Data Protection Reform in the EU as a Part of the Forming Digital Single Market

Daniela Ježová*

Summary: The article deals with the first milestone of the digital market formation which is the very discussed data protection reform and GDPR. I highlighted the most important changes in the protection of personal data in the European Union.

Keyworlds: Data protection – reform – changes – GDPR – Digital market

1. Introduction

European Union founds important to extend the current EU single market, which consist of free movement of goods, services, labour and capital. The single market makes the EU territory without any barriers. Currently four freedoms included in the internal market needs to reflect the development of the society and the digital era. After creating the Digital Single Market, the European Union can enjoy its full potential. The creation of a Digital Single Market is definitely a priority of the Union. Data protection reform is an important part of the formation of digital single market where the goal is to make the covers the European Union without any digital barriers. For reaching this goal firstly we need to make our date safe.

The Personal Data Protection Reform includes General Data Protection Regulation adopted in April 2016 and will apply from 25 May 2018 and the Directive that Member States have to transpose into their national law by 6 May 2018.[1] The Regulation replaces the original Data Protection Directive

* Daniela Ježová, Assistant professor, Comenius University in Bratislava, Slovakia. Contact: daniela.jezova@flaw.uniba.sk

[1] Regulation (EU) 2016/679 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 and directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

no. 95/46/EC from 1995. This unified legal regulation at European Union level will replace the current non-uniform national regulation of the Member States of the Union.

2. General Data Protection Regulation

The Regulation is primarily aimed at strengthening the rights of individuals to protect their personal data and to reduce the administrative burden associated with their protection. Another aim is to enable the free flow of personal data in the digital single market area. The Regulation also has a positive impact on increasing consumer legal certainty and improving competition in the European Union.

The aim of the Regulation is to guarantee a consistent level of protection of individuals throughout the Union and to avoid differences which impede the free movement of personal data within the internal market. The Regulation provides legal certainty and transparency for economic subject, including small and medium enterprises. The Regulation also provides individuals with the same level of protection of rights in all Member States and, on the other hand, sets equal sanctions in all Member States. On the contrary, the Regulation does not apply to the processing of personal data of legal persons. The purpose of the Regulation is to harmonize national laws on the personal data protection across the EU while addressing new technological developments without the need for implementation into national rules.

2.1. The most important changes in the personal data protection

2.1.1. Definition of the personal data

Personal data is defined in the Regulation as any information concerning an identified or identifiable natural person (hereinafter referred to as „the data subject"); identifiable natural person is a person who can be identified directly or indirectly, in particular by reference to an identifier such as name, identification number, location data, online identifier, or a reference to one or more elements specific to physical, physiological, genetic, mental , economic, cultural or social identity of that individual. Under this term can be understood, for example, an online identifier such as the IP address of the natural person, localization data. This is an expanding definition of personal data in order to ensure the protection of any identifiability of a natural person.

The regulation does not tell us about the entity that identifies a natural person based on the data in question, it is essential that identification is possible. Identification can also be done by combining multiple data, not all data must be necessarily available to the operator. It is necessary to consider whether there are absolute or relative criteria for determining the possible identifiability of a natural person based on data. If we used the absolute criterion to determine the possible identifiability of a natural person[2], it would mean that it would be data if anyone could associate this data with a particular person. The Court of Justice in its decision Breyer[3] stated that the possibility of a personal data with the other information at the disposal of this person is a mean that can reasonably be used to identify the data subject. However, this does not happen when the identification of the data subject is prohibited by law or virtually impossible, for example because it would require a disproportionate amount of time, finance or human resources, so that the probability of identification actually appears to be negligible. However, this decision relates to old legislation but it isa introduction of relative criteria for the purpose of defining the possible identifiability of a natural person on the basis of a particular data. The General Regulation also contains in recital 26 indications that this method of interpretation should also be applicable to this new regulation. Under the above recital, the data protection principles should apply to all information relating to an identified or identifiable natural person. Personal data that has been pseudonymized and could be attributed to a natural person by the use of additional information should be considered as information about an identifiable natural person. In order to determine whether a natural person is identifiable, all means where there is a reasonable probability that the operator or any other person will use it should be taken into account for example by specific selection, for the direct or indirect identification of the natural person. In order to determine whether it is reasonably probable that the means will be used to identify a natural person, all objective factors such as costs and time for identification with regard to the technology available at the time of processing as well as technological developments should be taken into account.

If the obtention of additional information about the person will be able to the operator on the basis of his or her ability, to identify the person without any inappropriate effort, which in order to obtain the additional information will exert there are the personal data protected by the Regulation.

