SOULIER BUNCH

Published on 28 June 2016

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

Read this post online

New regulation on data protection (Part II)

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 II; Part I published last month), we propose to identify the most important innovations in this Regulation.

Controller and processor (Chapter IV)

The definitions of controller, i.e. "*a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*" and processor, i.e. "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*" remain unchanged (Articles 4 (7) and 4(8)).

The stated determination to strengthen the obligations imposed on processors – who play a major role in the processing of data – is clearly reflected in the provisions of the GDPR.

Indeed, currently applicable rules only provide that "*the carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that: – the processor shall act only on instructions from the controller, and – the obligations set out in paragraph 1[1], as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor*" (Article 17 (3) of Directive 95/46)

The GDPR adopts the same principle but imposes a detailed content for this contract or legal binding act between the controller and its processor (Article 28) and aligns the rights and obligations of the processor and the controller, in particular with respect to the need to maintain a record of processing activities (Article 30), the security of the processing (Article 32), the designation of the data protection officer (Article 37), the application of codes of conduct (Articles 40 and 41), the certification (Article 42), the transfer of personal data (Chapter V), the data subject's right to an effective judicial remedy and to compensation (Articles 79 and 82) and administrative fines (Article 83).

Notification of personal data breaches (Articles 33 and 34)

There exists today with the European Union an obligation to notify national supervisory authorities (and, in certain conditions, the data subjects) of any personal data breaches, i.e. breaches of security that may lead to the unauthorized disclosure or loss of such data (Article 4 (12)). Statistics show that these breaches are becoming more common and result in increasingly harmful consequences, ranging from undesired spam to identity theft[2].

The obligation to notify data breaches, as provided for under Directive 2009/136/EC of November 25, 2009 amending, in particular, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, exists only in the telecommunications sector[3].

Once the GDPR will become effective, this obligation will apply to all controllers and processors (Article 33 (1) and (2)), no longer only to providers of electronic communications services.

Any and all data breaches will henceforth have to be notified to national supervisory authorities, whether under the currently applicable Directive 2002/58 and national transposition measures or under the forthcoming GDPR.

Since Directive 2002/58 left it to such supervisory authorities to adopt guidelines and issue directions for the implementation of this obligation, the content and form of the notification and the period within which it must be made vary from one Member State to the other[4]. The GDPR imposes a notification "*without undue delay and, where feasible, no later than 72 hours after having become aware of it*" (Article 33 (1)) and the minimum content to be included therein (Article 33 (3)).

The most complex issue with respect to data breaches it to determine the threshold that triggers the obligation to notify the data subjects.

Under Directive 2002/58, notification is mandatory "*when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual*" (Article 4 (3)). French law provides that the breach must be notified "*when such breach is likely to infringe the personal data or the privacy of a subscriber of another natural person*" (Article 34 bis, II of Law n°78-17 of January 6, 1978 on data processing, data files and individual liberties , also referred to as the French Data Protection Act). The DGPR stipulates that this obligation shall apply "*when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons* (Article 34 (1).

It remains to be seen how the national supervisory authorities of the Member States will implement this provision and, in particular, interpret the "highness" of a risk, even potential.

It should be noted that the GDPR restates and extends the possible exemptions to this obligations to notify the data subjects, including the implementation of appropriate technical and organizational protection measures or public communications (Article 34 (3)).

Transfers of personal data (Chapter V)

The principles governing the international transfer of data remain the same: The recipient country must offer adequate and appropriate safeguards.

The adequacy of the level of protection offered by the recipient country can be acknowledged by the European Commission in a so-called "adequacy decision" (Article 45 (1)).

If the recipient country is not mentioned in the European Commission's adequacy decision, specific safeguards must be provided (Article 45 (2)). For this purpose, the Standard Contractual Clauses issued by the European Commission remain applicable. Other options will be available: Codes of conduct, certification mechanisms, data protection seals and marks, and corporate rules.

Whenever any of these items is implemented, there will be no need to carry out a specific formality with, or obtain an authorization from, the national supervisory authority.

If the processing is based on consent, such consent must be explicit and the data subject must have been informed of the possible risks associated with such transfer (Article 49 (1) (a)).

As indicated above, these rules governing international transfers of data shall also apply to processors (Article 44).

Remedies and penalties (Chapter VIII)

Currently, Directive 2002/58 simply imposes on Member States the obligations to include in their domestic

legislation:

- *"the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question"* (Article 22);
- That *"any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered »* (Article 23).

Data subjects must, therefore, pursue the remedies and abide by the liability rules provided for by Member States, which may entail, for the same infringement, a difference of treatment from one Member State to another.

The GDPR stipulates instead that each data subject shall have (i) the "*right to an effective judicial remedy*" against the data controller or the processor, and also against the competent national supervisory authority (Articles 78 and 79), and (ii) a "*right to compensation*" (Article 82).

It also directly sets forth the rules that must be applied to determine the competent jurisdiction and, as such, the Member States' own private international law rules shall no longer apply (Articles 78 and 79).

Above all, while Directive 2002/58 gave Member States carte blanche to take "*suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive*", the GDPR includes general conditions for the imposition of administrative fines by national supervisory authorities (Article 83 (2)).

Depending on which provision(s) is/are infringed (by the controller or processor), such fines may be up to EUR 10,000,000, or in the case of a business, up to 2 % of the total worldwide annual turnover of the preceding financial year (Article 83 (4)), or even up to EUR 20,000,000, or in the case of a business, up to 4 % of the total worldwide annual turnover of the preceding financial year (Article 83, (5)).

By way of comparison, under applicable French legal provisions, the *Commission nationale Informatique et Liberté* (i.e. the French supervisory authority) may impose fines up to EUR 150,000 and, in case of repeated offenses, EUR 300,000 or, in the case of a business, 5% of its gross annual turnover up to a maximum of EUR 300,000 (Article 74 of the French Data Protection Act).

[1] Paragraph 1 impose on the controller the obligation to "*implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing*".

[2] European Commission's impact assessment report on the draft GDPR dated Janaury 25, 2012, SEC (2012) 72 final, pp. 29-32 (http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf)

[3] Cf. article entitled "Companies will soon be required to notify data breaches in France" published in our June 2011 e-newsletter.

[4] For France :https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles