The new legal framework and a guide to the General Data Protection Regulation (GDPR) (2016/679)

Aslı ALKIŞ[1]

Abstract

Because the data protection law should be comprehensive, the General Data Protection Regulation replaces the Directive 95/46/EC. GDPR was adopted in May 2016 and will be implemented directly in all EU member states on May 25, 2018, with no transposition needed. In addition, it is likely that GDPR applies to three members of the European Economic Area (EEA), which are not members of the EU and are included in Article 7 and Annex XI of the EEA Agreement.

Thus, this paper will examine the implementation of the new regulation as:

1) Lawfulness of processing
2) Rights of data subject
3) Obligations of the data controller and data processor
4) Legal framework

Finally, in the result part, I shall evaluate the new regulation based on my research from my point of view.

1. Lawfulness of Processing

The GDPR continues the approach under the previous regime requiring a data controller to justify the processing of personal data in accordance with Article 6.

The consent of the data subject has given for data processing only one or more specific purposes *(Article 6(1)(a))*.

Processing is necessary to perform or enter the data contract with the data subject *(Article 6(1)(b))*.

Processing is necessary to comply with a legal obligation that the data controller is subject to *(Article 6(1)(c))*.

The vital interests of data are to be protected *(Article 6 (1) (d))*. Recital 46 explains that this legal ground is, in principle, to be used only if it cannot be done clearly based on one of the other justifications of the process. It also emphasizes that some types of operations can serve both the vital interest (for instance, processing for the monitoring and controlling of epidemics, or the processing of personal data in humanitarian emergencies, such as natural or man-made disasters) of the data subject and for the public interest.

Processing which is an obligation in the public interest or in the exercise of the official authority of a third party or the data controller to whom the data is disclosed *(Article 6 (1) (e))*.

Data processing is necessary for the purposes of legitimate interests pursued by the data controller or a third party; except that these interests are invalidated by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data *(Article 6 (1) (f))*. The public authorities that process personal data while performing their duties cannot withstand this situation. When determining whether the interests of the database or its fundamental rights and freedoms invalidate the legitimate

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

interest of the data controller, reasonable expectations based on the relationship of the database to the controller should be considered *(Recital 47, GDPR).* The interests and fundamental rights of the data subject may invalidate the interest of the data controller in which personal data is processed, especially where the data subject is not expected to be further processed.

Conditions for which the process may be applied:

The legal grounds referred to in *Article 6 (1) (c) and (e)* shall be established in accordance with the EU or national law *(Article 6 (3), GDPR).*

In particular, these laws should determine the purpose of the transactions they authorize or authorize. To this end, the legislation may contain the following "special provisions" in order to comply with the implementation of the GDPR:

- General conditions governing the data processor's legality by the controller.
- The type of data being processed.
- Relevant data subjects.
- For what purpose and for what purpose the data can be explained.
- Purpose limitation.
- Storage times.
- Transaction processing and processing procedures. This will include measures to ensure legal and fair treatment, including other specific processing situations contained in *Chapter IX* (see National Derogations).

GDPR *Article 6 (2).* The Article gives the Member States the right to protect or adapt more specific provisions concerning the processing in terms of compliance with *Article 6 (1) (c) and (e).* Any such measure shall be taken to ensure that *Chapter IX. (See Article 6 (2))* (see National Derogations).

2. Rights of the Data Subject

3.

Data subjects have certain rights under the GDPR as:

- Information Right (Articles 12-14, and Recitals 58-62)
- Personal Data Access Right (Articles 12 and 15, and Recital 63)
- Personal Data Correction Right *(Article 16)*
- Personal Data Erasure Right (Right to be forgotten) *(Article 17, and Recitals 65 and 66)*
- Data Processing Restriction Right *(Article 18)*
- Data Processing Restriction Right (Article 21, and Recitals 69 and 70)
- Data Portability Right (Article 20, and Recital 68)
- Automated Decision-Making Objection Right *(Article 22, and Recital 71)*
- Breach Notification Right (Article 34, and Recital 86)

Additional data subject rights in the scope of particular circumstances and of consent

