Introductory Guide to the General Data Protection Regulation (GDPR) (2016/679)

Aslı ALKIŞ[1]

Abstract

GDPR (EU) 2016/679 is the regulation on data protection and privacy for all individuals within the European Union. The main aim of the GDPR is to simplify the regulatory environment for international trade and the single market by giving the control back to data subjects who are citizens or residents and by unifying the Regulations among the Member States. As of May 25, 2018, the GDPR will replace the 1995 Data Protection Directive (Directive 95/46).

This paper examines the legal benefit, general information, the scope including the exemptions and finally the principles of the GDPR. In the result, I shall explain the innovations of the GDPR compared with the Directive 95/46 and evaluate the progression from my point of view.

1. The legal benefit of the GDPR

With the developing technology and rapidly increasing use of computers, processing and protecting personal data has become more important and critical. It is perfectly illegal that personal data storing in data banks and sharing them with other entities have seen much more frequently without the consent of the data subject. This activation cause data profiling which makes the entities find and reach their potential clients easily but in an illegal way.

However, the need for personal data protection arises not only from the right of privacy but also the redressing the balance between protection and free movement in European common market.

2. General Information

The rapid change in the use and role of the data in economic activities has led to a change in the regulatory framework, in other words, the need to update the Directive.

[1] International and European Trade and Investment Law(LL.M.) Student of the University of Szeged

The renewal to be made in this field is deemed necessary in order to maintain a much higher level of confidentiality.

Considering that the Data Protection Directive has been implemented since 1995, it is evaluated that this regulation remained obsolete in the face of radical transformations that took place due to the commercialization of the internet, especially from the middle of the 90s. New technologies that have entered our lives sharply during this transformation have provided lots of benefits. On the other hand, they have brought privacy and/or security risks in terms of data collection, processing, storage and reuse of data.

One of the most basic drawbacks within the European Union has been the facilitation of transferring the personal data to third countries. Therefore, this situation brought the necessity of applying the rules of privacy against foreign countries.

In this context, the need for a replacement of the applicable law and adapting to the new digital world has become increasingly necessary due to the concrete disputes that have arisen.

"There is an important distinction between EU directives and regulations, and that distinction is among the reasons why the European Commission strived to replace the Data Protection Directive by a regulation. Directives are broad, goal-driven pieces of legislation which provide guidelines for Member State implementation but depend on the independent passage of a law in every Member State within a designated period of time. Regulations are narrow, specific pieces of legislation which become immediately enforceable-and binding-in every Member State without implementing a law in each State. When the European Commission first considered reforming data protection, it was not yet clear that a directive would be replaced by a regulation. The Commission committed to addressing the following issues:

(1) Addressing the impact of new technologies;

(2) Enhancing the internal market dimension of data protection;

(3) Addressing globalisation and improving international data transfers;

(4) Providing a stronger institutional arrangement for the effective enforcement of data protection rules;

(5) Improving the coherence of the data protection legal framework."[2]

The exposure draft of the Regulation adopted by the Council on 8 April 2016 was adopted and ratified by the European Parliament on 14 April 2016. These regulations were published in the Official Journal of the European Union in all official languages on 4 May 2016. GDPR entered into force on 24 May 2016. However, the exercise date of the Regulation is 25 May 2018.

According to Beata A. Safari, the regulation, as opposed to the current Directive, would be a huge step towards increasing coordination of national and European policy.[3]

3. The Scope of The GDPR

(1) Material Scope

The GDPR, which consists of approximately 90 pages with the text of the 173-paragraph recital section and the 99-articles, provides a comprehensive data protection framework.[4]

Like the Data Protection Directive, GDPR applies to the processing of personal data:

• Wholly or partly by automated means.

• Other than by automated means, if the data are form part of a filing system or are intended to form part of a filing system. (Article 2 (1).)

A filing system is mentioned as "any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis" in Article 4(6)).

Household Exception

Processing " *by a natural person in the course of a purely personal or household activity;* " does not have to conform to many of the Data Protection Directive (Article 2(2)).

[2] Beata A. Safari, Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection, 47 Seton Hall L. Rev. 809 (2017) p. 820-821
[3] *Id.* p. 824
[4] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

This exception is clarified in Recital 18 as:

"*This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities."*

This means that the use of personal data uploaded to the services by those service providers during personal or household activities remains an example of data processing subject to the rules of the GDPR.

