BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 11, Number 9 September 2011

France's New Data Security Breach Notification Requirement For Electronic Communications Service Providers

By Olivier Proust, of Hunton & Williams, Brussels.

On August 24, 2011, France's new law concerning electronic communications (*Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques*, or the "Ordinance") came into force. The Ordinance implements the provisions of the revised EU Directive 2002/58/EC (the "e-Privacy Directive") with respect to the French Data Protection Act of 1978, the French Postal and Electronic Communications Code and the French Consumer Protection Code. In particular, the Ordinance introduces new provisions under the French Data Protection Act (*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*), which impose an obligation on electronic communications service providers to notify any data security breach.

In this context, now seems a good time to review the general security obligations that apply to all data controllers and to examine the new specific requirements that apply to electronic communications service providers in France.

A General Security Obligation for All Data Controllers

Data controllers are generally required under Article 34 of the French Data Protection Act to take all necessary measures to preserve the security of personal data, taking into account the nature of the data and the risks of the processing. In particular, these measures must be taken to prevent alteration of or damage to the data, or their access by non-authorized third parties. Non-compliance with these provisions is punishable by five years of imprisonment and a €300,000 (U.S.$431,312) fine.

In October 2010, the French data protection authority, the Commission nationale de l'informatique et des libertés (CNIL), released a comprehensive handbook ("*Guide sur la sécurité des données personnelles*"), which provides general recommendations and best practices to data controllers to assist with the implementation of appropriate security measures[1] (*see WDPR, November 2010, page 22*).

These security measures equally apply to data processors, who must offer adequate guarantees to ensure the security and confidentiality of the data they process. Data controllers must verify that their processors provide such guarantees, which is why an agreement must be signed between the data controller and the data processor, imposing on data processors the obligation to implement adequate security measures when processing personal data on behalf of a data controller. Ul-

timately, the data controller may be held responsible in case the data processor experiences a data security breach.

Specific Notification Requirements for Electronic Communications Service Providers

The Ordinance of August 24, 2011, introduces a new provision under the French Data Protection Act, which requires electronic communications service providers to inform the CNIL without delay in case of a data security breach.

Regrettably, this new provision applies only to providers of publicly available electronic communications services (*e.g.*, internet service providers and telecom operators). This legal requirement does not apply to all data controllers, as was proposed by the French Senate in its draft proposal for a Law to Better Guarantee the Right to Privacy in the Digital Age.[2] Despite the Senate's fast adoption of this proposal and its subsequent transmission to the National Assembly, the proposal now lies in the hands of a parliamentary commission and stands little chance of ever being adopted.

The Ordinance defines a data security breach as any security breach that accidentally or unlawfully results in the destruction, loss, alteration, disclosure of, or unauthorized access to personal data that is being processed in the context of electronic communications services provided to the public.

In addition to notifying the CNIL, when a breach is likely to adversely affect subscribers' (or any other individuals') personal data or privacy, the service provider also must inform the potentially affected individuals without delay. The service provider is not required to inform affected individuals if the CNIL establishes that appropriate protective measures have been implemented to render the data unintelligible to unauthorized recipients. However, in the absence of such protective measures, and after considering the likely adverse effects of the breach, the CNIL may send a legal notice to the service provider requiring it to do so.

The content and format of the notification are unclear, since the Ordinance remains silent on the practicalities of such notification.

Therefore, one must refer to the provisions of the e-Privacy Directive, which state that the notification to the subscriber or individual shall at least 1) describe the nature of the personal data breach and the contact points where more information can be obtained, and 2) recommend measures to mitigate the possible adverse effects of the personal data breach.

Additional guidance from the CNIL is also expected. The e-Privacy Directive mentions that the competent national authority may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification must be made. To this day, the CNIL has not yet issued any guidance or instructions regarding data security breach notification.

Companies are nevertheless expected to implement an internal process that will enable them to respond swiftly to security breaches and to comply with the new legal provisions. Companies in the telecom industry are also required to maintain (and make available to the CNIL at all times) an inventory of all data security breaches they have experienced, including a description of each breach, its effect, and any remedial action taken by the company. Non-compliance with these provisions is punishable by up to five years of imprisonment and a €300,000 (U.S.$431,312) fine.

Transposition of Revised e-Privacy Directive across the European Union

The national transposition of the revised e-Privacy Directive is slowly progressing.[3]

While the implementation of the e-Privacy Directive under national law is likely to be similar in all EU Member States, the manner and practicalities of providing notice may still differ between Member States. Data security breaches have no borders and are likely to affect personal data of individuals in multiple jurisdictions.

Thus, to make sure that data breaches are reported in a consistent manner across the European Union, the European Commission in July 2011 launched a public consultation with a view to determine whether technical implementing measures are required to ensure harmonized national measures on personal data breach notifications and the form they should take (*see WDPR, August 2011, page 23*). The deadline for this consultation is September 9, 2011. Following this consultation, the Commission may propose "technical implementing measures" and practical rules (*e.g.*, the circumstances, formats, and procedures) to complement the existing legislation.

In the meantime, companies in the telecom sector may consider that the time is appropriate to assess their compliance with the e-Privacy Directive and to begin implementing adequate internal processes in order to comply with the law.

NOTES

[1] See Hunton & Williams' Privacy and Security Blog at http://www.huntonprivacyblog.com/2010/10/articles/european-union-1/french-dpa-releases-new-guidance-on-personal-data-security/.

[2] See Olivier Proust, "French Senate Proposes Amendments to the Data Protection Act", BNA's Privacy & Security Law Report, December 21, 2009.

[3] The transposition deadline for the revised e-Privacy Directive was May 25, 2011. As of August 31, 2011, 15 of the 27 EU Member States had transposed the Directive.

The text of France's new law concerning electronic communications, Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques (JORF n° 0197 du 26 août 2011), may be accessed, in French, at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024502658&fastPos=1&fastReqId=746339044&categorieLien=id&oldAction=rechTexte.

Olivier Proust is an Associate with Hunton & Williams, Brussels, and a member of the Paris Bar. He may be contacted at oproust@hunton.com.

   ISSN 1473-3579