Igor Salgues

Attorney at Law

The Guiding Principles of the General Data Protection Rules.

The importance of proactively documenting compliance.

Table of Contents

1. Background

The new European regulation on the processing of personal data, the General Data Protection Rules (GDPR), has entered into force on 25 May 2018,[1] repealing the Data Protection Directive (DPD),[2] which was previously incumbent for the matter. The advent of such norm to the European data framework represents a paradigm shift remarked by the intensification of measures intended to protect personal data as a fundamental right.[3'4'5]

The new regulation is intrinsically distinct from its former counterpart[6] and must be carefully assessed by companies handling personal data. That because, the norm has set specific requirements and principles, which noncompliance may impose harsh administrative fines up to '20 000 000 EUR' or '4% of the total worldwide annual turnover of the preceding financial year (whichever is higher).'[7]

The GDPR not just recognizes the real value of personal data and the risks cyber theft represents to individuals, but also the

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (GDPR).

[2] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995.

[3] First granted to 'everyone' by the Article 8 of the Charter of Fundamental Rights of the European Union, and the Article 16 of the Treaty on the Functioning of the European Union.

[4] See, CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION (2000/C 364/01).

[5] Also, CONSOLIDATED VERSION OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION.

[6] In contrast to the DPD, the GDPR has a status of regulation. Therefore, the GDPR is a law on itself, overriding incompatible national laws passed by Member States. As such, the GDPR is intended to unify the EU framework on personal data protection.

[7] GDPR, Article 83.

magnitude in which 'Big Data' analysis allows the tracking and prediction of individual behavior, what can be deployed in automated decision-making. These circumstances alongside the continuous development of technologies, and misuse of personal data, by governments and corporations, has induced the new regulation. As such, the GDPR is intended to clarify the data rights of EU citizens, as well to elevate the standards of the EU protection of personal data.[8]

Under this context, it is essential to analyze the principles, and legal aspects laid by the GDPR in order to assess the risk it may represent to a given entity in the private sector.

2. Territorial Scope

Beforehand, it is important to remark, the territorial scope of the GDPR have a transboundary characteristic,[9] meaning it applies for controllers and processors located in Europe, even in cases in which processing takes place outside the European Union. In this case, any European enterprise handling personal data abroad must also be aware of the guidelines and principles imposed by the GDPR. Further, such norm also applies for foreign controllers and processors not established in the EU, when offering services or goods to data subjected to the EU, or when monitoring behavior that takes place within the EU.

[8] IT Governance Privacy Team. (2016). *EU General Data Protection Regulation (GDPR) : An implementation and compliance guide*. Cambridgeshire, UK: IT Governance Publishing.

[9] GDPR, Article 3.

The territorial scope of the GDPR has a broad definition. Consequently, it is likely to disrupt the current data framework and policies adopted by any company handling personal data. This because, private entities, including those not located in the EU, offering its services or goods, would need to either ensure compliance with the GDPR or that its services are not provided whatsoever within, or somehow in association with data subjected to, the EU. As such, the GDPR is clear in imposing obligations and responsibilities to any company that may, even without intention, process data somehow connected to the EU. This transboundary characteristic leaves open questions such as regarding to (1) whether intent may be a determining factor for noncompliance with the norm, or (2) whether noncompliance can be determined in cases in which measures have been taken to ensure the service or goods are provided within national limits outside the EU (or any foreign jurisdiction where the EU jurisdiction apply), exclusively to data that appears not to be connected to the EU, when in reality it is - what could be the case when consumers opt for using data encryption or a Virtual Private Network (VPN), to gain access to a service not offered in the given region where he or she is located.

Either way, the stakes are high and possibly not worth the risk. Therefore, the private sector is prone to be placed in a position to proactively adapt its data frameworks in order to ensure compliance with the GDPR, even in regions where the EU jurisdiction do not apply.

That said, it is now possible to advance into the further analysis of the guiding principles of the GDPR.

