PROTECT YOUR DATA IN 5 LESSONS

By Aleksandra THÉLOT
Intellectual Property Lawyer,
REGIMBEAU

Paris, April 29, 2019

Between 2017 and 2018, approximately 70% of the National Commission on Informatics and Liberty's public decisions financially sanctioned the breach of a controller's security and confidentiality obligations.

The obligation to ensure security is one of the key principles of the processing of personal data of Act n°78-17 of January 1978 on Information Technology, Data files and Civil liberties. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) reinforces this principle.

Data security is therefore a major issue to be considered in the governance of IT tools and systems.

Who? As guarantor of data security, the controller [if applicable, the processor[1]] must take all necessary precautions to preserve data security and, in particular, to prevent it from being altered, damaged or accessed by unauthorised third parties. This principle is laid down in Article 34 of the French Data Protection Act and Article 5 of the GDPR.

What? The security obligation applies not only to so-called 'sensitive' data[2] but to all personal data. Indeed, the qualification of data as 'sensitive' has no influence on the determination of a breach of the obligation to ensure the security of processed data.

How? By '**own means**' and '**appropriate technical and organisational measures**' to ensure data security and guarantee a level of security appropriate to the risk. Neither Article 34 of the French Data Protection Act nor Article 32 of the GDPR are prescriptive as to the measures to be deployed by the controller, as long as the obligation to guarantee security is ultimately respected.

[1] Article 32 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016
[2] Deliberations n°SAN-2018-009 of 6 September 2018, n°SAN-2018-012 of 26 December 2018, etc.

Which Sanctions? Depending on the category of the offence, the supervisory authority in France (the CNIL) may impose penalties of between €10 to €20 million, or 2% to 4% of the company's worldwide annual turnover.

Even before the GDPR came into force, the CNIL had occasion to sanction breaches of security and data confidentiality obligations, particularly in its recent decisions Dailymotion (fine of €50,000), ADEF (€75,000), Optical Center (€250,000), Hertz (€40,000), Darty (€100,000), Association Alliance Française Paris île de France (€30,000), Bouygues Telecom (€250,000), and Uber France SAS (€400,000).

These decisions provide lessons for adopting good practices to ensure data security.

⊙ LESSON 1: IMPLEMENT BASIC SECURITY MEASURES

In the different cases submitted to the CNIL, we note in particular:

- The absence of a mechanism to avoid URL predictability;
- The absence of a user identification or authentication procedure (for example, a website that does not include a feature verifying that a customer has signed-in to his/her personal space before accessing documents);
- The absence of vulnerability testing of upstream websites (by checking, for example, that their production launch was preceded by a complete test protocol).

The GDPR establishes a data protection logic at the earliest stages of design and by default. Therefore, when designing IT tools or systems, it is recommended to follow the following basic steps:

- Check URL filtering rules (e.g., by changing a word in the URL);
- In the event of a remote connection to a company's internal computer network, at a minimum, implement IP address filtering measures to allow only identified and authorized IP addresses, or use a VPN;
- Consider implementing a procedure for identifying or authenticating website users to protect recorded information (e.g., uploading documents);
- In case of user authentication, identifications must not be disclosed or stored in an unprotected file;
- For passwords, scrupulously follow **deliberation n°2017-012 of 19 January 2017** adopting a recommendation relating to CNIL passwords (unique identifier per user, complex password, regular password changes, account locking after several failures, etc.);
- For workstation access, set automatic locking in case of inactivity, install a firewall, use regularly updated antivirus software, etc.;
- In case of use of service providers, check the characteristics of products, tools and IT systems;
- etc.

⊙ LESSON 2: REGULARLY MONITOR THE SECURITY OF YOUR IT TOOLS AND SYSTEMS

In most decisions pronounced by the CNIL, the authority emphasizes the importance of performing regular inspections of the security measures put in place by the controller.

In practice, these inspections must be done both before and during production start-up as well as after deployment of tools and/or systems or websites. Finally, controllers test the measures put in place throughout the process. Hence the term '**regular**' inspections. The CNIL specified in the BOUYGUES TELECOM decision that tests performed each year (for more than 2 years) were not sufficient to prevent a possible data breach.

