Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

Volume 12, Number 7 July 2012

Complying With Data Breach Requirements In France

By Olivier Proust, of Field Fisher Waterhouse LLP, Brussels.

Introduction

Data breach notification requirements are receiving more and more attention in the European Union. Recently, an obligation to notify data breaches was introduced by the revised EU e-Privacy Directive (2002/58/EC),[1] although this obligation is limited to electronic communications providers. As a consequence, more and more EU Member States are adopting voluntary or mandatory breach notification regimes in order to comply with the provisions of the revised e-Privacy Directive.[2]

The European Commission has also proposed in its draft regulation on the processing of personal data (the "Regulation")[3] to introduce a general data breach notification requirement that would apply to all data controllers, regardless of the business sectors in which they operate (*see analysis at WDPR, February 2012, page 4*). Under the proposed Regulation, data controllers would be required to notify the national regulator within 24 hours from discovering a breach, if feasible, and the individuals concerned without undue delay.

In France, the provisions of the e-Privacy Directive regarding data breach notification were implemented by an Ordinance[4] of August 24, 2011, concerning electronic communications (*see analysis by the author at WDPR, September 2011, page 9*).[5] This Ordinance introduces a new provision ("Article 34 *bis*") under the French Data Protection Act of 1978,[6] imposing an obligation on electronic communications service providers to notify any data security breach. This Ordinance was completed by an implementing Decree[7] of March 30, 2012, which specifies the conditions that apply to data breach notifications.[8] On May 28, 2012, the French data protection authority, the Commission nationale de l'informatique et des libertés ("CNIL"), issued guidance[9] on data security breach notification requirements also specifying the measures and practical steps for complying with these new provisions (*see analysis at WDPR, June 2012, page 34*).

In light of these new provisions, the guidance issued by the CNIL, and the upcoming changes under the Regulation, now seems a good time for companies to assess their level of compliance with regard to data breaches and to begin implementing appropriate measures and procedures.

General Data Security Obligations for All Data Controllers

As a general rule, data controllers must comply with the data security requirements under Article 34 of the French Data Protection Act that apply to any data processing activity. Data controllers must 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 unauthorised third parties. Non-compliance with these provisions is punishable by five years of imprisonment and a fine of up to €300,000 (U.S.$368,729).

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 the data processor an obligation to implement adequate security measures when processing personal data on behalf of a data controller.

The CNIL has also released several guidebooks aimed at assisting companies to implement adequate security measures. In October 2010, the CNIL released a first security handbook (*Guide sur la sécurité des données personnelles*),[10] which provides basic recommendations and best practices for all types of data processing activities (*see WDPR, November 2010, page 22*). In 2012, the CNIL published two new security guidebooks aimed at helping companies to implement the appropriate security measures for complex processing activities. The first guidebook provides a methodology for identifying and managing potential risks of processing activities for individuals (*Guide Sécurité avancée: méthode*)[11]; the second handbook comprises a detailed summary of practical measures and best practices aimed at mitigating the identified risks (*Guide Mesures pour traiter les risques sur les libertés et la vie privée*).[12]

In particular, with regard to data security breaches, the CNIL considers that companies should have an operational structure enabling them to detect and mitigate incidents that are likely to affect the privacy rights of data subjects. To this end, organisations should:

- define roles and responsibilities within the organisation and establish internal procedures for dealing with data breaches;
- create an inventory of individuals responsible for handling data breaches;
- develop a response plan for data breaches, which must be regularly updated and tested;
- measure the seriousness of data breaches and categorise them according to their impact on the privacy of individuals;
- respond to data breaches according to their degree of seriousness;
- maintain an inventory of data breaches describing the type of breach, its consequences and remediation measures; and
- analyse how to improve security measures after a data breach has occurred.

Specific Data Breach Notification Obligation for Electronic Communications Service Providers

The provisions regarding data breaches under Article 34 *bis* of the Data Protection Act have a limited scope. They apply only to electronic communications service providers ("service providers"), meaning companies that are registered with the French telecommunications regulator, ARCEP,[13] notably internet service and telephone service providers. They do not apply to "information society" companies such as online banks and e-commerce websites. In other words, the provisions on data breach notification apply only if 1) the processing of personal data 2) is carried out by an electronic communications service provider 3) in the context of its activities as a provider of electronic communications services (*i.e.,* telephone or internet services).

