Read this post online

Investigations and sanctions: What lessons can be drawn from the CNIL's activities?

On April 15, the *Commission Nationale de l'Informatique et des Libertés*(French Data Protection Authority, hereinafter the "CNIL") presented its 2018 activity report, i.e. the assessment that it draws from its activities during the year 2018 which has been marked by the application of the General Data Protection Regulation and the new French Data Protection Act.

From the CNIL's assessment and the decisions it took in 2018, we can learn lessons to prevent the risks incurred when processing personal data.

Lesson n°1

Almost one out of four investigations are triggered by a complaint or a report. The CNIL received a record number of complaints in 2018 (a 32.5% increase compared to the number of complaints in 2017 which according to the CNIL is due the media impact of the GDPR and increased public awareness). 73% of these complaints/reports concerned the exercise of a right.

The data controller has indeed the obligation to provide information and ensure transparency vis-a-vis the persons whose data are processed, and to respond as expeditiously as possible to their requests (to consult, rectify or delete their data).

In practical terms, each time personal data is collected, the controller must mention in the medium used (form, questionnaire, contract, etc.) a certain amount of information on the data processing and provide the means to effectively exercise the rights of access, rectification, opposition, deletion, portability and limitation of the processing. Most often it will be about providing a specific contact form, a telephone number or a dedicated email address, or else the possibility of exercising rights from an account. Of course, an internal process must be put in place to ensure that requests are identified and processed in a timely manner.

© 2024 - **SOULIER Avocats** All rights reserved

If we add to these figures the decision made by the CNIL to include respect for the rights of individuals in its 2019 investigation strategy (the annual work program, which accounted for 16% of investigations in 2018, refers to the 3 topics chosen by the CNIL each year on which it will focus its control strategy), and its willingness to make the request to exercise rights a prerequisite before referring a matter to it, we can only recommend that all controllers ensure that they inform the persons whose data they collect and respond to the requests they receive.

Lesson n°2

The CNIL may carry out onsite inspections, online inspections, inspections on the basis of documents (which consist in requesting any useful information or document) and hearings (which are carried out in the CNIL's premises, after summoning the controller).

In 2018, one out of three investigations were carried out onsite, at the controller's premises.

The Decree enacted for the application of the French Data Protection Act stipulates that "*Where the Commission* [i.e. CNIL]*carries out an on-site inspection, it will inform, at the latest at the beginning of the inspection, the custodian of the premises of the purpose of the intended verifications as well as of the identity and capacity of the persons conducting it (…)*".

Pursuant to Article 44 III of the French Data Protection Act, CNIL's members "*may ask for the communication of all the documents necessary for the performance of their mission, whatever their medium, and take a copy of them. They may collect, on-site or upon summons, all useful information or proof necessary for the performance of their mission. They may have access, under conditions preserving confidentiality vis-à-vis third parties, to electronic data processing programs and data, and ask for their transcription, by any appropriate process, into directly utilizable documents for the purposes of the investigation. Secrecy may not be invoked against them except in respect of information covered by the professional secrecy applicable to lawyer-client relationships, by the confidentiality of journalistic sources or, subject to the second paragraph of this III, by medical secrecy.*"

In other words, it is essential to set up an internal control management procedure detailing the various actions to be taken in practice, in order to avoid any confusion during the investigation.

One out of six inspections are carried out online, i.e. from the premises of the CNIL which consults, from an online public communication service (website, app., connected product, etc.), data accessible online or made accessible, including through carelessness, negligence or actions by a third party. The new Data Protection Act now allows the CNIL to do so under an assumed identity. This means that it can use an e-mail address other than its own and a pseudonym to perform investigations on the Internet or on an app.

Lesson n°3

The CNIL pronounced 11 sanctions, including 10 monetary sanctions, 9 of which were made public (including 400,000 euros for Uber, 250,000 euros for Bouygues, 250,000 euros for Optical Center[1]).

© 2024 - **SOULIER Avocats** All rights reserved

Out of the 9 sanctions made public, 7 were pronounced as a result of a complaint or report. All of them concerned breaches of the security of personal data. These decisions show that the CNIL also check compliance with the cybersecurity basics, and not only with purely legal rules provided in the GDPR.

It should be noted that these fines concern facts that took place before the entry into force of the GDPR. They were, therefore, pronounced on the basis of the "previously applicable" Data Protection Act, which provided for a maximum amount of fine of 3 million euros. Today, depending on the type of breaches, the amount of financial penalties under the GDPR can reach up to 20 million euros or, in case of a company, up to 4% of its worldwide annual turnover.

It should not be forgotten that it was the CNIL that imposed on Google in January 2019 the largest fine ever pronounced on the basis of the RGPD (50 million euros)[2].

Lesson n°4

The CNIL does not elaborate much on the appeals lodged against its decisions before the Council of State. It must be said that the Council of State rarely has the opportunity to express its opinion on the decisions rendered by the CNIL.

As the GDPR takes a more repressive logic, it will be interesting to follow the evolution of the CNIL's practice and to observe – perhaps – the progressive development of a line of case law governing the CNIL's inspection and sanction activities.

In this respect, it should be noted that on April 17, 2019 the Council of State handed down a decision in which it upheld but reduced the 250,000 euros fine imposed by the CNIL on Optical Center.

According to the Council of State, a monetary sanction imposed by the CNIL must take into account in particular the behavior of the data controller following the observation of the failure to fulfil its obligations. The Council of State considered that the sanction imposed by the CNIL was disproportionate because it did not take into account the speed with which Optical Center remedied the alleged breaches and, therefore, reduced the amount of the fine to 200,000 euros (i.e. a 20% reduction).

[1]Cf. article entitled Data leak: The French Data Protection Authority imposes a record fine on Optical Center

[2]Cf. article entitled Personal Data: Google gets fined

Soulier Avocats is an independent full-service law firm that offers key players in the economic, industrial and financial world comprehensive legal services.

We advise and defend our French and foreign clients on any and all legal and tax issues that may arise in connection with their day-to-day operations, specific transactions and strategic decisions.

Our clients, whatever their size, nationality and business sector, benefit from customized services that are tailored to their specific needs.

© 2024 - **SOULIER Avocats** All rights reserved

For more information, please visit us at www.soulier-avocats.com.

This material has been prepared for informational purposes only and is not intended to be, and should not be construed as, legal advice. The addressee is solely liable for any use of the information contained herein.

© 2024 - **SOULIER Avocats** All rights reserved