In addition, security controls must be proportionate to the human and technical resources at the disposal of the controller. The CNIL has specified that: 'when *the controller has had, from the outset, a system to ensure user data security, the use of this security solution does not represent a disproportionate effort and is inexpensive as long as it is available in the tool used to design its websites*'.

Furthermore, in the HERTZ decision, the CNIL notes that the fact that the company took the initiative to proceed with a security audit of its subcontractor only a few weeks after the occurrence of a data breach is a good indication of this regular monitoring.

⊙ LESSON 3: MONITOR THE ACTIONS OF YOUR SUBCONTRACTORS

When data processing operations are entrusted to subcontractors, this does not relieve the controller of his responsibility to preserve the security of data processed on his behalf. Indeed, the controller must ensure and verify that all components and options of the tool or system of the service provider comply with security measures in accordance with the GDPR.

<u>Before a data breach</u>

It is the controller's responsibility to inspect the characteristics of the (standard) product selected from his service provider. In the DARTY decision, these inspections would have 'allowed the risk resulting from the existence of an access to customer data contained in the management tool to be identified and would have prevented the risk of a data breach'.

In the HERTZ decision, the data breach results from an error made by the service provider during a server change operation due to an accidental deletion of a line of code. The CNIL found that HERTZ had been negligent in monitoring the actions of its service provider. Specifically, this negligence seems to be characterized by the absence of specifications related to the development of the website and of a complete test protocol when changing servers.

After the data breach

In the DARTY decision, in view of the elements of the case, the CNIL considered that the controller had not regularly monitored the actions of his subcontractor and was negligent in monitoring his subcontractor when the data breach was resolved. DARTY made only one request for clarification from the subcontractor with regard to the corrective measures put in place to resolve the security breach.

In relations with subcontractors, it is recommended that the controller take an active role and be able to justify requests for corrective measures to his subcontractor. These requests must be daily and occur both before and for the duration of the breach.

⊙ LESSON 4: DOCUMENT TO PROVE

The **'accountability'** logic of the GDPR[3] requires the controller to document in order to demonstrate compliance. To control the security of IT tools and systems, the CNIL recommends performing complete test protocols and audits. These tests (e.g. penetration tests or audits) must of course be appropriate. For example, concerning a line that composes a computer code for a website, 'special attention must be paid to the authentication mechanism, which requires a manual review of the code'.

Other documents can also help control tool security, such as the processing register, impact assessments, various contracts and contract amendments with your service providers

More generally, the GDPR provides methodological tools such as certifications, labels or codes of good conduct, the application of which [...] can serve as an element to demonstrate compliance with the obligations incumbent on the controller (Article 24.3) and which may also be taken into account by the supervisory authority in the event of litigation proceedings (Article 83).

⊙ LESSON 5: DO NOT WAIT TO ACT

[3] Article 24 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

Securing and protecting processed data, and more generally the process of compliance with the GDPR, seems complex.

Complex but not impossible, don't hesitate to act!

All of REGIMBEAU's teams are available to support and advise you in setting up technical and legal solutions to protect and secure your data processing in accordance with the new rules resulting from the GDPR.

Aleksandra THÉLOT (thelot@regimbeau.eu)
Intellectual Property Lawyer

- About REGIMBEAU:

> *REGIMBEAU, a French IP law firm, has been assisting companies and private and public project developers to protect, enhance and defend their innovations (patents, trademarks, designs) for more than 85 years. Fifteen partners head a team of more than 200 people whose skills are put into practice in every strategic aspect of Intellectual Property - business intelligence and information search, license agreements, IP portfolio audits, partnership negotiations, acquisition of industrial property rights, litigation. Thanks to its wide-ranging expertise, REGIMBEAU (present in Paris, Munich, Lyon, Rennes, Grenoble, Montpellier, Toulouse and Caen) can meet its clients' needs for international strategic consulting while preserving personalized relations of the highest quality.*