The regulation changes the definition of personal data to reflect changes in technology and the way that organizations or firms collect and store information.

---

[2] See also Voigt, P. Datenschutz bei Google, MMR 2009, p. 377–382.

[3] Judgment of the Court of Justice of the EU from 19. 10. 2016, Breyer vs. Federal Republic of Germany, C-582/14.

Under the definition of personal data, and thus under the data protected by the Regulation, there are no data anonymized and the data of the deceased.

Data anonymization is the process of modifying personal data, with the result that there is no possibility of connection of the data in question with a particular person. Anonymous data is, on the one hand, information that does not contain data for the possible identification of a particular person, or personal data that can no longer be attributed to a particular person. It can be achieved in two ways: randomisation or generalization. Randomization represents a change in the accuracy of the data in order to remove the connection between the data and the person. If the data becomes inaccurate, it is not possible to connect them further with a particular person. Generalization is a generalization of data. Anonymization is commonly used for statistical purposes.

Pseudonymisation is a common tool to remove the possible connection between an individual and a data. According to the definition of the regulation, it is the processing of personal data in such a way that personal data can no longer be attributed to the particular data subject without the use of additional information unless such additional information are kept separate and are subject to technical and organizational measures to ensure that personal data are not assigned to an identified or identifiable natural person. The use of pseudonymisation of personal data can reduce the risks for the relevant data subjects and help operators and brokers to meet their data protection obligations. The explicit introduction of "pseudonymisation" in this Regulation is not intended to exclude any other data protection measures.[4] Pseudonymisation is mentioned in several places in the Regulation, namely Article 6 Paragraph 4 (e), Article 25 Paragraph 1 of the Regulation under which the operator must take appropriate technical and organizational measures, for example if there is a pseudonymisation, Article 32 Paragraph 1 under the security rules for the processing of personal data.

2.1.2. Territorial validity of the Regulation

The most important change that this regulation brings is about ithe protection of the personal data of Union citizens and residents, which is binding on all companies and operating systems processing EU citizens 'and residents' data, regardless of where they are located and where they have their registered office or place of server. The General Data Protection Regulation extends, upgrades and clarifies the scope of the EU data protection jurisdiction. The term "supply of goods or services" under the various provisions of the Regulation obliges companies outside the EU providing services to consumers in the EU and processing data

[4] Recital 28 of the regulation.

of data subjects of the EU. Article 3[5] of Recital 22[6] of the Regulation clarifies the territorial scope so that the Regulation is applied "whether or not the processing itself takes place within the Union".

It is a change to the concept in the law of personal data protection, which replaces the concept of placement relevance by the concept of people within the EU, ie the personal concept. It can be said that the concept of territoriality has been replaced by the concept of personality when the determining factor is the person whose data is being processed and not the location of the data processor or the data itself. The General Regulation applies to processing about the activity of company in the EU where processing is taking place (eg cloud storage abroad). The general regulation will apply to the activities of a data controller or data processor when goods or services are offered to the data subjects or their persons, behaviour is monitored within the EU [Art. 3 Paragraph 2, recital 23].

2.1.3. New rights of the individual

Right to data portability to another service provider means that the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. The data subjects should be able to exchange a service provider, including the transfer of their personal data directly from one operator to the other operator, as far as technically possible and without loss of data (such as contacts or previous emails) and the need to re-enter them.

The right of data transfer is entirely new and includes the right to receive personal data in a structured, commonly used and machine-readable format, and the right to transmit this data to another operator without hindrance from the operator to which the personal data have been provided. The right includes the right to transfer data directly from one operator to another. This means that data controllers who externally process data or process data together with other controllers must have clear contractual terms for assigning each party's responsibility in responding to data portability requests and implementing specific procedures in that regard. The right consists of a) the right to obtain and reuse personal data

[5] This Regulation applies to the processing of personal data in the context of a operator's or a brokers establishment in the EU, whether or not the processing takes place in the Union or not.

[6] Any processing of personal data in the context of an operator's or an broker's establishment in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place in the Union. An establishment means effective and real performance through fixed arrangements. The legal form of such arrangements, whether it is a branch or a subcompany with legal personality, is not a determining factor in this respect.

for further personal use (eg contact list, etc.), b) the right to transfer personal data from one operator to the other at the request of the data subject. This right creates an indirect obligation for data controllers not to impose any transmission barriers; c) the right to control, which means that the directors responsible for the data portability request have a specific obligation to check and verify the quality of the data prior to the transfer. On the other hand, the data recipient is responsible for ensuring that the portable data provided are relevant and not excessive in relation to the new data processing. The Regulation also stipulated that data portability based on the regulation would be provided without any requested payments unless the exemption applies.

