Regulation 2016/679 (Practical aspects of implementation in a comparative approach with previous data protection provisions in Europe)

Dea Nini

San Francisco Bay Area technologist Gary Kovacs stated that privacy is not optional and should never be the price we pay for getting the services. The European legal framework has historically paid attention to personal data. The Directive 95/46/EC "On the protection of personal data" defines as such any information that could be used to identify a person and stated the obligation of every controller to obtain consent before collecting, processing, and/or using any personal data[1]. With the innovations brought by globalization, technology, and digital evolution, many controllers moved their servers "offshore", which coincides with a smaller control space for legal entities regarding the treatment of personal data at their disposal.

After a transition period of almost 2 years, May 25, 2018, brought *in vigorem* in the European community the Regulation 2016/679, which represents one of the most significant changes within the European legal corpus of personal data protection over the last 20 years. The GDPR[2] works as a unique regulatory framework for all member states of the European Union[3], despite all previous national legal predictions that took place before it entered into force, paying more attention to individual guarantees for personal data subjects and adjusting in more detail the framework of obligations for the controllers.

One of the innovations brought by Regulation 2016/679 in comparison to the precursor legal corpus of personal data protection is specifically related to its

[1] *Handbook on European data protection law*; FRA; 2018.
[2] *The General Data Protection Regulation- Regulation* (EU) *2016/679.*
[3] *The GDPR: new opportunities, new obligations*; Publications Office of the European Union, 2018.

territorial scope of applicability on any entity that processes personal data within the European Union, regardless of where the actual data processing takes place as well as on entities established outside of the EU offering goods or services to, or monitoring the behavior of individuals within the EU[4]. The extension of the territorial scope of the GDPR is specifically related to its extraterritorial applicability even on non-European processors or those established outside the territorial confines of the European Union, giving special attention to what is processed and not where the processing takes place or who performs it.

Following our modest research endeavor, we will try to address the concept of the controllers and their responsibilities, but also the important principles of accountability, reliability, documentation of processing activities, cooperation, data security, and legal sanctions in the field of personal data protection, through a comparative approach amidst the previous provisions of the European legal corpus and those brought by the GDPR to clarify the impact of each change.

Regarding the concept of controlling party and its definition, through an extended comparative interpretation between Article 2/d of the Directive 95/46/EC and Article 4/7 of the Regulation, it appears that there is no essential change in what the controlling party represents within the European legal corpus. In this line, any entity that was a controller under the Directive likely continues to be a controller also under the GDPR.

Concerning the important principles of responsibility and accountability, it appears that the GDPR in comparison with the provisions set out in Article 6/2 of the Directive strengthens the obligation of the controlling party, as it sets as a prerequisite the obligation to demonstrate that the processing activities will be on par with the Principles of Data Protection, moving the focus precisely on the need for factual demonstration[5].

With regards to the responsibility of the controller at first sight the principle basis remains unchanged, as each controlling entity will be directly responsible and will have the burden of proof to prove that the processing activities are lawful. Despite following the same principle, the GDPR provides additional details on how entities, through the application of direct technical and/or organizational measures, can demonstrate that their processing activities are lawful[6].

The concept of personal data security as a precondition for their lawful processing is one of the aspects that in a comparative view with the predictions of the predecessor legal corpus in the field has changed. The difference consists of the fact that compliance with the GDPR should be treated as a crucial aspect from the planning to the implementation and/or production stage of any new product

[4] Ibid.
[5] GDPR; **Rec.85; Art.5(2).**
[6] GDPR; **Rec.74; Art.24.**

or service that includes the procession of personal data[7]. Although the preceding Directive required controllers to ensure compliance with its requirements, this obligation did not provide any specific measures in the planning, production, or implementation stages of the product or service. The GDPR obliges controllers to ensure that compliance with data protection principles is an integrated aspect of every stage of the control activity, which in any case must follow the principle of collecting the minimum amount of personal data necessary for the specific case.

Joint controllers represent another concept underlined within the GDPR, while the previous Directive did not use it as a term although it recognized the case where two or more controllers could jointly define the purposes and means of personal data processing. On the other hand, GDPR in Rec.79; Art.4 (7), 26 of it deals specifically with the cases of joint controllers and obligations arising in this situation. In some circumstances, the entities involved in the control and processing activities may not realize that a joint controllership has come into existence, but the GDPR obliges controllers to keep watch for potential instances of joint controllership, emphasizing the importance to treat them differently through specific "agreements" which reflect and separate the responsibilities between two or more co-controlling entities.

The previous Directive in its Rec.55; Art.23 (2) provided for the full or partial exemption from the responsibility of the joint perpetrator in case it could prove that it was not directly responsible for the event or act that caused the violation. The GDPR, on the other hand, treats the joint controller as individually responsible to the same extent, at least in the first stage of handling the case[8]. Only after the full *restitutio in integrum* of the subject of personal data the joint controllers may recover damages from one another, which means that some of them may face much higher liability due to the claims made under the GDPR despite the potential existence of force majeure.

Another innovation of the GDPR is related to the obligation of entities performing control activities outside the territory of the European Union to appoint a representative in the EU[9], as a contact point for data subjects. Contrary to the provisions of the preceding Directive, under the GDPR, a representative may be liable for the controller's failure to comply with the GDPR.

Regarding the appointment of external processors by the original data collection and control entities, the GDPR provides for increased requirements[10] in comparison to previous provisions. These requirements should necessarily be addressed by all data processing agreements and contracts with third parties, making outsourcing agreements more complex to enter into and implement.