3. Guiding Principles of the GDPR

The guiding principles of the GDPR are described by the Article 5 of the regulation. In this sense, the Article 5 establishes that personal data shall be treated in accordance to the following principles:

- **Lawfulness, fairness, and transparency** - This principle is represented by legal criteria that may be considered both objective or subjective. In this case, Lawfulness and transparency may be described as objective criteria once it can be defined by the law. Arguably, though, the concept of fairness may seem somewhat ambiguous, leaving room for subjective interpretation. Further, the concept of lawfulness is further refined by the Article 6 of the GDPR; without prejudice to the norm, the concept of transparency is delineated by the paragraph 39 of the Recitals in the legislative act which has adopted the GDPR.[10] Anyhow, these three components of the principle are interconnected. In this sense, the data subject must be made aware that: his or her information will be processed (transparent); the processing matches the description (fair); and, the processing takes place within the boundaries of the regulation (lawful).[11]

- **Purpose limitation** - Establishes that data shall be collected only with specific, explicit, and legitimate purpose,

[10] OJ L 119, 4.5.2016, p. 1–88.
[11] See IT Governance Privacy Team, n. 7 above,

precluding further processing nonrelated and incompatible to the initial purpose.[12] In this case, the controller must define upfront the reason why the data is being collected and for what it will be used, limiting the processing to such purpose. [13]

- **Data minimisation** - Announces that personal data must be adequate, relevant and limited to what is only necessary for its intended purpose. In this sense, the collection of data should be more than what is strictly necessary.

- **Accuracy** - This principle establishes that personal data must be accurate and up to date. It also imposes the necessity of taking all reasonable steps to ensure that inaccurate data is erased or rectified without delay. Such provisions also seem somewhat ambiguous, leaving room for subjective interpretation.

- **Storage Limitation** - This principle represents a temporal criterion restricting the identification of data subjects only for the necessary period related to its purpose.

- **Integrity and confidentiality** - Delineates the burden of securing personal data against both unauthorized or unlawful processing and accidental loss, destruction or damage.

- **Accountability (burden of proof)** - Described by the paragraph 2 of the Article 5, as imposing a reverse onus of

[12] With the exception of further processing in favor of public interest, scientific or historical research or statistical purposes, accordingly to the Article 89 (1).

[13] See IT Governance Privacy Team, n. 7 above, page 101.

proof to the controller. In this case, the controller must be able to prove compliance with the guiding principles.

4. The Lawfulness of Processing

The Article 6 of the GDPR has determined the circumstances in which processing is to be considered lawful. The mentioned provision makes use of restrictive language; Therefore, as a general rule, processing is only to be considered lawful if it falls into at least one of the categories described by the Article 6, paragraph 1. As such, the processing will be lawful if it configures at least one of the following circumstances:

A. In the cases in which the data subject has consented the processing of his or her personal data, for one or more specific purposes;[14]

B. When processing is made imperative to the performance of a contract in which the data subject is a party, or in order to take steps at the request of the data subject before entering into contract;[15]

C. When processing is necessary for compliance with the legal obligation to which the controller is subjected;[16]

D. When processing is necessary for protecting vital interests of the data subject or another natural person;[17]

[14] GDPR, 6 (1) a.
[15] Ibid., 6 (1) b.
[16] Ibid., 6 (1) c.
[17] Ibid., 6 (1) d.

E. When processing is necessary for the performance of a task carried in the public interest or in exercise of official authority vested in the controller;[18]

F. When processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party; with the exception of cases in which the interests and fundamental rights of the data subject - requiring protection of personal data, especially being the data subject a child - represents a higher priority.[19] However, this entire provision does not apply to public authorities in the performance of their tasks.[20]

In this sense, the paragraph 2 has allowed Member States to create specific provisions with precise requirements and other measures to ensure lawful and fair processing on what relates to the the topics 'C' and 'E', and also other specific processing situations as described by the chapter IX of the GDPR.[21] Further, the paragraph 3 has determined that the basis of processing referred by the topics 'C' and 'E' will be laid down either by Union law or Member State law to which the controller is subjected.

Nevertheless, the paragraph 4 of the Article 6 has announced the factors which must be taken into consideration by the controller in cases where the purpose of processing is not based on the data subject consent or on a Union or Member State law. In such cases the controller must assess:

[18] Ibid., 6 (1) e.
[19] Ibid., 6 (1) f.
[20] Ibid., 6 (1), last paragraph.
[21] The GDPR foresees specific processing situations in the Chapter IX, such as, for example, it is the case of circumstances involving the purposes of journalism, academia, arts or literature.

