SOULIER BUNCH

Published on 29 June 2018

Soulier Bunch, Cabinet d'avocats d'affaires basé à Paris et Lyon

Read this post online

France adopts a new Data Protection Act

Law n°2018-493 of June 20, 2018 on the protection of personal data was promulgated on June 20, 2018 and published in the Official Journal on June 21, 2018.

The purpose of this new Law is to adapt Law n° 78-17 of January 6, 1978 on information technology, data files and liberties (commonly and hereinafter referred to as the 'French Data Projection Act") to UE law following the General Data Protection Regulation that entered into force on May 25, 2018 (hereinafter the "GDPR")[1] (a Regulation is binding in its entirety and directly applicable in all EU Member States) and Directive 2016/680 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 (a Directive is binding on Member States as to the result to be achieved but leaves them the choice of the form and method) that ought to be transposed into domestic law by May 6, 2018 (hereinafter the

“Directive 2016/680”).

In order to comply with EU law, the French State decided not to repeal the 1978 French Data Protection Act but to adapt it.

The new Law on data protection (the “New Data Protection Act”) includes a Title I that addresses the common provisions of the GDPR and Directive 2016/680, a Title II that contains provisions on the numerous derogations available to Member States under the GDPR, a Title III that contains provisions transposing Directive 2016/680, a Title IV that includes specific provisions to facilitate the enforcement of personal data protection rules by local authorities (by empowering the French Government to use ordinances to adopt measures that are normally a matter of law to improve the readability of the new French data protection legislation), and lastly a Title V that contains various miscellaneous provisions.

It should be noted that approximately ten Implementing Decrees of the *Conseil d’Etat* (Council of State) are expected to be published, after receiving the opinion of the Commission *nationale de l’informatique et des libertés* (French Data Protection Authority, also known under the acronym “CNIL”), in order to finalize the adaption of French legislation to EU law.

The end of prior formalities

While the French Data Protection Act enshrined a process of prior formalities, the GDPR makes a radical change and imposes a process of continued compliance: All relevant actors must ensure at all times compliance was applicable data protection rules and must be able to demonstrate compliance.

The New Data Protection Act replaces the *a priori* control mechanism – based on prior declarations and authorization – by *a posterori* control mechanism based on the data controller’s assessment of risks related to data protection.

On the other hand, the powers of the CNIL have increased and fines up to 20 million euros or 4% of the annual worldwide consolidated revenue can be imposed.

It should be noted, however, that the prior formality process is maintained for the most sensitive data, such as *biometric data necessary to identify or verify the identity of individuals, genetic data, data using the registration number of a given individual in the national register of natural persons, or healthcare data*.

The CNIL

The New Data Protection Act defines the tasks entrusted to the CNIL, as per the provisions of the GDPR.

The CNIL becomes the national authority responsible for monitoring the enforcement of the GDPR.

It is in charge of publishing reference frames, codes of good conduct and model regulations on the new obligations imposed on operators. It has the power to certify bodies and services. It can be consulted on any

bill on personal data protection by the Chairs or the competent committees of the National Assembly or the Senate as well as by the chairs of parliamentary groups.

The New Data Protection Act clarifies and expends the CNIL's control powers. CNIL agents can access, from 06 :00 am to 09 :00 pm, places, premises, buildings, facilities or establishments used in connection with a system that processes personal data, excluding part of such places that correspond to private residence. Secrecy is not enforceable against such agents, except for information covered by professional secrecy between lawyers and clients, secrecy of journalistic sources or, subject to certain restrictions, medical secrecy. For online controls, CNIL agents may henceforth use a cover identity.

Sensitive data

As per the provisions of the GDPR, the scope of sensitive data (racial origin, political opinions, etc.) is extended to genetical and biometric data as well as data concerning the sexual orientation of a person.

In principle, these data may not be processed because of their very nature.

Derogations from this general prohibition are, however, allowed under EU law (e.g. if the person has expressly agreed to the processing of his/her data or has made them public, for social security purposes, etc.).

The New Data Protection Act adds other derogations. In particular, the processing of biometric data (fingerprints, etc.) strictly necessary to control access to workplaces, computers and applications used at work are allowed. Similarly, the processing concerning the re-use of information included in court decisions disseminated in the framework of the open data is allowed.

Minors' consent

For minors under the age of 15, the consent of the holders of the parental authority will be necessary for the processing of personal data on social networks. From the age of 15, minors will be entitled to register on social networks without parental or guardian authorization.

Use of algorithms

The New Data Protection Act expends the situations where, by way of exception, a decision that produces legal effects on the data subject or affects him/her significantly can be taken solely based on automated processing of personal data (i.e. the use of algorithms to make automated individual decisions).

These provisions were strongly discussed between the Senate and the National Assembly in the context of great controversy about the use of algorithm by universities in connection with the so-called *Parcoursup* web site (i.e. French higher education admission online platform that receives and manages the wishes of the students).

In its decision dated June 12, 2018, the Constitutional Council approved these provisions but, however, specified that the administration must "*master the algorithm process and its developments*" and consequently

held that "*cannot be used, as an exclusive ground for an administrative individual decision, algorithms likely to revise themselves the rule that they apply, without the control and the approval of the data controller*" (so-called "self-learning algorithms").

Collective action

The collective action with respect to personal data was introduced in France by Law n° 2016-1547 of November 18, 2016 for the modernization of justice in the 21st century that had inserted Article 43 ter in the French Data Protection Act.

When several natural persons placed in a similar situation suffer a damage, the common cause of which is a breach of a similar nature of a provision of this Act by a person liable for processing personal data or by a subcontractor, a collective action can be brought before the competent civil or administrative court to put an end to a breach by a person liable for processing personal data or by a subcontractor (it being specified that only associations or organizations are entitled to bring such an action).

The New Data Protection Act enhances the scope of this type of collective action to seek compensation for the material and non-material damage suffered as a result of a breach of personal data, in a context where the association called *Quatradure du Net*, an association for the defense of internet surfers, announced that it had filed five collective complaints against Google, Apple, Facebook, Amazon and LinkedIn (Microsoft), as it considers that these companies do not comply with the requirement of the GDPR on the "*freely given and informed consent*" of internet surfers.

[1] Cf. our articles entitled "New regulation on data protection (Part I)" and "New regulation on data protection (Part II)"