SAFETY&DEFENSE
ISSN 2450-551X

The Protection of Individuals in the light of EU Regulation 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data

Mirosław TOKARSKI
Military University of Aviation, Dęblin, Poland;
m.tokarski.mil.pl, ORCID: 0000-0003-1882-668X

DOI: https://doi.org/10.37105/sd.86

Abstract

The process of establishing normative acts in the European Union does not occur out of nowhere, but in the context of specific social needs. That was the case of the genesis of establishing legal regulations regarding the protection of personal data in the European Union. Socio-economic integration, which resulted from the functioning of internal market in the European Union, has led to a significant increase in cross-border transfers of personal data. It led to situation in which various economic operators or state institutions of the Member States have increasingly processed the personal data of the EU citizens. Within time, these data have become an equally valuable commodity - not to say even more valuable – compared to goods and services (Costa-Cabral, and Lynskey Orla, 2017, p. 11). Making use of personal data on a large scale especially by public and private entities, associations and companies over time has posed a threat to the security of personal data. This has made it necessary to introduce legal protection measures for personal data in the European Union that would eliminate the negative effects of any form of personal data processing. The purpose of this article is to evaluate legal regulations regarding legislative protection of personal data in the European Union against the background of EU Regulation 2016/679 of the European Parliament and the Council with respect to the protection of individuals due to processing personal data, its free movement and repealing Directive 95/46/EC (hereinafter referred to as Regulation 2016/679). Due to initially adopted purpose of the considerations there arose a problem which was formulated in the form of a question: Do the legal measures introduced by the Regulation constitute an effective tool for the protection of personal data in the event of a violation of the law by personal data administrators and entities while processing such data? The presented purpose of the considerations and the research problem determined the order of the analysis.

Keywords: Protection, Security, Personal data, European Union.

1. Introduction

Although discrepancies in the protection of personal data in individual countries of the European Union were a natural consequence of state independence and the sovereignty of national legislators, the persistence of such implemented procedures in the long run was a highly undesirable phenomenon. Not only did it weaken the feeling of legal security of natural persons whose data were processed, but above of all, it denoted uncertainty when referred to their legal situation. The meaning to ensure uniformity in the field of personal data security became therefore a value of significant social importance. A member of the European Union had the right to expect proper interpretation and application of regulations in a predictable and equal manner throughout the European Union area. On the other hand, the state authorities were obliged to shape the direction and the content of provisions in such a way that they could be brought as close as possible to the ideal of uniformity and consistency in the field of personal data protection. Therefore, it needs to be stressed that the collection and processing of citizens' personal data by various entities did not use to ensure their security, but often threatened their privacy (Robinson, et al., 2009, p. 1). In this situation, an attempt was made to introduce a stable and coherent framework for the protection of citizens' personal data throughout the Union and the legal mechanisms for its enforcement. This was expressed in Regulation 2016/679. It needs to be noted that according to Article 4 (1) of the Regulation, "personal data" denotes any information related to an identified or identifiable natural person they refer to. On the other hand, protection of personal data was defined as "a set of legal provisions aimed at protecting the rights, freedoms and interests of natural persons whose personal data can be collected, stored, processed, distributed, destroyed, etc." (Dove, 2018, p. 5). In this way, the protection of personal data has become one of the fundamental rights in the European Union. It should be noted that the effectiveness of legal norms in the field of personal data protection and the rights of the subjects is not determined by the mere introduction of normative provisions on personal data protection procedures, but it is also influenced by establishing effective mechanisms towards their enforcement (Pantlin et al., 2018). Even a brief analysis of the Regulation 2016/679 reveals that it plays a key role for people whose personal data are processed by the administrator and entities that further process personal data. It retains the main principles of personal data protection included in the Directive 95/46 / EC of 1995 (Directive, 1995) and it contains corrections referred to obedience and enforcement of these data over the area of the European Union. At this point, it should be clarified that according to the above-mentioned regulation, the "data administrator" is "a natural or legal person, public authority, agency or other body that either single acting or jointly with others determines the purposes and means of processing personal data" (Article 4, Act 7). Conversely, "the processor" means here a natural or legal person, public authority, an entity or other entity that processes personal data on behalf of the administrator (Article 4, Act8). In this context, normative solutions aimed at implementing the rights of citizens to protection of their personal data and the guarantees that processing such data will be carried out in accordance with the law prove to be significantly important. The protection of personal data introduced by the regulation applies to both private and public persons. At the same time, the legal regime of the regulation defined the rights of persons whose data are processed and it imposed obligations on personal data administrators and entities processing such data.