The right of data portability has more practical challenges in the practical way. The right of data portability applies to data provided to subjects on the basis of the wording of Article 20 of the Regulation. This could limit the current development of the cyberspace if the data added by others could also be an important part of the data in question that the legitimate subject could have been interested in. On the other hand, the data added by the subject may also contain third party data. It remains to be asked whether these data should also be transmitted on the basis of the wording of Article 20 of the Regulation. Until now, the issue of the practical application of the right of data transfer is questionable. The costs and technical support needed to realization of this right are not yet known. Under the wording of Article 20 there is only the word 'technically feasible'. The explanation of the working group lies rather in the fact that no obligation is imposed on the data controller, which would only require them not to create obstacles in the transfer. In practice, this could lead to blocking the real use of the right with the indication of the operator that the transfer is not technically feasible. The Union should provide more practical guidance on technical support for real application of law, otherwise it may happen that the right will not be practiced in practice because of technical issues.

Profiling is any form of automated processing of personal data that consists of the use of such data to evaluate certain personal aspects relating to a natural person, in particular the analysis or anticipation of aspects of the individual concerned related to performance at work, property, health, personal preferences, interests, reliability, behaviour, position or movement. The data subject shall have the right not to be covered by a decision which is based exclusively on automated processing, including profiling, and which has legal effects which affect him or her or affect him or her in a similar significant way. The new rules introduced by the Regulation limit the use of profiling without the prior consent of the data subject. Profiling must not discriminate against the person whose data is being processed, and profiling must not be based on data that are defined as.

2.2. Other important changes

Penalties for violating the rules of the regulation are serious and up to twenty million euros. Generally speaking, the sanction model is based on the worldwide market turnover of an enterprise, as is known in antitrust law.

The consent and its terms have been changed in order to simplify and make granting of a consent and its download simply and comprehensibly as possible. The processing of sensitive personal data is prohibited unless the exception applies (for example, a person publishes such data voluntarily (in social media or otherwise or on a separate consent basis).) Separate consent to profiling is also required. The debate on consent is terminated in a regulation stating that consent should not be a condition for concluding a contract if the data are not necessary for the preliminary conclusion of the contract. The Regulation further defines the „consent of the data subject" as any free, specific, informed and clearly manifestation of the will of the data subejct by which with the form a statement or a clear confirmatory act, agrees with the processing of the personal data relating to him or her. Under this consent, we can also include publishing personal data and publishing them on the social network. On the other hand, everyone has the right to withdraw his or her consent to the processing of personal data. There is a particular importance of the Article 9 Paragraph 2 (e) of the General Regulation according to which there is no prohibition on the processing of personal data of so-called specific category (eg political opinion, religion, genetic data, data related to the health, sexuality, etc. if the data subject demonstrably publish them.

One contact mechanism has been set up to make it easier to contact public authorities. The Supervisory Authority is the only authority with which the processors and operators will work. In the case of multinational companies, they deal with the powers based on its establishment as well as the supervisor.

3. Conclusion

The impact of the establishment of the Digital Single Market will be on grow will be on all areas of life, law, technology, medicine, research, education, etc. To reach this goal the European Union has lots of work ahead of it. The first base stone was already laid down and that is the personal data protection reform. Personal data protection reform enables people "to move" in the digital world safely having specified clear rules, rights and a clear mechanism of supervision was set.

The General Data Protection Regulation has brought several important changes to the perception of the personal data protection. The article addresses several changes brought by the regulation in question and begins with the definition of

personal data. The definition itself is significantly changed, and as a result, more data are considered to be a personal data subject to the regime and protection of the regulation as compared to previous regulation. The article addresses absolute or relative understanding of the term of the identifiability of a natural person on the basis of information, while I incline to the relative understanding of that term. Anonymization and pseudonymisation are data protection tools, the first term means that data are not under the directive regime. The second term relates rather to the security and interconnection of other processed data. The article deals with a fundamental change in the area of the perception of obligatory subjects, where the change from the principle of territoriality to the principle of personality has occurred. Last but not least, it deals with the individual aspects of data transfer right and the challenges associated with this right.

References:

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, 119/1.

Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHADecision of the Court of Justice of the EU dated 19. 10. 2016, Breyer vs. Germany, C-582/14.