[7] GDPR; **Rec.78; Art.25.**
[8] GDPR; **Rec.79; Art.4(7), 26.**
[9] GDPR; **Rec.80; Art.4(17), 27.**
[10] GDPR; **Rec.81; Art.28(1)-(3).**

Another important aspect introduced is the record of processing activities in registers accessible by stakeholders and personal data protection entities, an obligation that has not materially changed under the GDPR, although at first glance it seems that controllers are more favored than before as this information is made available only upon request and the legal entities with less than 250 employees are exempted (unless the processing they perform is of special importance).

The security of personal represents a crucial aspect within the legal corpus of personal data protection, where the right of the data subject to security corresponds to the obligation of the controller to pay special attention to this security during every stage of the processing activity[11]. The previous Directive in comparison to the GDPR was less detailed[12] on how to achieve the necessary level of security, however, we do not single out substantial changes or innovations in this regard.

Immediate reporting of data breaches is one of the most important obligations of controllers set out by data protection legislation. The preceding Directive did not specifically require controllers to report breaches to data protection agencies, although such efforts were noted in the national legislation of some Member States. The GDPR is quite strict in this frame where in case of violation it imposes the obligation of the controller to immediately **report the breach without undue delay, and in any event within 72 hours** of becoming aware of it[13], except for the cases where the data breach has no potential to harm data subjects.

The obligation for immediate and rigorous reporting by controllers, as an innovation of GDPR, stands not only concerning data protection agencies but also to direct data subjects. This obligation coincides with an increased burden for the controlling entities, which can often irreversibly affect their reputation.

In addition to the aforementioned changes and innovations brought by the GDPR, its financial impact is currently the most discussed aspect, which is why we decided to bring it to the attention of our research, focusing on the structure of administrative fines imposed by the GDPR, in response to potential breaches. Through a literal interpretation of Article 83 under the GDPR, it is clear that potential infringements can incur penalties, and are classified within two categories based on their severity.

Less severe infringements under the GDPR are considered those related to:

- Obligations controllers and processors[14], which must act quite rigorously in following the main principles that make controlling and processing activities legal and fair, focusing on the direct interest of the personal data subject.

[11] GDPR; **Rec.83; Art.32.**
[12] Directive 95/46/EC; **Rec.46; Art.17(1).**
[13] GDPR; **Rec.73, 85-88; Art.33.**
[14] GDPR; Art. 8, 11, 25-39, 42, 43.

- Obligations of certification bodies[15], which must carry out their assessments without prejudice and through a transparent process.
- Obligations of the monitoring bodies[16], which must demonstrate their independence and strictly follow the procedure for handling complaints, addressing them with impartiality and transparency.

The less severe infringements could result in a fine of up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.

Regarding the more severe infringements, they are related to the cases where the violation is related to:

- Basic principles of processing17, which consist of the collection and processing of personal data only for a specific purpose, taking care of their accuracy and up-to-dateness in accordance with a high level of their security. In relation to sensitive personal data, which includes information on racial origin, political views, religious beliefs, trade union membership, sexual orientation, medical records, or biometric data, the GDPR allows their collection and processing only in very specific circumstances, as the general principle is that this category of data should not be collected nor processed.
- The conditions for consent18, which consists of the fact that the processing of data must be based on the consent of the person, regarding which there must be factual evidence.
- The rights of data subjects19, regarding being aware of the data that are being processed, their correction, deletion under "the right to be forgotten" principle, or transfer of the right for their processing to another subject.
- Transfer of data to an international organization or a subject in a third country20, where before an entity transfers any personal data to a third country or international processor, the European Commission must have expressed its suitability in the context of adequate protection.

All violations related to the above-mentioned cases can result in fines of up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.

[15] GDPR; Art. 42, 43.
[16] GDPR; Art. 41.
[17] GDPR; Art. 5, 6, 9.
[18] GDPR; Art. 7.
[19] GDPR; Art. 12-22.
[20] GDPR; Art. 44-49.

According to the GDPR, penalties are administered by National Personal Data Protection Entities in each EU member states, which will assess whether there is a breach and impose the respective fine in this case. The assessment of breaches under the GDPR should be based on the cumulative assessment of 10 criteria, which include:

i. The severity and nature of the violation in a general view, the damage it caused, and the time of its recovery;
ii. The fact that the violation represents an act committed intentionally or by negligence;
iii. The fact if the subject of the violation took any action to mitigate the damage suffered;
iv. Existing precautionary measures, regarding the level of technical and organizational preparation that the entity had undertaken to comply with the GDPR;
v. History of breaches, including those related to Directive 95/46/EC as well as corrective actions are taken;
vi. Cooperation with the supervising entity to detect and correct the violation;
vii. Categories of data affected by the violation;
viii. Correct notification of the violation to the supervisory authority;
ix. Existence of subject certification relating to approved codes of conduct;
x. The existence of aggravating or mitigating factors, including financial benefits or losses avoided as a result of the breach.

The GDPR indicates that if from the cumulative assessment of the above criteria it is shown that an entity is liable for more than one violation, it will be penalized only for the most severe one, provided all the infringements are part of the same processing operation.

At the end of our analysis regarding the main changes brought by the GDPR within the European context, in the framework of its extraterritorial applicability, and its potential financial impact we find it appropriate to come up with a recommendation for all controlling entities, to comply with the provisions and obligations arising from the implementation of the GDPR.

It would be worthwhile to appoint a specific person responsible within each controlling entity for investigating, reviewing, reporting, and documenting potential cases of violations, in line with the obligation to addressing violations within 72 hours, which is one of the most stringent obligations set forth by Regulation 2016/679. Given the importance of this Regulation and the sanctions and fines it imposes on perpetrators, it is of great importance to building sustainable human resources, amid clear policies of identifying and reporting violations through different trainings and rigorous reporting protocols.