Article 34 *bis* defines a breach as "any destruction, loss, alteration, disclosure or unauthorised access to personal data that is accidental, illicit, malicious in intent or otherwise." According to the CNIL, certain types of "intrusion" would not be classified as a breach under the requirements (*e.g.,* a virus that attacks the computers of subscribers to a particular ISP or a breach affecting the service provider's human resources database). On the other hand, unlawful access to the service provider's customer database, or a breach in the service provider's online store exposing customer bank card details, would qualify as a breach. The CNIL specifies that the new law covers "material" breaches, for example, the loss of a paper contract in a mobile telephone operator's shop (where individuals purchase phones and sign up for the service), as well as electronic breaches, such as unauthorised access to a client database.

Service providers are subject to two types of notification requirements:

- notification to the CNIL, and
- in some cases, notification to the users or subscribers affected by the breach.

Notification to the CNIL

In the event of a breach, service providers must notify the CNIL of the breach without delay. The law does not specify any threshold for notification and, thus, all breaches must be notified to the CNIL to the extent that the breach 1) involves personal data; 2) concerns an electronic communications service provider; and 3) occurs within the context of the provision of services. The CNIL's guidance does not specify what is meant by "without delay," but this notion is usually interpreted by the CNIL to mean "immediately."

Notification to the CNIL must be carried out by sending a letter via registered mail detailing 1) the nature and consequences of the breach; 2) the measures taken or planned to remedy the breach; 3) a contact person who may provide additional information; and 4) if possible, an estimate of the number of individuals affected by the breach. The law does not require this letter to have any particular form, and the CNIL has not issued any spe-

   ISSN 1473-3579

cific model. Therefore, companies are free to use their own models as long as the letter contains the legally required content.

Notification to Individuals

If the breach is likely to affect the personal data and privacy rights of subscribers or other individuals, the service provider must also notify the affected individuals. The law does not explain in more detail when to notify individuals, and it is therefore up to the service provider to analyse the consequences of a breach for the individuals concerned and to assess its seriousness. For example, a breach affecting the service provider's customer database or the customer invoicing details would require informing the individuals.

Notice must be provided to the individuals affected by a breach without delay and by any means available that enable the service provider to preserve evidence that it gave notice. The notification must inform the individuals about: 1) the nature of the breach, 2) the contact person from whom they may request additional information and 3) the measures recommended by the service provider in order to limit the negative impact of the breach. Once again, the law does not require any particular form for this notice. Therefore, notice may be provided by email, postal mail or possibly even by short message service ("SMS").

Notification to the individuals affected by a breach is not required where the service provider has implemented "appropriate protection measures" to the personal data involved in the breach.

Appropriate Protection Measures

Appropriate protection measures are defined by the law as any measures that have been rendered "undecipherable" or "unintelligible" to unauthorised persons and have been applied to the data affected by the breach. Depending on the type of breach and its seriousness, the service provider must assess whether to implement protection measures, bearing in mind that, if it does not notify the individuals concerned, it must then inform the CNIL about the protection measures that it has implemented. The CNIL will then review those protection measures and decide whether they are valid given the circumstances of the breach.

The CNIL states that "all technically effective measures" that serve the purpose of rendering personal data unintelligible can be used, but notes that, if data are encoded or encrypted and the key to the code is also accessed or lost in the course of the breach, the exemption would not apply. In practice, the CNIL recommends that the service provider inform the CNIL about the protection measures being used at the same time it provides notice of the breach.

The information regarding the protection measures must specify:

- the last name, first name, address and telephone details of the data controller;
- a description of the protection measures;
- the measures applied to guarantee the efficiency of those protection measures;
- if applicable, reference to the registration filed with the CNIL prior to implementing the data processing activity in question; and
- whether the individuals concerned have been notified and, if not, the reasons justifying the absence of such notification.

