JONES DAY

COMMENTARY

JULY 2018

French Data Protection Authority Confirms Enforcement Trend on Security Obligations for Data Controllers

IN SHORT

The Situation: Even before the General Data Protection Regulation ("GDPR") became effective on May 25, there has been a noticeable trend in the enforcement of security obligations through increased sanctions.

The Development: The French Data Protection Authority (*Commission Nationale Informatique et Libertés*, or "CNIL") issued a pecuniary sanction against optical provider Optical Center for a security breach affecting the company's e-commerce website.

Looking Ahead: Especially now that GDPR has taken effect, it is important for controllers and processors to confirm that they have robust security policies and procedures in place.

Lire la Version Française >>

In a decision dated May 7, 2018, the CNIL issued a pecuniary sanction of €250,000 against optical provider Optical Center for a security breach affecting the company's e-commerce website. Although the decision was taken before May 25, when the GDPR became effective, this decision confirms a trend in the enforcement of security obligations through increased sanctions, as already evidenced earlier this year in the CNIL's decision against a household appliance distributor.

In spite of the company reacting swiftly to correct the anomaly as soon as it became aware of it, the CNIL considered that "elementary security measures" had not been implemented on the website, and thus found that Optical Center had breached its security obligations in relation to its customers' personal data.

The CNIL had been able to access documents stored on customers' accounts, such as customers' invoices and order history, on the company's e-commerce website. The documents the CNIL was able to access also included health information contained in prescriptions uploaded by customers, as well as social security numbers. The website did not contain an authentication system allowing it to restrict access to documents to a specific customer, and customers' accounts could be accessed merely by changing urls.

> The CNIL considered that "elementary security measures" had not been implemented on the website, and thus found that Optical Center had breached its security obligations in relation to its customers' personal data.

The CNIL noted that communications with the company's supplier regarding new website features had remained informal. This resulted in Optical Center, as data controller, lacking visibility on its supplier's actions, corrections or recommendations, including in terms of security measures.

Based on the CNIL's reasoning detailed in the decision, the following minimal security measures should have been applied on the website:

- Implement access control features allowing the company to verify that a user is authenticated prior to giving a user access to personal documents;
- Conduct security audits on the website, including to test access control features;
- Formalize communications with suppliers regarding website development, corrections, and recommendations, including in terms of security;
- Describe the testing procedures to be applied prior to launching new features or updates, and document that the testing procedures have been followed in each case (e.g., through a formal acceptance form).

By issuing a sanction without providing prior formal notice, the CNIL used its new sanctioning powers granted under Article 45 of the French *Data Protection Act* as modified by the *Act for a Digital Republic* of October 7, 2016. The provision allows for direct sanctions without prior formal notice when the violation

is such that it could not have been corrected in the context of formal notice—similar to what is now applicable under the GDPR.

The CNIL ordered that the additional sanction of publicity of the decision be applied, in spite of the company's arguments that the security violation was not intentional, that the company had not derived any advantage from it, that there was no evidence that anyone but the CNIL's investigation teams had found the breach, and that no harm seemed to have been caused to the data subjects concerned.

With the increase in sanctions under the GDPR, this decision confirms that controllers and processors ought to check that they have robust security policies and procedures in place, including in terms of restrictions on suppliers involved in setting up data processing tools. Under the GDPR, sanctions for breaches relating to security obligations occurring since May 25 are set to a maximum of €10 million or two percent of a company's worldwide annual turnover for the preceding year.

KEY TAKEAWAY

Given the current trends and the recent increase in regulations under GDPR, companies need to ensure they have robust plans and procedures to protect consumer data. Breaches to security obligations will be met with financially significant sanctions.


Olivier Haas
Paris


Undine von Diemar
Munich


Daniel J. McLoon
Los Angeles


Mauricio F. Paez
New York

YOU MIGHT BE INTERESTED IN: [Go To All Recommendations >>]


Draft EU CLOUD Proposal—Enabling Law Enforcement Access to Overseas Data


U.S. Government Releases Report on IoT Botnets and Other Distributed Attacks

Jones Day Talks: Privacy & Data Security GDPR is Coming: Is Your Company Ready?