An extremely important solution of the mentioned regulation mentioned above was the introduction of legal protection measures for people whose personal data are being processed. In reference resources, legal measures are defined as: a procedural institution by means of which authorized entities may demand verification of legal status or actions performed in the course of proceedings by the body conducting such procedures (Przybysz, 2020). In that way, legal actions may be taken up by an individual and denote a possibility, not an obligation, to act in order to change the legal situation of a natural person. Such measures may become a tool to defend the interests of an individual; and, as a result, he or she becomes the subject not the object of any actions (Pierzchała, 2013, p. 123). Referring to the term "legal measures" found in Regulation 2016/679, two groups of legal measures can be distinguished where a natural person is entitled to make the use of them against the entity processing his/her personal data: legal protection measures in connection with implementation of operational programs using personal data and administrative legal protection measures in connection with violating personal data regulations. It should be noted that in addition to the indicated legal measures, the EU legislator introduced in its Regulation 2016/679 regulations on the liability of subjects contravening provisions on the protection of personal data. These regulations are further discussed below.

2. Principles of personal data processing

Confronting the legal articles referred to in Regulation 2016/679 with practical experience reveals that normative solutions towards the protection of personal data are increasingly being followed by administrators and subjects that process them. Nevertheless, a lot of controversy has arisen around this issue, concerning the principles of personal data protection and liability for their violations. Since ignorance of them may further lead to the imposition of financial sanctions on the administrator or the subject processing personal the data, it is worth mentioning them in their original form.

According to Art. 5 of the Regulation, the following rules apply to the processing of personal data:

1) processing should be lawful, fair and transparent for the data subject (González-Fuster, 2014, p. 102);
2) collecting data for further processing must result from a specific and legitimate purpose and adequate to it;
3) processing should comprise only up-to-date personal data, whereas outdated data should be deleted or put right;
4) processed personal data should be stored for no longer than it is necessary for the purpose of processing;
5) processing personal data should be secured against accidental loss, destruction or damage by appropriate technical or organizational measures.

The presented rules for the processing of personal data are accepted in related subject literature. As argued, negligence or conscious actions of the subjects during data processing has resulted in negative effects for those whose data had been processed. For this reason, it was necessary to introduce rules securing personal data contained in a data filing system in relation to their automated or manual processing (Comforte AG, 2018, p. 7).

It needs to be clearly emphasized that the right to protect personal data is not an absolute right: it should be perceived in its social function and balanced against other fundamental rights in the context of their proportionality. That results from Art. 89 of the Regulation, which allows for derogation from the main principle of personal data protection due to the need of processing it

for archival purposes in the public interest, scientific, historical or statistical research.

In the field references, it was emphasized that the indicated exceptions are allowed, provided that appropriate technical and organizational safety measures are introduced by the administrator and the subject processing such personal data (Ducato, 2020, p. 5).

It needs to be clarified that these are not the only restrictions on the protection of processed personal data. Namely, personal data protection is excluded from the regulation's jurisdiction due to activity related to national security and the processing of personal data by the Member States based on activities related to common foreign and security policy of the Union. The protection provided by the regulation also excludes personal data processing by a natural person within a purely personal or domestic activity, without any connection with a professional or commercial activity. It needs to be stressed that any personal or domestic activity should be understood as correspondence and the storage of addresses, maintaining social bonds and any Internet activity undertaken towards such activities. However, the provisions of the Regulation may apply to administrators or entities processing personal data if they make the means of processing personal data available either for personal or domestic purposes. In the light of the presented regulations, it can be concluded that the rules on personal data processing are undoubtedly the most prominent example of "federal EU law in the field of personal data security of natural persons (Lenaerts, and. Gutiérrez-Fons, 2010, p. 1631).

