SOULIER BUNCH

Published on 30 May 2016

Laure Marolleau, Cabinet d'avocats d'affaires basé à Paris et Lyon

Read this post online

New regulation on data protection (Part I)

The very much expected Regulation n°2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (also known as "General Data Protection Regulation" or "GDPR") has just been published on the Official Journal of the European Union (OJ, L 119, May 4, 2016).

Based on a proposal from the European Commission of January 25, 2012, this Regulation jointly adopted by the European Parliament and the Council repeals Directive 95/46/EC and provides for a general and unique framework for the data protection in Europe.

In this article (Part I; Part II to be published next month), we propose to identify the most important innovations in this Regulation.

Background

The General Regulation on Data Protection (hereafter the "Regulation") is part of a complete reform of the European rules on data protection.

This reform also includes a Directive n°2016/680 of the European Parliament and the Council dated 27 April 2016 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. The Directive will apply to the data transfers across the European Union (hereafter the « EU ») and will determine, for the first time, minimal standards for the data process for investigation/prosecution and judicial purposes in each Member State. The Member States have until May 6, 2018, to implement the Directive with laws, regulations and administrative

rules.

The Regulation which has entered into force on May 25, 2016 will apply in each Member State two years after this date, so from May 25, 2018 (Article 99).

It has to be noted that whereas a directive "*shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods*", a regulation "*shall have general application*" and "*shall be binding in its entirety and directly applicable in all Member States*".[1]

With the application of the Regulation, from May 25, 2018, the Member States of the EU will have a uniform and updated legislation on data protection.

The above-mentioned 1995 Directive 95/46/CE (hereafter the « Directive »), that it repeals, was the main regulation on personal data protection in Europe. Its goals and the national measures that implemented them will remain applicable until the day the Regulation will apply.

The need to adapt the actual legal framework to our digital environment and the new competence of the EU in data protection[2] are the reasons why this new Regulation has been proposed and adopted after 4 years of discussions.

Territorial scope (Article 3)

The current rules to determine the national law applicable to the data process are established by the Directive 95/46 and allow for a cumulative and simultaneous application of different national laws to a same data controller established in several Member States (Article 4, 1, a), and this can mean complexity and costs for this data controller. According to the European Commission, the unique Regulation could lead to savings for businesses of around €2.3 billion a year.

Considering that the notion of "*establishment*", which is not defined in the Directive, has generally been interpreted broadly by DPAs (In practice even an attorney office, a one-man office or a simple agent in a Member State are often considered as an "establishment"), they indeed can lead to the application of the national laws of each Member State for each establishment concerned.[3]

Even more subtle, they allow for the application by a Member State of its legislation to the processing of personal data where even though the controller is not established on European Union territory he, "*for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through th(is) territory*" (Article 4, 1, c)

Here again, the notion of "*means, automated or otherwise, situated in the territory*", which is not defined in the Directive, is much discussed and leads to a very broad and different interpretation amongst the Member

States. It includes human and/or technical intermediaries, even outsourcing activities, notably by processors.[4]

The application of the Regulation should tackle these legal uncertainty and extra cost issues since it is directly and immediately applicable in all Member States. The same rules will apply, without further national implementation measures being needed. In case of multiple establishments, the place of the main establishment will be considered.

If the data controller's and also the processor's establishment criterion will continue to apply, the Regulation keeps the basic idea that the European rules on data protection should apply to a data controller or a processor even if he is not established in Europe. Except that, instead of the location of the "means" used to process the data, the Regulation will look for the context within which the data are collected: if the controller or the processor, without being established in the Union, has "*processing activities that 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 behavior as far as their behavior takes place within the Union*", the Regulation will apply as well (Article 3).

How the national authorities of the Member States will monitor and enforce this provision remains to be seen, but we can be sure that it will probably result in all the economic players operating on the European market being bound by the new European data protection rules.

As proof, one needs only to read the Regulation's preamble:

- On the offering of goods and services, "*Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.*" (paragraph n°23);
- On the monitoring of behavior, *"In order to determine whether a processing activity can be considered to monitor the behavior of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes" (paragraph n°24).*

Consent

For sure, the current European and national rules on data protection are not always sufficient to make sure that the data subject's consent is freely given and an information indication of his will.[5]

The « consent » is currently defined by Directive 95/46 as "*any freely given specific and informed indication of*

his wishes" by which the data subject "*unambiguously*" agrees to personal data relating to him being processed (Combination of Article 2-h and 7-a).

Member States have implemented this concept quite differently in their national laws. For instance, and since no form is required, consent has to be given expressly in some Member States, in some cases even in writing, while other Member States accept some forms of implied consent.[6] For instance, in France, the French Data Protection Act does not provide for a definition of "*consent*" and simply lists the situations where it must be explicit (Articles 8, 33 and 56). It is only for commercial marketing, in particular by means of e-mails and SMS messages, that French law provides a definition of consent (in compliance with Article 2, f of the Directive 2002/58/CE dated July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector which has the same meaning as the one defined in Directive 95/46), and which must be explicit according to the French *Conseil d'Etat* (French Supreme Administrative Court)[7].

The Regulation is rather clear on this issue: the consent will be "*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°)

As a result, the consent will necessarily be made "*by a statement or by a clear affirmative action*".

Once again, the preamble provides for clear indications on what is and what is not a "statement" or "clear affirmative action": "*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*" (paragraph n°32)

The burden of proof of the consent relies on the data controller (Article 7, 1°).

The only thing is that the Regulation doesn't substantially change the scope of application of this principle. If the data process remains based on the consent (Article 6, a), the cases where processes are valid without the consent of the data subjects remain the same (Article 6, b to f).

Finally, it will be possible that "*The data subject shall have the right to withdraw his or her consent at any time*" and "*It shall be as easy to withdraw as to give consent*" (Article 7, 3°).

[1] Article 288 TFEU, ex article 249 TEC.

[2] Article 16 TFEU, ex-article 286 TEC.

[3] See Opinion 8/2010 on applicable law of the Article 29 Working Party: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp17

9_en.pdf. This working group is based on Article 29 of Directive 95/46/CE.

[4] Idem., p. 20 and sq.

[5] See Opinion 15/2011 on the definition of consent of the Article 29 data protection working group (in English : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf).

[6] European commission Impact assessment on the Regulation dated January 25, 2012, SEC (2012) 72 final, p. 15 (in English only : http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf)

[7] Article L. 34-5 of the French Post and Electronic Communications Code, and Judicial decision by *Conseil d'Etat*, dated March 11, 2015, *Société TUTO4PC*, n°368624.