Read this post online

Companies will soon be required to notify data breaches in France

It is within the context of the recent hack attacks on Sony that the French government made public a draft order[1] imposing on companies responsible for personal data the obligation to notify so-called "data breaches" (i.e. the loss/release of personal data).

On April 18 and April 19, 2011 Sony's PlayStation network[2] was the target of a massive hack attack that resulted in the theft of personal data from 77 million user accounts (including 2.2 million of credit card numbers). Sony then discovered that another system (Sony Online Entertainment[3]) had been hacked on April 16 and 17, affecting 25 million customer accounts. Just when Sony was considered to have brought the situation under control, So-Net (another subsidiary of Sony) was hacked by intruders on May 21. At the time being, it is not possible to know for sure the consequences of these personal data thefts.

What is clear, however, is that these data breaches will cost a lot to the company. In fact, the actual cost will depend on several factors, e.g. do the personal data that have been stolen relate to credit cards? Can a class action lawsuit be filed and lead to the award of damages (which is the case in the USA and in Canada, where a class action lawsuit has already been filed against SONY. In France, the class action still does not exist)? Or do the competent data protection authorities may impose fines (which is the case in France for the *Commission nationale de l'informatique et des libertés*, i.e. the French National Data Protection Commission CNIL, hereinafter "CNIL")?

These historical hack attacks emphasize the need in France to enhance and strengthen existing rules. With respect to data breaches, many countries such as the United States, Germany, the United Kingdom and Austria have opted for transparency and make sure that companies report breach of the data for which they are responsible ("data breach notification").

In France, for the moment, there is no such obligation. Indeed Article 34 of the Law on Data Processing, Files and Individual Liberties only requires the data controller to "*take all useful precautions to preserve the security of the data*".

However, the forthcoming deadline for the implementation of the so-called Telecoms Reform Package (a set of EU Directives passed into law in 2009 that includes provisions on data breach notification) explains that the French government presented on May 3, 2011 a draft order imposing such a notification obligation. Article 38 of the draft order provides that all electronic communications services provider that suffer a data breach

should report such breach to the CNIL and, as the case may be, to the individuals concerned.

Yet, companies will not be required to systematically report a data breach to the individuals concerned. It will be up to the CNIL to decide, depending on whether appropriate protective measures to safeguard security have been implemented by the service provider, whether or not such provider is required to make the data breach public: "*if the CNIL has approved the technological protective measures implemented by the service provider to remedy any violation of personal data and has ascertained that such measures had been applied to the personal data concerned by the breaches*", the data controller is not under the obligation to notify the breach to the individuals concerned.

The adoption of such a rule will constitute an improvement in the area of personal data security, forcing companies to show transparency towards the authorities and, possibly, the individuals. However, according to terms of the draft order, the obligation to notify data breaches only concern electronic communications service providers and does not extend to all data controllers, regardless of the nature of the data.

At the present time, and even if companies are not required to make public data breaches in their computer systems, it is still possible to sanction a company that lost/released personal data.

A data breach is a violation of the Law on Data Processing, Files and Individual Liberties. Under French criminal law, carrying out or causing to be carried out the processing of personal data without putting into practice the measures required by the aforementioned Article 34 is punished by five years' imprisonment and a fine of 300,000 Euros. The disclosure of personal data by carelessness or negligence is also punished by 3 years' imprisonment and a fine of 100,000 Euros (Article 226-22 of the French Criminal Code).

If the notification obligation, as provided for under the draft order, enters into force, the applicable sanctions for failing to notify a data breach would be those set forth in Article 226-17 of the French Criminal Code, i.e. five years' imprisonment and a fine of 300,000 Euros.

Of course, in the absence of notification obligation, the existence and imposition of sanctions rely on the discovery of data breaches. The CNIL may be informed of such data breaches through the filing of a complaint or in the framework of investigations launched on its own initiative. This is precisely what the CNIL is about to do concerning the hack attacks on Sony. The investigation will enable the CNIL to determine the number of individuals concerned by the attack in France, the nature of the personal data that have been stolen, the exact breach, whether the personal data were sufficiently encoded and what information was sent to the individuals concerned. It may lead to administrative sanctions. The sanctions that the CNIL may impose range from the mere warning to fines up to 150,000 Euros.

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.