Published on 30 January 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 security: Darty sanctioned by the French Data Protection Authority

In a deliberation dated January 8, 2018, the *Commission Nationale de l'Informatique et des Libertés* (French Data Protection Authority or "CNIL") imposed a 100,000 euros fine on Darty (a leader in the retail of entertainment and leisure products, consumer electronics and household appliances) for not having sufficiently secured the data of its customers who had made online requests for after-sale services.

The sanction imposed by the CNIL serves as a warning to companies which must comply with the General Data Protection Regulation that will enter into force on May 25, 2018.

Having been informed of a security incident by the publisher of a website specialized in the security of information systems, the CNIL carried out an online inspection in March 2017. It identified a security breach that allowed people to freely access all of the requests made and information provided by the customers of Darty in an online after-sale service request form.

Thousands of requests or complaints containing data such as the name, first name, postal address, email address or phone number were thus potentially accessible.

An on-site inspection carried out a fortnight thereafter established that the online after-sale service request form – that created the security breach – had been developed by an external contractor.

Even though Darty had been informed of the security incident after the first inspection, the CNIL observed that customer records were still accessible between the first and second inspection and that new records had

been created during this period. However, in the evening of the second inspection, Darty declared to the CNIL that the necessary security measures had been implemented to remedy the breach.

Based on these elements, the CNIL considered that Darty had failed to comply with its obligation to maintain the security of data, an obligation imposed by Article 34 of the French Data Protection Act, as it did not sufficiently secure the data of its customers who had completed the online after-sale service request form.

In addition to the 100,000 euros fine, the CNIL decided to publish its decision because of "*the current context of escalation of security incidents and the need to alert Internet users on the risks to their data*".

This sanction also provides the opportunity to inform businesses of their obligations with respect to data protection. And to illustrate the major changes brought about by the GDPR.

Subcontracting

In its deliberation, the CNIL recalled that the fact that the request form had been developed by a subcontractor did not in any way release the data controller of its obligation to main the security of the data.

While the obligations imposed by the French Data Protection Act apply only to data controllers, the GDPR will impose specific obligations on subcontractors.

These new obligations will require the definition of a subcontractor management policy and the adaptation of contracts and agreements.

Accountability

The CNIL considered that Darty should have ensured beforehand that the settings of the device developed for it did not allow unauthorized third-parties to access customers' data, and further specified that "*the preliminary verification of the URL filtering rules in particular is part of the basic tests that must be performed by a company with respect to the security of its information systems*".

It also took the view that the company should have regularly reviewed the forms that fuel the after-sale service request management tool and underlined that "*a good practice in the security of information technology systems would be to disable the features or modules of a tool that are not used or required*".

With the GDPR, the declarative process is abandoned and replaced by a logic of accountability: Companies must implement any appropriate measures to ensure that they comply with their obligations under the GDPR, and must be able to demonstrate compliance at any time.

As such, the CNIL provides examples of good practices to ensure compliance.

Security incident

The CNIL blamed Darty for its poor management of the data breach. It is only after the second inspection that the breach was remedied. Between the first and the second inspection, almost 6,000 customer records were created, bringing the total number of accessible records to almost 1 million.

With the GDPR, all organizations will have the obligations to notify the CNIL of any data breach via a teleservice system without undue delay and, where feasible, no later than 72 hours after having become aware of such breach. They will also have the obligation to inform the data subjects of the breach if there is a high risk that they will suffer adverse effects.

It is, therefore, essential that each organization adopts a specific internal incident management policy.

Penalties

The 100,000 euros fine imposed on Darty is not the highest fine that the CNIL may impose.

While the maximum amount of the fines that the CNIL may impose was raised from 150,000 euros to 3 million euros following the enactment of the Law for a digital Republic, the fines provided for under the GDPR can reach, depending on the nature of the infringement, 10 to 20 million euros or, for businesses, 2% to 4% of the annual worldwide revenue, whichever is higher.