We aren't counting rights regarding consent *(if it's the chosen legal basis for a specific type of personal data processing)*, additional 'rights' with regards to those special categories of personal data which are called 'sensitive data' in GDPR Recital 10, rights in the scope of proceedings, lodging complaints, representation, compensation, rights in the scope of the occurrence of personal data breaches *(e.g. notification if serious risks)* and far more.[2]

4. Obligations of The Data Controller relating to The Data Subject's Rights

GDPR applies a variety of obligations on data controllers, including obligations, in particular, to the rights of the data subjects and their ability to exercise those rights. The data controller should assist in the use of data subject to the rights *(Article 12 (2), GDPR).* In addition, they must comply with certain conditions regarding the rights of data subjects in the following situations:

- Communicating with Data Subjects
- Responding to Data Subject Requests
- Data Portability Requests
- Joint Controller Relationships Automated Decision-Making Obligations
- Handling Personal Data Breaches

Another duty of the controller is to make sure that the GDPR's Data Protection by Design and by Default principles are enabled. This again means taking the mentioned proper technical and/or organizational measures but here the GDPR goes a bit further *(Article 25)* by:

- Recommending the use of pseudonymisation,
- Pointing to measures designed to implement the previously mentioned data protection principles,
- Emphasizing measures with regards to the fact that only personal data which are needed for each single processing purpose are indeed processed with additional details.[3]

Appointment of a data processor

Unlike the Data Protection Directive, GDPR imposes an important burden not only to the data controller, but also to the data processor that contributes to the accountability principle, to demonstrate compliance with the data protection regime.

The data controller must enter into a contract or another legally binding action on the processor that must fulfil the following obligations:

- Process personal data only on the documented instructions of the controller, including international data transfers to a third country or an international organization. This may mean that data processors will not be able to use cloud computing technology or services without the data controller's approval.
- Comply with security requirements equivalent to those of auditors under Article 32 of the GDPR.

---

[2] https://www.i-scoop.eu/gdpr/data-subject-rights-gdpr/#Data_subject_rights_list

[3] https://www.i-scoop.eu/gdpr/data-controller-data-controller-duties/#Responsibilities_of_the_controller_under_the_GDPR

- Only recruit staff who are committed to confidentiality or under confidentiality obligations.
- Obtain a subprocessor only on the pre-authorization of the controller.
- Help data controllers to fulfil the obligations of the data subjects to apply the rights mentioned in the Chapter III.
- Help data controller to carry out its security obligations under the Article 32 to 36 of the GDPR.

(Article 28(3))

Appointment of a data protection officer

Data controllers and data processors must designate a data protection officer (DPO) in any of the following situations:

- Where the proceedings are carried out by a public authority or body, except courts serving in judicial capacities.
- Where the controller or the operator's core activities consist of processes that require a large and regular and systematic monitoring of data issues due to their nature, scope, and purpose.
- Where the controller or operator's core activities consist of the processing of large-scale private data categories and the processing of data relating to criminal convictions and crimes (Articles 9 and 10, GDPR).

(Article 37(1))

Article 30 of the GDPR sets out document requirements for both data controllers and data processors.

Documentation Requirements

Article 30 of the GDPR sets out document requirements for both data controllers and data processors.

Exceptions

The documentation requirement does not apply to data controllers and data processors who have fewer than 250 employees unless at least one of the following conditions is fulfilled:

What they do is likely to pose risks in terms of data rights and freedoms.
Processing is not occasional.
Processing includes personal data or data categories relating to criminal convictions and offenses (Articles 9 (1) and 10, GDPR).

(Article 30 (5))

5. Legal Framework

***i)*National Data Protection Authorities**

Member States should establish one or more NDPAs with responsibility for monitoring compliance with the GDPR *(Article 51 (1)) and Article 54)*. NDPA must act with complete independence when it fulfils its duties and powers under the GDPR *(Article 52 (1)).*

In particular, each of the NDPA members should:

- Have the qualifications, experience and skills necessary to perform their duties and use their powers (Article 53 (2)).
- Avoid external influences and do not take anyone's instructions while performing their duties (Article 52 (2)).
- Avoid any action incompatible with its powers (Article 52 (3)).
- During the term of office do not engage in any incompatible profession, whether profitable or not (Article 52 (3)).