3. Subjectively and objective scope of personal data protection

Directive No.14 of Regulation 2016/679 indicates that protection concerning personal data processing should apply to natural persons, regardless of their nationality or place of residence. Also, the provision included in Article 8 Section 1 of the Charter of Fundamental Rights of the European Union (Official Journal, 2012) and Article 16 Section 1 of the Treaty on Functioning of the European Union (Official Journal, 2012) provide that every person has the right to the protection of his/her own personal data. Such legal articles become more significant as they create the principle of equality before the law when referring to personal data protection. It means that all natural persons whose personal data are processed should be treated equally, according to the same measure, without discriminating or favoring differences.

The Directive corresponds to its second counterpart of Regulation 2016/679, which requires that the legal articles on the protection of individuals with regard to processing of their personal data, regardless of their nationality, place of residence should not violate their fundamental rights, freedoms and the right to protection of personal data.

Considering this, actions undertaken by the administrator of personal data and subjects processing them should be conducted in such way so as not to cause negative effects in the sphere concerning the person whose data is processed, provided that he or she is a citizen of the European Union member country.

Directive No. 11 of Regulation 2016/679 states that this is the personal data which become the subject of legal protection with reference to natural persons. It does not apply to all data, but only these which allow identification of a natural person based on his name and surname, identification number, location data, online identifier or just factors determining physical, physiological, genetic, mental, economic, cultural or social identity of that person. In addition, it concerns personal data about the natural person who previously presented it to an administrator.

It should be emphasized that according to Article 4 Point 2 of the Regulation, processing of personal data denotes a wide scope. It either includes one or more operations performed with the use of personal data or personal data sets in an automated or manual manner. The range of processing such data may comprise: collecting, recording, organizing, storing, adapting or modifying, downloading, making use, revealing by sending, circulating or other ways of sharing, adjusting or combining, limiting, deleting or removing personal data.

In terms of the range of its impact, the protection of personal data processing has an extended territorial scope (Dove, 2018, p. 5). It includes activities carried out by the organizational unit of the administrator or the subject processing data within the territory of the Union and outside its borders. Such protection also applies to processing the personal data of people residing in the Union by the administrator or the subject converting information which is not officially established in the EU once the processing activities involve offering goods, services or monitoring their behavior in the territory of the Union. In addition, the protection extends to processing personal data by an administrator which is not established in the Union but in a place where the law of a Member State is applicable under public international law.

4. Legal protection measures related to personal data processing during the implementation of operational programs

Generally, processing personal data during the implementation of operational programs is directed towards original personal data. In order to avoid violating the security of the data mentioned above, the EU legislator allowed for possibility of processing personal deprived of elements which might identify its owner by means of "pseudonymization" or "anonymization". In the light of Article 4 Section 5 of the "pseudonymization" regulation, it is based on the concept of processing personal data in such way that it can no longer be attributed to the data subject without the use of any additional information. By contrast, "anonymization" refers to a technique that removes personal information from certain sets of data. However, if it occurs that following the processing of the data in connection with implementation of operational programs, a security breach has been found, a natural person then has the right to request: access to his personal data and rectification; the deletion or limitation of their processing; the transfer of personal data; an objection claim towards processing of personal data.

1) The right to access and rectify personal data allows for the possibility of posing to the administrator or the subject processing the data the question: what personal data are processed and where were they obtained, what is the purpose of processing, what is its legal basis and how long will the data be processed. Once the processed information is out of date, the person may request to update it.

2) The right to request the deletion or limitation of personal data processing becomes effective when further processing is no longer necessary to achieve the purpose indicated by the administrator or processor, or it was processed against the law. Restricting personal data processing may result in the administrator of personal data or the subject processing data being able to store such information. However, they are not only allowed to transfer data to other subjects, modify or delete it. Restricting the processing of personal data may be also implemented in the event of an objection against data processing until the objection is previously examined.

