national systems and unnecessary administrative burdens. These rules apply across the EU, regardless of where the data is processed and where the company is established.

The GDPR reinforces cooperation duties and transparency between the actors of the processing, internally and with regard to the supervisory authorities, which should create a more integrated EU data protection system and diminish some useless administrative costs by decentralising elements of the data protection governance towards data controllers and processors.

References

1. 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). Available at: https://eur-lex. europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016 R0679 &from=EN# d1e1384-1-1.

2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri= CELEX:31995L0046&from=EN.

3. Charter of fundamental rights of the European Union, 2000, consolidated version. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/ PDF/ ?uri= CELEX: 12012P/ TXT &from=EN.

4. Treaty on the functioning of the European Union, 2009, consolidated version. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/ PDF/?uri= CELEX:12012E/TXT&from=EN.

5. Melnyk K.S. Inozemnyi ta vitchyznianyi dosvid stanovlennia instytutu zakhystu personalnykh danykh. *Informatsiina bezpeka liudyny, suspilstva, derzhavy*. 2013. № 2 (12). S. 97–103.

6. Melnyk K.S. Udoskonalennia normatyvno-pravovoho rehuliuvannia zakhystu personalnykh danykh v Ukraini. *Pravova informatyka*. 2014. № 1 (41). S. 30–44.

7. Rohova O.H. Zakhyst personalnykh danykh u zakonodavstvi Yevropeiskoho Soiuzu ta Ukrainy. *Teoriia ta praktyka derzhavnoho upravlinnia*: zb. nauk. pr. Kharkiv: Vyd-vo KharRI NADU «Mahistr», 2011. Vyp. 3 (34). 512 s.

8. Bryzhko V.M. Zakhyst personalnykh danykh: realii ta praktyka suchasnosti. *Informatsiia i pravo*. 2013. № 3 (9). S. 31–49.

9. The EDPB guidelines on Consent under Regulation 2016/679. Available at: https://ec.europa.eu/ newsroom/article29/item-detail.cfm?item_id= 623051.

10. Data Protection in the EU. Available at: https://ec.europa.eu/commission/sites/beta-political/ files/data-protection-overview-citizens_en.pdf.

11. The EDPB Guidelines on the application and setting of administrative fines for the purposes of Regulation (EU) 2016/679. Available at: https://ec.

europa.eu/newsroom/article29/item-detail.cfm? item_id=611237.

References

1. 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). Available at: https://eur-lex. europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016 R0679&from=EN# d1e1384-1-1.

2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri= CELEX:31995L0046&from=EN.

3. Charter of fundamental rights of the European Union, 2000, consolidated version. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/ PDF/?uri= CELEX:12012P/TXT&from=EN.

4. Treaty on the functioning of the European Union, 2009, consolidated version. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/ PDF/?uri=CELEX: 12012E/TXT&from=EN.

5. Мельник К.С. Іноземний та вітчизняний досвід становлення інституту захисту персональних даних. *Інформаційна безпека людини, суспільства, держави*. 2013. № 2 (12). С. 97–103.

6. Мельник К.С. Удосконалення нормативно-правового регулювання захисту персональних даних в Україні. *Правова інформатика*. 2014. № 1 (41). С. 30–44.

7. Рогова О.Г. Захист персональних даних у законодавстві Європейського Союзу та України. *Теорія та практика державного управління*: зб. наук. пр. Харків: Вид-во ХарРІ НАДУ «Магістр», 2011. Вип. 3 (34). 512 с.

8. Брижко В.М. Захист персональних даних: реалії та практика сучасності. *Інформація і право*. 2013. № 3 (9). С. 31–49.

9. The EDPB guidelines on Consent under Regulation 2016/679. Available at: https://ec.europa.eu/ newsroom/article29/item-detail.cfm?item_id= 623051.

10. Data Protection in the EU. Available at: https://ec.europa.eu/commission/sites/beta-political/ files/data-protection-overview-citizens_en.pdf.

11. The EDPB Guidelines on the application and setting of administrative fines for the purposes of Regulation (EU) 2016/679. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

Х. В. Кметик

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ЄС

Національний авіаційний університет
проспект Космонавта Комарова, 1, 03680, Київ, Україна
E-mail: khkmetyk@gmail.com

Мета: *дослідити обробку фізичною особою, компанією чи організацією персональних даних, що стосуються фізичних осіб в ЄС.* ***Методи:*** *документальний аналіз та синтез, порівняльний аналіз, об'єктивна істина, когнітивно-аналітичний тощо.* ***Результати:*** *25 травня 2017 року в Європейському Союзі вступили в силу нові правила захисту персональних даних – Загальний регламент захисту даних. Цей Регламент не оновлювався ще з 1995 року. Персональні дані – це процес, який невід'ємно супроводжує комерційну активність. Цей процес нікуди не зникне, він буде завжди і буде супроводжувати будь-яку комерційну діяльність. Мета законодавства з питань захисту персональних даних та, зокрема, регламенту – це надати можливість суб'єктам персональних даних контролювати цей процес, знати де, ким, коли, з якою метою вони обробляються, що їхні персональні дані захищаються відповідно до регламенту і у разі, якщо персональні дані обробляються незаконно, вони можуть захистити свої права щодо цього. Автор робить висновок про те, що Загальний регламент ЄС захисту даних є важливим кроком для зміцнення основних прав людей у цифрову епоху та полегшення бізнесу шляхом уточнення правил для компаній і державних органів на єдиному цифровому ринку. Зміни торкнулися безлічі країн, включно з Україною. Тепер перелік прав громадян країн ЄС значно розширився. Так, вони мають право бачити, яку інформацію про них має та чи інша компанія, а самим компаніям за витік або розголошення персональних даних загрожують великі штрафи. Новий Регламент має на меті захист всіх громадян ЄС від порушень конфіденційності та втручання в персональні дані. Разом вони створюють більш чіткі і ефективні умови для бізнесу. Суть Регламенту ще і в тому, що він має наднаціональний характер. Тобто поширюється абсолютно на всі країни ЄС і на ті, які входять в Європейську економічну зону. До того ж, компанії з інших країн, які обробляють дані громадян, які живуть на цих територіях (наприклад, онлайн-магазини, туроператори тощо), також повинні виконувати всі правила.* ***Обговорення:*** *роз'яснені основні правила Загального регламенту ЄС захисту даних як важливий крок для зміцнення основних прав фізичних осіб у цифрову епоху та полегшення умов здійснення бізнесу.*

Ключові слова: *фізична особа; обробка; персональні дані; Загальний регламент ЄС захисту даних; ЄС; дані.*