Data breach - The French Conseil d'Etat lowers the amount of a fine imposed by the French Data Protection Authority

In a decision dated 17 April 2019, the Conseil d'Etat (the Supreme Administrative Court) confirmed a decision of sanction issued by the French Data Protection Authority (the CNIL) but reduced the amount of the sanction from €250,000 to €200,000.

Submitted	30 April 2019
Applicable Law	France
Topic	Information, Communication & Technology > Data protection & privacy
Sector Focus	Technology Media and Telecommunications
Contact	Christophe Fichet, Anne Baudequin

Conseil d'Etat, decision No.422575 dated 17 April 2019, 10ème-9ème Chambre

In a decision dated 17 April 2019, the Conseil d'Etat (the **Supreme Administrative Court**) confirmed a decision of sanction issued by the French Data Protection Authority (the **CNIL**) but reduced the amount of the sanction from €250,000 to €200,000.

The context

On 28 July 2017, the CNIL received the information of the occurrence of a data breach affecting the website of an optical company (hereinafter the **"Company"**) and more specifically that personal data was publicly available when entering several URLs in a browser's address bar. The investigation launched by the CNIL revealed that it was possible to access to customers' invoices from the website, including data of such as surnames, names, postal addresses as well as health data and in some cases, the social security numbers.

The Company immediately requested its website provider to implement measures to cure such breach and on 2 August 2017, said breach was remedied.

The decision of the CNIL

The CNIL however decided to initiate a procedure of sanction against the Company on the grounds that the Company had failed to comply with its security requirements with regards to personal data and thus had breached article 34 of Law No 78-17 on Information Technology, Data Files and Civil Liberties dated 6 January 1978[1]. The instruction had indeed demonstrated that the Company's website did not implement a feature requiring customers to log in to their personal space before any invoices were displayed.

The CNIL held that:

- Restricting the access to documents made available to clients from their personal space was an essential measure of use that should have been implemented by the Company.

- The Company was fully aware of the security requirements as it had already been fined for a security breach on its website in 2015.

The breach was qualified as critical with regards to (i) the fact that these invoices contained sensitive personal data, (ii) the number of the clients impacted, and (iii) the volume of documents contained in the company's database at the time of the incident (more than 334,000). As a result, the CNIL issued a €250,000 fine and ordered the publication of its decision. This was the first time that the CNIL issued a fine of this amount.

The decision of the Conseil d'Etat

The Company challenged this decision before the Conseil d'Etat which has the power, to re-examine the alleged breaches.
On 17 April 2019, the Conseil d'Etat confirmed the decision and held that the CNIL had duly characterized the existence of a breach of the security obligations by the Company. However, on the amount of the fine, the Conseil d'Etat gave right to the request of the Company. It considered that the amount of this fine did not take into account the celerity in which the Company had provided corrective measures to remedy the breach. As a result, the CNIL hold that the sanction was disproportionate and reduced the fine to €200,000 euros instead of €250,000.

***

This decision gives precious guidance: in case of a data breach, the implementation of corrective measures is an argument to obtain a reduction of a fine in case of further prosecution by the CNIL. Therefore, where a data breach occurs, the affected company should be as proactive as possible in order to cure the breach but also to limit the amount of a potential sanction by the CNIL.

---

[1] Law No 78-17 on Information Technology, Data Files and Civil Liberties dated 6 January 1978 (the so called "Loi Informatique et Libertés") as modified by law No 2018-493 on the protection of personal data dated 21 June 2018

This document (and any information accessed through links in this document) is provided for information purposes only and does not constitute legal advice. Professional legal advice should be obtained before taking or refraining from any action as a result of the contents of this document.

© Simmons & Simmons LLP 2019. All rights reserved. Registered in England & Wales Registered Number OC352713

elexica Limited, CityPoint, One Ropemaker Street, London EC2Y 9SS