3) The right to withdraw consent to personal data processing may be implemented at any time, if the basis for data processing is the agreed consent. Withdrawing consent has the effect that current data being processed cannot be considered as an unlawful act. It has been pointed out in the field references that personal data processing may be performed on the basis of the approved consent of the data subject, therefore it is necessary to ensure that he or she makes a deliberate choice when referred to sharing personal data (Rubinstein, 2013, p. 78).

4) The right to transfer the data to another administrator is based on the concept of demanding the transfer of personal data from one administrator who previously owned such data to another appointed owner. The primary purpose of the data transfer regulation is to increase individuals' control over their personal data and to ensure that they play an active role in the data ecosystem (Graef, et al., 2918, p. 1365).

5) The right to file an objection referred to personal data processing becomes effective once the basis for data processing is the performance of the administrator's public tasks or its legitimate interests. The objection should result in ceasing personal data processing by the administrator, unless he/she demonstrates the existence of legitimate grounds for data processing which are superior to the interests, rights and freedoms of the data subject.

The presented legal protection measures in connection with the implementation of operational programs based on the use of personal data are generally available. This translates into possibility of using any of the discussed legal actions by a natural person, regardless his intellectual, physical or financial conditions.

5. Administrative and judicial remedies in connection with violation of the articles referring to personal data protection

As it was already mentioned in the introduction, European Union countries have recorded a massive amount processed personal data, commonly introduced even against the will of the people these data referred to. On the other hand, natural persons have become more and more aware of the use of their personal data for commercial purposes (Robinson et al., 2009, p. 7). In order to meet the needs of the personal data protection of natural persons, the EU legislator introduced Regulation 2016/679 which allowed for legal protection measures of administrative and judicial nature in relation to subjects violating rules on the protection of personal data. It needs to be pointed out that the term "infringement of provisions on personal data" denotes a broad meaning and it includes any action which contradicts the regulation along with the acts which allow for its implementing (Polanowski, and Lasek, 2018).

Thanks to the presented legislative procedure, the natural person whose personal data has been violated has the right to undertake legal protection in the form of: the right to file a complaint addressed to the supervisory body; the right to bring a lawsuit against a supervisory authority; the right to file a claim in court against the administrator or processing subject; the right to compensation.

1) The right to file a complaint addressed to the supervisory authority, in accordance with Art. 77 of the Regulation 2016/679 is allowed to any person in the Member State of his residence, place of work or place of committing the infringement, if he decides that processing his/her personal data is in conflict with the regulation discussed. It should be clarified that in the light of

Article 4 Point 21, the "supervisory authority" has the status of an independent public authority established by the Member State to protect fundamental rights and freedoms of natural persons with regard to personal data processing. Such a provision imposes an obligation on the supervisory body to inform the person making the complainant about the progress and effects on the examined case.

2) The right to legal protection in a court against a supervisory authority, in accordance with Art. 78 of Regulation 2016/679 is offered to any natural or legal person against the decision of the supervisory authority that concerns him. The right becomes effective in a situation where the supervisory authority has not dealt with the complaint or the petitioner has not been informed within a three month period about the progress or effects of his complaint, and the processing of personal data is still in conflict with the regulation. Proceedings against a supervisory authority shall be brought before the court of the Member State where the supervisory authority is established.

3) The right to legal protection before a court against the administrator or processor in accordance with Article 79 of Regulation 2016/679 is possessed by every data subject if he/she considers that his/her rights have been violated as a result of personal data processing. According to this regulation, proceedings taken up against the administrator or the personal data processor are initiated before the court of the Member State in which the administrator or the processor is established. It should be emphasized that the provision of Article 79 of Regulation 2016/679 also allows for the initiation of proceedings in the court of the Member State in which the aggrieved party is residing, unless the administrator or the processor are public authorities of the Member State using their powers.

4) Every natural person is entitled to compensation based on Article 82 of Regulation 2016/679, if he/she has suffered material or non-material damage as a result of violation of rules referred to personal data protection. The right to compensation is effective in the event of any loss suffered caused by the administrator or the data processor. According to this regulation, every administrator involved in the processing is liable for the loss caused by the processing. On the other hand, the processor is liable for any losses caused by processing only when obligations related to data processing were not fulfilled or he/she acted in way that is contrary to the instructions issued by the administrator. However, either the administrator or processing information entity shall be released from liability once they prove that they were not at fault for the circumstances that led to its initiation. When it occurs that more than one administrator or processor is involved in the processing of personal information, then all the sites involved become jointly and severally liable for the entire loss. If the administrator or the personal data subject has paid compensation for the entire damage caused, he has the right to request from the other administrators or processors who participated in the same processing scheme, partial compensation corresponding to the part of the damage the subjects were responsible for. Actions taken up for damages are sent to a court in a particular Member State.

