Published on 30 August 2018 by **Laure Marolleau**, Member of the Paris Bar
l.marolleau@soulier-avocats.com
Tel.: + 33 (0)1 40 54 29 29

Read this post online

Data leak: The French Data Protection Authority imposes a record fine on Optical Center

250,000 euros. This is the amount of the fine imposed by the *Commission Nationale de l'Informatique et des Libertés* (French Data Protection Authority or "CNIL") on Optical Center, a French company specialized in optics, for having failed to properly secure its website www.optical-center.fr.

This is the first time that the CNIL imposes such a heavy fine. And this is not under the General Data Protection Regulation ("GDPR") which provides that companies may be fined up to 20 million euros and 4% of their turnover.

On July 28, 2017, the CNIL was informed of a possible significant data leak concerning the company Optical Center. Specifically, it was told that data were freely accessible from several URLs with the same structure.

On July 31, 2017, the CNIL carried out an online inspection which established that it was possible, by entering several URLs in the address bar of a browser, to access hundreds of invoices concerning customers of the company. These invoices contained data such as the last name, first name, postal address as well as health data (ophthalmic correction) or, in some cases, the social security number of the persons concerned.

The CNIL immediately alerted Optical Center which in turn asked its provider to take the necessary measures to put an end to this security incident. The breach was remedied on August 2, 2017 through the addition of a new functionality.

On August 9, 2017, the CNIL then carried out an on-site inspection in the premises of the company that acknowledged that it had a website security breach.

Specifically, the website www.optical-center.fr did not include a functionality to verify that a customer is connected to his personal space ("customer area") before displaying his/her invoices. It was thus relatively simple to access documents concerning another client of the company.

The CNIL immediately initiated a sanction procedure against Optical Center.

It is interesting to note that Optical Center complained about the lack of any prior formal notice which it considered as a "substantial component" of the procedure to ensure due process and respect of the rights of the defense.

The CNIL simply swept aside this argument as the law provides that when the detected breach cannot be remedied through a formal notice, it has the power to impose at the end of an adversarial process penalties, in particular fines, without any prior formal notice.

The CNIL held that the company had failed to comply with its obligation to ensure the security of personal data, in breach of Article 34 of the French Data Protection Act, and thus issued a 250,000 euro fine.

Even though Optical Center had acted proactively to remedy the breach, the CNIL considered that:

- the issue of the restriction of access to documents made available to clients from their personal area should have been given specific attention by the company. The implementation of such a functionality was, according to the CNIL, an essential precaution of use;
- exploiting the data breach did not require any specific technical skills. The CNIL recalled that the fact of making resources available without any prior access control device had been identified for many years as one type of security breaches that must be carefully monitored and tested in the framework of security audits;
- Optical Center could not be unaware of the risk associated with a lack of security of its website as it had already been fined 50,000 euros in 2015 for a security breach.

The CNIL also explained that the publication of its decision was necessary notably because of:

- the particular sensitivity of the data that were made freely available,
- the number of clients impacted, and
- the volume of documents contained in the company's database at the time of the incident (more than 334,000).

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.

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