SROUJI AVOCATS
AVOCATS A LA COUR

www.sroujiavocats.com

215 rue du Faubourg Saint-Honoré
75008 Paris
France

Tel: +33 (0)1 78 64 64 83
info@sroujiavocats.com

November 2018

GDPR: Revolution or evolution? Recap since May

Daphné Moutardier, Counsel
Joseph Srouji, Partner

The General Data Protection Regulation (GDPR) officially came into force on 25 May 2018 and has more or less lived up to expectations, effectively marking the dawn of a new awareness in data protection. A revolution? Not quite, but close enough.

In the case of France, the GDPR was adopted into French law in August with the modification of the *Loi informatique et libertés* (French Data Protection Act). Other EU countries are following the same approach, tweaking national legislation to fall in line with GDPR standards.

In practical terms, indications are that companies with EU operations have been proactive in implementing policies and procedures relatively quickly to be GDPR compliant. The French Supervisory Authority (*Commission Nationale de l'Informatique et des Libertés* , or CNIL), widely regarded as a thought-leader in EU data protection matters (having been very active during GDPR drafting), has as yet been shy when exercising its newly-granted powers of sanction but nevertheless remains as active as ever.

So while the GPDR *event* may not be a revolution per se, a recent CNIL report (*RGPD : quel premier bilan 4 mois après son entrée en application ?*) indicates that, four months since taking effect, the GDPR has definitely been a wake-up call for some slow adopters as the CNIL raises the bar in its enforcement posture. To date the CNIL has already issued several formal notices (*mise en demeure*) and (modest) administrative fines.

I. Changing times since May

According to the CNIL's report, the data protection landscape is indeed quickly changing:

- 15,000 Data Protection Officers (DPOs) have been designated (compared to 5,000 *Correspondant Informatique et Liberté*s (CILs))
- More than 1,000 data breach notifications received
- 7 million visits to the CNIL website
- 130,000 downloads of the CNIL's simplified data protection register
- 9700 complaints received (34% more than in 2017 over the same period)

Consistent with its role as data protection "leader" among supervisory authorities, the CNIL has announced the introduction of several guidelines and toolkits to help companies work towards compliance, for example:

- Toolkits (*référentiels*) relating to customer and prospect management; human resources; health vigilance
- A standard regulation on biometrics, in order to set a stringent and protective framework for this sensitive data
- A certification procedure (as a reminder, certification replaces the CNIL's labelling activity). The CNIL has already adopted two standards for DPO certification
- Codes of conduct are being prepared, including medical research and so-called "cloud" infrastructures
- An online training module on the fundamental principles of the GDPR
- Thematic sheets for local authorities, covering various issues such as teleservice, electronic administration, etc.

II. Speak softly and carry a stick

Several formal notices or sanctions have been published by the CNIL since the GDPR's adoption. While the sanction amounts are relatively modest it is clearly a sign of things to come (especially for bigger companies with global operations and international data flows). Here is a summary of a few cases that caught our eye:

1) Biometric data

The CNIL identified several non-compliant practices during an on-site inspection of a company specialising in remote monitoring of elevators and car parks (dating from 2016):

- The company had set up a biometric system to monitor its employees' schedules, consisting of collecting employee fingerprints who had not provided their consent prior to system implementation
- The company had also set up a system for recording telephone calls, without informing employees or other stakeholders
- The workstations were not sufficiently secured with "robust" passwords or automatic screen locking

The CNIL first gave formal notice to the company to comply with the French Data Protection Act. However, during a second audit in 2018, the supervisory authority noted that some shortcomings persisted, resulting in a modest fine of 10,000 euros.

2) Video surveillance (CCTV)

In February 2018, the CNIL carried out an inspection at the premises of the "42" school, an institution devoted to training students in information technology.

The supervisory authority found that:

- Students' workspaces, offices dedicated to administrative staff, as well as living areas such as the cafeteria were permanently filmed by cameras
- The people filmed were not properly informed
- The video surveillance images were accessible in real time to students on the school's intranet network (from their personal working space)

Association "42" – creator of the school – was given notice to permanently cease filming classrooms and living spaces. The CNIL reminded the association that any video surveillance system placing employees or students under constant surveillance is considered as excessive. The CNIL also noted that the video surveillance images must only be accessible by authorized persons, determined by their function within the school. The supervisory authority also asked the association to duly inform those being filmed by the CCTV system.

3) Misuse of personal data

In February and March 2018, the CNIL carried out an on-site audit of several companies responsible the implementation of supplementary pension schemes, and which have access to personal data made available by federations for the purpose of collecting contributions to pay pension benefits.

The supervisory authority noted that the personal data were also being used for other purposes.

In the case at hand, personal data of several thousand people were processed by these companies for “secondary purpose” with the intent to market products and services offered by partner companies.

The CNIL issued a formal notice to these companies to cease the practice within one month. Once this period has expired, a sanction will likely be levied if the personal data continue to be used for other purposes.