It needs to be stressed that the starting point for any application of the presented legal protection measures was the specification of the subject of personal data protection and its scope in Regulation 2016/679. Providing the protection of personal data with a normative character has resulted in the possibility of introducing specific measures aimed at enforcing the lawful actions of administrators and entities processing personal data. They were

manifested in legal protection measures of an administrative and judicial nature in connection with the violation of the provisions on personal data. In this way, a natural person who has suffered a breach of his own personal data can effectively oppose entities that have violated the provisions on the protection of personal data.

6. Administrative fines

The Article No. 83 of the Regulation introduced a procedure for imposing administrative fines by the supervisory authority in the event of a breach of personal data security by the administrator or the data processing entity. He/she needs to bear in mind that Regulation 2016/679 does not apply to the processing information considered as anonymous, but only data relating to a specific natural person (Lindgren, 2015, p. 241). Moreover, the quoted regulation is ineffective against data which were previously agreed on for further processing by given consent of its owner.

However, if the processing of personal data is based on invalid consent, there is no legal basis for their processing by any entity (Helberger et al., 2917, p. 25). In consequence, illegal activity will result in imposing an obligation to pay an administrative fine. According to the Directive 2016/679, the administrative fee should be effective, proportionate and it should discourage from further infringement of violating the regulation.

According to Article 83 Section 2 of the Regulation, the administrative fine imposed may be independent or combined with legal measures taken by a supervisory authority against the administrator or data processing subject in the form of:

1) warning about the possible breach of personal data security during processing;
2) ordering the fulfillment of the data subject's request;
3) reminders in the event of violation of legal articles on data processing;
4) ordering the adjustment of the processed data to applicable legal articles;
5) ordering the administrator to notify the data subject about a breach of data protection;
6) introduce temporary or total restriction towards data processing, including given prohibition;
7) ordering the rectification, deletion of personal data, restriction of further processing and notification of these actions to recipients whose personal data have been revealed;
8) withdrawal of certification or ordering the certifying subject to withdraw certification or not to grant certification if the requirements are not met or they are no longer fulfilled;
9) ordering the suspension of data flow to a recipient in a third country or to an international organization.

The presented set of legal measures reveals that neglecting duties through unlawful data processing can be very severe. In the light of Article 83 Section 2 of the discussed Regulation, administrative fines may be imposed taking into account:

1) the nature, weight and duration of the violation, number of people who suffered the situation and the extent of the loss;
2) intentional or unintentional nature of the violation;
3) actions taken by the administrator or processor to minimize the loss suffered by the data subjects;
4) the degree of responsibility of the administrator or the subject processing personal data;
5) identified previous violations on the side of the administrator or the subject processing personal data.

Moreover, according to the applicable procedure, when imposing an administrative fine, a supervisory authority is obliged to take into account the following:

1) the degree of cooperation with the supervisory authority in order to remove violation and alleviate its possible negative effects;
2) categories of the personal data the violation concerned;
3) the way the supervisory authority learned about the breach;
4) financial benefits gained directly or indirectly in connection with the breach of personal data security.

It should be noted that according to Article 83 Section 2 of Regulation 2016/679 also specifies the method of imposing the amount of an administrative fine. Based on that article, once an administrator or subject processing data intentionally or unintentionally infringes a few of the articles of this Regulation in the processing operation, the total amount of administrative fine may amount to EUR 20 million. Imposed financial sanctions for any indicated violations are deliberate. The lowest fine is equal up to EUR 10 million or 2% of the total annual turnover of the previous financial year and it applies to infringements of the provisions related to: obligations of the administrator and the subject processing the data, obligations of the certifying subject, obligations of the monitoring subject. In that case, the prerequisite for applying a penalty is administrative inconsistency, which is treated less severely than any direct violation of the privacy of the data subjects.