Territorial Scope

GDPR will be directly applicable to all member states. However, it is important that data controllers outside the EU know the conditions under which their processing activities can be managed by strict EU regime. This concerns especially three types of processing.

First, the GDPR applies to *"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."(Article 3 (1)).* It is likely to be expanded to the EEA. This provision indicates that data processors are now specifically included in the GDPR.

Second, the GDPR applies to *"the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*

(a) 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

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union." (Article 3 (2)).

Third, the GDPR applies to *"the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."(Article 3 (3)).*

Where the GDPR applies to a controller or processor not included in the European Union, an EU representative must be appointed (Article 27 (1)) subject to certain exceptions (Article 27 (2)). The EU representative must be established in one of the Member States where the controller or the operator provides goods or services or monitor behaviours (Article 27 (3)).[5]

National Exemptions

Such restrictions have to respect the substance of fundamental rights and freedoms and they should be necessary and proportionate measures in a democratic society to protect:

a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

(Article 23)

Chapter IX allows Member States to provide exemptions, exceptions, conditions or rules relating to the following specific processing activities:

[5] For further information see the Article 27 :
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

- Processing and freedom of expression and information
- Processing and public access to official documents
- Processing of the national identification number
- Processing in the context of employment
- Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
- Obligations of secrecy
- Existing data protection rules of churches and religious associations

4. Basic Concepts

i) Personal data**:** GDPR defines personal data as "any information about a data subject" (Article 4 (1)).

ii) Data subject: A person who is defined or identifiable as being related to personal data.

iii) Data controller: Most obligations under GDPR fall to the data controller which determines the purposes and means of processing personal data (Article 4 (7)). The Controller may act alone or in conjunction with others as is covered by the Data Protection Directive.

iv) Data processor: In contrast to the Data Protection Directive, GDPR also imposes specific and separate tasks and obligations on data processors. A processor is " a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (Article 4 (8)).

v) Identifiability: A natural person is identifiable if he/she "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". (Article 4(1))

vi) Processing of data: This has been extensively described as "any operation or set of operations" on the data, including the following:

- collection,
- recording,

- organisation,
- structuring,
- storage,
- adaptation or alteration,
- retrieval,
- consultation,
- use,
- disclosure by transmission,
- dissemination or otherwise making available,
- alignment or combination,
- restriction ('restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future(Article 4 (3))).
- erasure or destruction.

(Article 4(2))

vii) Third Party: It means "a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data." (Article 4 (10)).

viii) Consent: Consent of the data subject means "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." (Article 4 (11)).

ix) Filing System: It means "any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis." (Article 4(6)).

x) Recipient: It means "a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those

public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing." (Article 4(9)).

5. Principles relating to processing of personal data

GDPR sets out a set of principles that the data controller and the data processors must comply with for processing personal data (Article 5).

These principles are the core of the data controller's obligations and are often the basis for a claim that a data controller does not comply with the legal duties.

Article 5 contains the following data protection principles:

- Lawfulness, fairness and transparency:

  Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject (Article 5(1)(a)). Detailed information in regard to the lawfulness of processing is mentioned in Article 6.

- Purpose limitation:

  Personal data should only be collected for specified, explicit and legitimate purposes. It should not be processed in any way incompatible with these purposes. (Article 5 (1) (b).)

Exceptions:

i) Further processing with the consent of the data subject

Further processing of personal data intended for an incompatible purpose, where the data are collected for the first time, is allowed if the data subject is compatible with this new transaction activity *(Article 6 (4), GDPR).* This may mean that the controller must notify the intention to use the data for the new purpose *(Recital 50)* and not process the data for this new purpose until the data has been approved.

ii) Further processing on the basis of EU or member state law

Personal data may be processed for more mismatched purposes on the basis of an EU or Member State legislation that constitutes a necessary and proportionate measure in a democratic society for the protection of the objectives set out in the GDPR. *(Article 23 (1)) (Article 6 (4))* (see national derogations).

