25 May 2016

Newsletter

Data Protection & Privacy

DATA SECURITY BREACH: A FRENCH COMPANY SANCTIONED

A major French company with a worldwide presence has been sanctioned by a public warning of the French Data Protection Authority due to a data security breach.

On July 2015, the French Data Protection Authority ("the CNIL") performed an online investigation on the website of a French company dedicated to a loyalty program as well as promotional items of the brand.

During the online investigation, the CNIL pointed out the weakness of security measures implemented on the website. Indeed, the CNIL agents were able to freely access to several personal data about the company's clients (name, surname, postal and email address, phone number, etc).

Being informed of this security breach by the CNIL, the company answered that corrective actions had been implemented by its hosting service provider.

However, after a second online investigation performed on November 2015, the CNIL noticed that the clients' personal data was still accessible by imputing the direct URL.

The CNIL therefore issued a public warning to sanction the company's failure to comply with the French Data Protection Act.

Here are the key points of the decision :

- The company's website was not secure enough which led to the online disclosure of several personal data about its clients (name, surname, address, phone number, etc);
- the company contacted its hosting service provider which apparently implemented measures to fix the issue;
- The CNIL pronounced a public warning[1] to sanction the company's breach to comply with the articles 34 and 35 of the French Data Protection Act (articles dedicated to security measures).

What should be learned about it?

- As provided by the Article 35 of the French Data Protection Act, the data controller remains responsible of any breach;
- It is always the data controller that is sanctioned in case of a failure to implement sufficient security measures, even if (i) third party providers are involved in the provision of services which lead to the security breach or/and if (ii) there is a contract with third party providers which delegates the provision of such services;
- The absence of any damage for the data subjects (here the company's clients) does not have any impact/consequence on the establishment of the breach/infringement;
- Activities and correction measures implemented by third party providers should always be controlled/monitored by the data controller;
- Provisions regarding security measures inserted in the contract and eventually in the Data Transfer Agreement (e.g. Standard Contractual Clauses) should be clear enough and should allow the data controller to seek for damages/indemnification;
- This decision is in line with the sanction pronounced against a French telco in 2014 (confirmed by the Supreme Court in February 2016);
- This problematic should be taken even more seriously due to the future implementation of the bill for a digital republic, which will considerably increase the sanctions powers of the CNIL (€ 1.5 millions) and will give the opportunity to the CNIL to sanction data controllers to inform personally each data subject of said sanction/breach.

PDGB Société d'Avocats
www.pdgb.com
helene.lebon@pdgb.com

Hélène LEBON - Sandra TUBERT

[1] The full decision is only available in French : https://www.cnil.fr/sites/default/files/atoms/files/deliberation-formation-restreinte-avertissment-public-ricard_ananonymisee.pdf