Each NDPA has the power to carry out its duties and exercises its authorities in relation to the data processing activities of the data controllers established in its Member State (Article 56 (1)).

If the processing of personal data by an EU data controller or processor occurs in more than one member country, one single NDPA should assume leadership role and have the authority to monitor its activities across the EU (one stop-shop). In this case, the competent authority shall be the NDPA of the member state in which the controller or the processor has its main or the single establishment (Article 56 (1)).

The Regulation also provides for derogation from the application of the one-stop shop, by setting up an urgency procedure for exceptional circumstances when a DPA considers that it is urgent to act so as to protect the interests of data subjects.[4]

It is designed for the following:

- Carry out a consistent implementation of GDPR
- Provide legal certainty
- Reduce the administrative burden for controllers and processors that process personal data in an international context

Powers

As opposed to Directive 95/46/EC, the Regulation now foresees a set of clearly defined tasks and powers equally applicable to all European DPAs. The tasks circumscribe their fundamental duties, such as monitoring and enforcing the application of the Regulation, promoting awareness, dealing with complaints, cooperating with other DPAs etc. The powers represent the means to perform these tasks. The powers of DPAs are now grouped into three main categories, namely investigative powers, corrective powers as well as authorisation and advisory powers. [5]*(Article 58)*

Co-operation

The chapter VIII of the GDPR sets out the scope of cooperation between the NDPAs of the different member states where data processing activities affect more than one member state.

---

[4] Andra Giurgiu; Tine A. Larsen, Roles and Powers of National Data Protection Authorities, 2 Eur. Data Prot. L. Rev. 342 (2016) p. 350

[5] Andra Giurgiu; Tine A. Larsen, Roles and Powers of National Data Protection Authorities, 2 Eur. Data Prot. L. Rev. 342 (2016) p. 348

Joint operations of NDPAs

Article 62 of the GDP provides a framework for cooperation between data protection authorities in different regions in relation to research, implementation and other joint operations. Each NDPA has the right to participate in all processes related to the process which, if appropriate, is likely to affect the data subjects in their area.

***ii)* European Data Protection Board**

It ensures the creation of a new European Data Protection Board (EDPB) consisting of NDPAs 68 to 76 of the GDPR, each of the member states, and the European Data Protection Supervisor. EDPB replaces the Working Group of Article 29.

EDPB must act independently while performing its duties (Article 69 (1)). *Without prejudice to requests by the Commission referred to in Article 70(1) and (2), the Board shall, in the performance of its tasks*[6] *or the exercise of its powers, neither seek nor take instructions from anybody (Article 69(2)).*

EDPB should take its decision with a simple majority (Article 72(1)). The discussion should be confidential (Article 76). Where feasible, it should consult with interested parties and give them the opportunity to comment within a reasonable time. The results of the consultation process should be made publicly available. (Article 70(4)).

***iii)*Remedies, Liability and Penalties**

VIII of the GDPR has set out solutions for the violations of the GDPR and the penalties that the NDPA may be subject to.

Article 77- Data subject's right to lodge a complaint with a NDPA

If each of the data subjects considers that the processing of their personal data violates the GDP, they have the right to file a complaint with an NDPA, in particular in the member states, such as the place of residence, place of work or alleged violation place (Article 77(1)). This right exists without prejudice to any other administrative or judicial resolution.

The NDPA to which the complaint is lodged shall ensure that the data subject is informed of the progress of the complaint and the outcome, including whether or not the judiciary is present (Article 77 (2)).

Article 78- Right to an effective judicial remedy against a NDPA

Article 78 of the GDP opens the way to jurisdiction over data issues:

- Against a legally binding decision by an NDPA concerning them (Article 78 (1)).
- If the NDPA under the authority to designate the leading authority (Articles 55 and 56) does not file a complaint or does not inform the complaint about the progress or the result within three months from the date of the complaint (Article 78 (2)).