The EU or member state law may harmonize and legally determine the tasks and objectives to be taken into consideration in the future proceedings, if it is necessary for the performance of the undertaking to be carried out in the public interest or in the performance of the official authority granted to the supervisor *(Recital 50).*

In theory, this would allow, for example, member states to adopt legislation authorizing the subsequent use of personal data collected by private organizations for their own commercial purposes (including clarification to public authorities and further processing of authorities). This is an important departure from current legal restrictions and may potentially allow public authorities more access to existing data pools on the basis of legislation that can be adopted after these data repositories have entered into force.

iii) Further processing for the public interest purposes

Further operations for public interest, scientific or historical research purposes or for archiving purposes for statistical purposes will not be considered incompatible with the original purposes. For this reason, further processing of existing data is usually allowed, depending on the particular circumstances.

- Data minimisation:

  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Article 5 (1)(c)).

- Accuracy:

  Personal data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (Article 5 (1)(d)).

- Storage limitation:

  Personal data should not be kept in a form that allows the data to be identified for a longer period than is necessary for the purposes for which it is being processed (Article 5 (1) (e)). Personal data may be stored for a longer period as long as it is processed for the public interest, for scientific or historical research purposes, or for archival purposes for statistical purposes. This is subject to the implementation of

appropriate data security measures designed to protect the rights and freedoms of data subjects.

- Integrity and confidentiality:

  The personal data should be processed in a way that ensures proper security (Article 5 (1)(f)). This includes protection against unauthorised or illegal operations and accidental loss, destruction or damage. In this context, data controllers and processors must use appropriate technical or organisational security measures.

- Accountability:

  It is a new principle introduced by GDPR. The controller must be responsible for and be able to observe the principles mentioned above. (Article 5(2)).

  This is significant as it shifts the burden of proof to the data controller in the event of a compliance investigation by a data protection authority. Organisations should view this principle in light of the record keeping obligation, the requirement to prove that consent is obtained and the concept of privacy by design and default.[6]

The GDPR includes a range of other obligations and requirements that will impact on different organisations to varying degrees, but the overall objective is to recognise that data about individuals belongs to them, and they should be entitled to determine how it is used.[7]

Result and Assessment

As the rapid development of data processing technologies and the internet become an integral part of social life, the importance of the protection of personal data has been increasing. For this reason, unlike the Directive, it was necessary to make a regulation that would have a direct effect on all European Union countries from the moment it entered into force.

[6] https://www.mhc.ie/uploads/MHC_GDPR_web.pdf

[7] https://s3-eu-west-1.amazonaws.com/5874multi/wp-content/uploads/sites/63/2017/11/28150840/ML4200-AIHO-Data-Protection-and-the-GDPR-Key-Priciples-FIN_WEB.pdf

Compared to Directive 95/46/EC, the GDPR has brought more stringent and comprehensive rules that are made in terms of responsibilities, sanctions, individual rights and data protection measures.

The responsibilities of data processing parties have been increased. In contrast to the Directive, the data processor is also responsible for processing under the GDPR. The responsibilities of the data controller have been made even stricter with the principle of "accountability".

Moreover, the GDPR has stronger norms in terms of implementation area. It's been criticised that the "territorial scope" was not included in the Directive. However, it is involved in the GDPR to prevent complications and harmonize practices among the Member States.

Furthermore, basic concepts have been examined and diversified in more detail. For instance, the concept of clear consent has been strengthened. As stated in Recital 32, data subjects' silence to the privacy settings on their online social networks or web browsers or if they have not raised any objections until then, the default setting does not mean that a valid consent has been received.

It is clear that there are areas where Member States are competent, for example in national security and defence matters. It is natural that GDPR does not present all the possibilities for certain data processing activities. However, it should be said that the Regulation is a real revolution and it will affect not only European Union countries but also the third countries with its detailed and strict rules. According to Jan Philipp Albrech, From 24 May 2018 the fragmented digital market of today and the lack of enforcement in the field of data protection provisions will end. There will be a unified and directly applicable data protection law for the European Union which replaces almost all of the existing Member States' provisions and which will have to be applied by businesses, individuals, courts and authorities without transposition into national law.[8]

The GDPR now directs almost all the matters and leaves only exceptional and limited powers to the Member States, but it is difficult to foresee what will happen as a result of new and speedily developing technological developments.

[8] Jan Philipp Albrecht, How the GDPR Will Change the World, 2 Eur. Data Prot. L. Rev. 287 (2016) p. 287