On the other hand, violation of the articles which might concern: basic principles of processing, including the conditions of consent, the rights of data subjects, the transfer of personal data to a recipient in a third country or an international organization, non-compliance with an order, temporary or final limitation of processing or suspension of data flow ordered by supervisory authorities – this all allows for imposing an administrative fine up to EUR 20,000,000. In the case of a company, it may amount up to 4% of its total annual worldwide turnover based on previous financial year record, however it is the higher one which is usually taken into consideration.

In the event of non-compliance with the order stated by a supervisory authority, an administrative fine is imposed at the amount of up to EUR 20,000,000, and referred to a company – it equals up to 4% of its total annual worldwide turnover based on the previous financial year's records, and it is the higher amount which is applied.

On the basis of the presented procedure of imposing administrative fines, there is no doubt that the protection of data of natural persons to whom they refer (Comforte AG, 2018, p. 1) becomes effective, as it provides for direct interference in the event of a violation of the articles of Regulation 2016/679. In that meaning, a personal data protection instrument aims at shaping the manner of using personal data by various types of entities in accordance with standards set by the EU legislator for all countries within the European Union.

It should be added that in a situation where the legal system of a Member State does not provide imposing administrative fines, then in accordance with the discussed regulation, application of the fine is requested by a competent supervisory authority and it is imposed by a competent state court. In that case, the same principle is applied which means that the imposed fine on the perpetrator must be effective, proportionate and dissuasive - against further violation of the law on personal data protection.

7. Conclusions

Summing up, this article focuses on the assessment of legal protection measures for personal data in the European Union against the background of Regulation (EU) 2016/679 of the European Parliament and of the Council. The conducted analysis allows for concluding that the problem formulated

in the form of a question: Do the legal measures introduced by the regulation constitute an effective tool towards protection of personal data in the event of violation the law by personal data administrators and other subjects during processing of such data and whether it has been positively solved.

First of all, referring to the problem question, it needs to express an opinion that the point of intersection between protection of personal data and legal regulations concerning legal protection measures enclosed within Regulation 2016/679 coincides with social expectations of the European Union citizens. In that way, the law goes beyond theoretical assumptions and is part of the procedural approach which assumes that enforcement is autonomous and independent of the will of administrators and other legal subjects regarding protection of personal data.

The model of administrative or judicial proceedings against subjects violating the articles referred to personal data protection is based on the assumption that there is a need to synchronize the procedures preventing violations of the law in all countries which are members of the European Union. In this context, it needs to be stated that specificity of the principles contained in Regulation 2016/679 makes that the incorporated system of personal data protection of natural persons is stable. In addition, it constitutes a detailed regulatory system that forces personal data administrators and subjects using such information to apply lawful practices in the field of personal data processing.

Thanks to provisions of Regulation 2016/679, processing personal data is based on a voluntary consent of the data owner. Thus, it enables eliminating consent to further data processing in an insidious manner. For example, it may be achieved by forcing confirmation of the addressee consent on the Internet system using the phrase "I agree" appearing on the computer screen, without the possibility of familiarizing with the content of the offer or advertisement. As a consequence of the agreed solutions, voluntary consent to processing personal data is required, which cannot be rescinded by the data processor itself (Hoofnagle, et al., 2019, p. 86). Thus, the personal data protection measures introduced by Regulation 2016/679 become an effective tool to fight entities violating its articles in a stateless sense. First of all, it has led to eliminating any normative gaps in the existing legal systems of the Member States in the field of personal data protection. Thanks to such kind of solution, there is coherence in the legal system in the field of personal data protection among the European Union member states. At the same time, the principles introduced constitute the basis for interpretation of provisions referred to protection of personal data contained in the regulation. Moreover, they enable us to refer to legal regulations based on articles regarding the prevention of unlawful acts of personal data processing when using legal remedies.