[6] For further information about the tasks of the EDPB: https://gdpr-info.eu/art-70-gdpr/

Article 79- Right to an effective judicial remedy against controllers and processors

Article 79 of the GDPR recognizes data entities and auditors' rights to violate their rights under GDPR as a consequence of transactions that do not comply with the requirements of GDPR.

Article 80-Representation of data subjects

Although GDPR ultimately rejects the concept of collective or class action, Article 80 stipulates that data subjects should appoint a non-profit organization, association or association to have a complaint in their favor and use the right of data collection under the title of the Articles. 77, 78, 79 and 82 in their name.

The relevant organization should:

- It was created in accordance with the law of a member state.
- Having legal objectives in the public interest.
- Be active in the area of protecting the rights and freedoms of data concerning the protection of personal data.

Member States may also obtain a more general right under national law for an organization, institution or organization to lodge an appeal against an NDPA by a data subject independently of an authority (Article 80 (2)).

Article 81-Suspension of proceedings

Article 81 of the GDPR provides for the right of a second judge in the courts of another member state to suspend the proceedings if he/she obtains knowledge that the proceedings are continuing, in order to prevent the same issue involving the same controller or operator in different Member States.

In cases where these proceedings are anticipated in the first instance, a court from another court may first refuse the jurisdiction of the court upon the application of one of the parties, if the court first has jurisdiction over the actions and if the law permits such actions to be consolidated. (Article 81 (3)).

Article 82- Right to compensation and liability

A person who has suffered financial or non-material damages as a result of a violation of GDPR has the right to receive compensation from the controller or the processor of the damage.

In this context, auditors are liable for damages caused by the transaction if they are involved in the infringing transaction. Processors are only responsible for:

- Has not complied with any of its obligations under GDPR.
- Have acted in violation of or outside the controller’s legal instructions.
- (Article 82 (2)).

Article 83-General conditions for imposing administrative fines

Article 83 (1) of the GDPR empowers the supervisory authorities to impose administrative fines for the breach of the GDPR. Infringements of the obligations of the

controller and the processor; the obligations of the certification body; the obligations of the monitoring body carry an administrative fine which can be as much as 10 Million Euros or 2% of the worldwide annual turnover of the preceding financial year. Infringements of the basic principles for processing including consent; the data subject's rights which include the right to data portability, the right to be forgotten etc.; the transfer of personal data to a recipient third country or international organization; obligations pursuant to member state law; non-compliance with any order by the supervisory authority for restriction of processing or suspension of data flows attracts an administrative fine of up to 20 Million Euros or 4% of the worldwide annual turnover of the preceding financial year. Also non-compliance with the orders of the supervisory authority under Article 58 (2) of the GDPR attracts an administrative fine which can be as much as 20 Million Euros or 4% of the worldwide annual turnover of the preceding financial year.[7]

Member states are also allowed to introduce sanctions for infringements not covered under the GDPR and such penalties are to be notified to the Commission by the 25th May, 2018.[8] *(Article 84)*

Result and Assessment

The amount of data circulation on the Internet continues to increase day by day. In this direction, cyber attacks and threats will continue to increase. Hence, the GDPR, in comparison with the Directive 95/46/EC, has introduced more stringent and comprehensive regulations in terms of responsibilities, sanctions, human rights and data protection measures.

Innovative approaches such as data portability and impact assessment and data protection by design and by default, strengthening deterrence by increasing the sanctions for administrative fines, the remarkable rights of the data subjects such as right to rectification, right to be forgotten, right to restriction of processing, notification obligation are considered to be beneficial not only to the EU member countries but also as a role model to the whole world.

Furthermore, if the Digital Single Market Strategy is effectively alive with all the legal regulations, the EU economy is expected to add an annual value of 415 billion Euros and provide hundreds of thousands of new jobs.[9] Therefore, the GDPR is looked forward to being successfully implemented as it is one of the pillars in the Digital Single Market Strategy.

[7] Salami Emmanuel Akintunde, An Analysis Of The General Data Protection Regulatıon (EU) 2016/679. (2017) p. 32
[8] Id. p 32
[9] https://ec.europa.eu/commission/priorities/digital-single-market_en