A. The link between the initial data collection purpose and the purposes related to further processing;[22]

B. The context in which the data was collected, especially on what touches the relationship between data subjects and controller;[23]

C. The nature of the personal data;[24]

D. The potential consequences of further processing for data subjects;[25]

E. The existence of safeguards such as encryption or pseudonymisation.[26]

As a conclusion, the provisions on the article 6 demonstrates the intention of the GDPR in specifying what in fact consists lawful personal data processing. In this case, the regulation has not just established the different circumstances in which data processing is to be considered legal, but also the focus of legality being associated to the consent offered by the data subject to the controller, what will be further analysed in the next section.

[22] GDPR 6 (4) a.
[23] Ibid., 6 (4) b.
[24] Ibid., 6 (4) c.
[25] Ibid., 6 (4) d.
[26] Ibid., 6 (4) e.

5. Consent

The conditions for consent are delineated by the Article 7 of the GDPR. This provision has established the following four conditions which the controller must be aware of:

- First, the controller has the responsibility to demonstrate the data subject has consented to the processing of his or her personal data.

- Second, If the consent was given as written declaration also related to other matters, the request for such consent must be clearly presented and distinguishable from the other matters in an 'intelligible and easily accessible form,' with clear and plain language.

- Third, the data subject must be allowed to withdraw his or her consent at any time, without prejudice to the lawfulness of the processing based on the consent before its withdraw. The data subject must be informed about this condition, and withdraw should be as easy as to give consent.

- Fourth, the assessment of whether consent is freely given, must take into account whether the performance of the contract and provision of the service is conditional on consent to the processing of unnecessary personal data for such contract.

The conditions for consent are further refined by the recital 32, which describes that:

> "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."

In addition, the Article 8 in the GDPR has determined an extra protection of children's data in relation to information societies.[27] In this sense, consent is lawful when given by children of at least 16 years of age; Processing of the personal information of children under the age of consent will only be lawful if consent is given or authorized by the holder of parental responsibility.[28]

[27] Information societies may be defined as: "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service". See recital 17 of the Directive 2000/31/EC, and Article 1(2) of Directive 98/34/EC, amended by Directive 98/48/EC.

[28] See also Recital 38 of the GDPR.

6. The Reverse Burden of Proof

The reverse burden of proof is stimulated by the principle of Accountability, in the Article 5 (2), consisting of the obligation imposed to the controller in being capable of proving his behavior in compliance with the norm, what may be somewhat challenging in certain circumstances.

In ordinary cases, the rule of law establishes that one who accuses the other of wrongdoing must also prove his claim. In the GDPR, however, the situation is the opposite, and the 'accused' would need to prove its 'innocence'. In this case, companies handling personal data must preemptively demonstrate to be compliant with the norm. Either way, any claims made against such company are likely to prevail.

Such reverse onus of proof demonstrates the intention of the GDPR in promoting a proactive data protection culture among controllers. However, in doing so, the GDPR also creates an environment prone to establish liability for entities involved with the processing of personal data. As a consequence, it is of prominent importance for the interested parties to take the necessary proactive measures to document its compliance with the GDPR.

Companies handling personal data must be aware of such proactive requirements,[29] being able to demonstrate and document to have embedded the GDPR principles of data

[29] See also GDPR, Article 24.

protection in their organizational culture.[30] Therefore, it is essential to structure and maintain a compliance framework within the company in order to meet the requirements of the GDPR.

Important to remember, the GDPR has a transboundary character. For this reason, companies with branches in different countries must be aware of the necessity of implementing such compliance framework even for subsidiaries outside Europe.

7. Conclusion

The GDPR have set high expectations for the private sector, once it has established high fines in case of noncompliance with the norm. In this case, the GDPR has adopted the concept of reverse burden of proof, and it is up to the controller to prove to be compliant with the norm. That meaning, it is not enough to do everything by the rule, but it is also required to be able to prove and document compliance. Consequently, companies handling personal data are expected to implement an internal compliance framework that must seek to establish a proactive culture of protection of personal data, even for subsidiaries outside Europe.

[30] IT Governance Privacy Team, n. 7 above, page 16.

About the Author

LLM candidate at the Scandinavian Institute of Maritime Law at the University of Oslo. First professional law degree issued by Laureate International Universities. European lawyer, and registered attorney in both Brazil and Portugal, with more than ten years of legal experience in litigation and extrajudicial settlement.

Contact the Author

+47 46 86 28 49

igor@salgues.one

http://salgues.one