Providing a catalogue of legal measures in Regulation 2016/679 aimed at protection of personal data referring to natural persons in a situation in which a personal data administrator or any other subject processes information against legally binding articles is an extremely important normative solution. In that way, each natural person, in order to avoid the negative effects of unlawful data processing, may effectively demand that further processing to be stopped or demand that his/her identifying features be removed.

References

1. Charter of fundamental rights of the European Union (Official Journal of the European Union (C 326/391, 26.10.2012).
2. Costa-Cabral, F., Lynskey, O. (2017). Family ties: the intersection between

data protection and competition in EU Law. Common Market Law Review, Kluwer Law International, Available online http://eprints.lse.ac.uk/68470/.
3. 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 (Official Journal L 281, 23/11/1995).
4. Dove, E.S. (2018) The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era, *Journal of Law*, 46(4). pp. 1013-1030. DOI: 10.1177/1073110518822003
5. Ducato, R. (2020). Data protection, scientific research, and the role of information, *Computer Law & Security Review*, 37.DOI: https://doi.org/10.1016/j.clsr.2020.105412
6. González-Fuster, G. (2014) How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection, *IDP Revista de Internet Derecho y Política*, 19. DOI: 10.7238/idp.v0i19.2424
7. Graef, I., Husovec M., Purtova N. (2018), Data Portability and Data Control: Lessons for an Emerging Concept in EU Law. *German Law Jurnal,* 19(6). DOI:https://doi.org/10.1017/S2071832200023075
8. Helberger, N., and Borgesius, F.Z. and Reyna, A. (2017), The perfect match? a closer look at the relationship between EU consumer law and data protection law, Commo*n Market Law Review*, 54(5).
9. Hoofnagle, Ch.J., and van der Sloot, B. and Borgesius, F.Z. (2019) The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28, pp. 65-98, Published online: 10 Feb 2019. DOI:10.1080/13600834.2019.1573501.
10. Lenaerts, K., and Gutiérrez-Fons J.A. (2010). The constitutional allocation of powers and general principles of EU law. Powers and general principles, *Common Market Law Review*, 47, pp 1629-1669.
11. Lindgren, P. (2016). GDPR Regulation Impact on Different Business Models and Businesses, J*ournal of Multi Business Model Innovation and Technology*, 4(3). DOI: 10.13052/jmbmit2245-456X.434
12. Pantlin, N., Wiseman, C., Everett, M. (2018). Supply chain arrangements: The ABC to GDPR compliance - A spotlight on emerging market practice in supplier contracts in light of the GDPR*, Computer Law & Security Review*,34(4). DOI: https://doi.org/10.1016/j.clsr.2018.06.009
13. Pierzchała, E. (2013). *Standardy funkcjonowania administracyjnych środków prawnych w postępowaniu przed organami pomocy społecznej,* Wrocław: Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.
14. Polanowski, A. and Lasek, Ł. (2018), *Private enforcement under the GDPR*, newtech.law., https://translate.google.com/translate?hl=pl&sl=en&tl=pl&u=newtech.law (Access 2018.07.10).
15. Przybysz, P.M. (2012). Administracyjne środki prawne w postępowaniu egzekucyjnym w administracji, https://sip.lex.pl/komentarze-i-publikcje/monografie/administracyjne-środki-prawne-w-postepowaniu-egzekucyjnym-w-369243969 (Access 14.07.2020).
16. 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 (Official Journal of the European Union L 119/1, 4.5.2016).
17. Robinson, N., Graux H., Botterman M., Valeri L. (2009*), Review of the European*

Data Protection Directive, RAND Corporation - Office of the Information Commissioner.
18. Rubinstein, I., Big Data: The End of Privacy or a New Beginning? (October 5, 2012). International Data Privacy Law (2013 Forthcoming), NYU School of Law, *Public Law Research Paper*, 12-56, Available at SSRN: https://ssrn.com/abstract=2157659 or http://dx.doi.org/10.2139/ssrn.2157659 Treaty on the Functioning of the European Union (Official Journal C 326, 26/10/2012, P. 0001 – 0390).
19. Three Key Risks and Opportunities of GDPR (2018), Comforte AG. https://www.comforte.com/resources-detail/news/whitepaper-three-key-risks-opportunities-of-gdpr/. (Access 20.08.2020).