Once the notice is received, the CNIL has two months to analyse and pronounce on the validity of the protection measures in relation to the seriousness of the breach. If the CNIL confirms that the action taken is sufficient, then the service provider is not required to inform the individuals. In case of non-response from the CNIL within two months, the service provider must then notify the affected individuals. After investigating the severity of the breach, if the CNIL considers that the protection measures are insufficient with regard to the seriousness of the breach, it may issue a formal notice requesting that the service provider inform the individuals affected within one month (unless the service provider has already done so).

After a breach has occurred, service providers must maintain and update a register of security incidents, recording information on the breach, its consequences, and the measures taken to remedy the breach. Such register may be kept in paper or electronic format and must be kept available to the CNIL at any time.

Sanctions and Enforcement

The failure to comply with the notification requirements is punishable by imprisonment for up to five years and a maximum fine of up to €300,000 (U.S.$368,729).[14] In case of an investigation, the CNIL may pronounce administrative sanctions, including fines of up to €150,000 (U.S.$184,364) for non-compliance with the general provisions of the Data Protection Act. In this regard, companies could face double sanctions for 1) failing to notify the regulator and/or the individuals concerned, and 2) not implementing appropriate security measures to protect the data against unlawful access or disclosure.

The CNIL announced in its 2012 audit programme that, among other things, it will enforce the new legal requirement for electronic communications operators to report data breaches to affected individuals.[15] However, the CNIL has given little guidance as to how it intends to enforce these measures and whether companies will be given time to comply with the new provisions.

Future Developments within the European Union

At an EU level, several initiatives indicate that the data breach notification requirement could soon be extended across all business sectors. In July 2011, the European Parliament approved a resolution[16] calling for the addition of a "system of mandatory general personal data breach notifications to sectors other than the telecommunications sector," which would extend the notification obligations created in the e-Privacy Directive (*see*

WDPR, July 2011, page 23). More recently, the European Parliament issued a report calling on the Commission to propose an EU framework for the notification of security breaches in critical sectors such as energy, transport, water and food supply, as well as in the information and communications technologies and financial services sectors, to ensure that relevant Member State authorities and users are notified of cyber incidents, attacks or disruptions.[17]

One of the most significant developments for data breaches is the proposal for a Regulation on the processing of personal data that was released by the European Commission at the beginning of 2012. The proposed Regulation would introduce a broad notification requirement for any personal data breach similar to that set out in the amended e-Privacy Directive. Data controllers would be required to notify the local data protection authority of any breach of security without undue delay and no later than 24 hours after the controller became aware of the breach. A delay in notification would be possible, but the controller would have to make a reasoned justification for taking longer than 24 hours to notify. If the breach was likely to adversely affect the protection of an individual's personal data or privacy, the controller would also have to notify each individual concerned. Notification to the individuals would not be required where the organisation could demonstrate that it applied appropriate protection measures to protect the data. Failure to report a breach would be sanctioned by administrative penalties of up to 2 percent of an organisation's annual global turnover.

Before the proposed Regulation becomes EU law, both the European Parliament and the Council of the European Union ("Council") must jointly agree on the final text in the "co-legislation procedure." During the co-decision procedure, the European Parliament and the Council must review the draft Regulation, may propose amendments, and must come to an agreement before passing the legislation. On June 22, 2012, the Council issued a formal note providing a detailed overview of the EU Member States' discussions to date on the proposed Regulation. In particular, the Council noted the broad scope of personal data breaches. The duty to notify breaches was questioned by some Member States that thought this could lead to over-notification, while others supported a broader definition that would cover each and every incident. The Commission clarified that its aim is to have a provision similar as in the e-Privacy Directive. The Parliament is understood to be drafting a first Working Document, and aims to present its Opinion in the summer of 2013.

Practical Steps Towards Compliance

The difficulty for companies to comply with data breach notification requirements is that data breaches have no borders and often affect individuals in multiple jurisdictions. In view of the variety of legal regimes in the European Union and elsewhere, it is advisable that organisations draft an internal incident response plan. When a breach occurs, a response plan serves as a reference guide for best practices in dealing with the breach, as well as how to identify and comply with the relevant legal requirements.

Set out below are the different steps that organisations may follow when creating their own response plans.

Before a Breach Occurs

Companies should take reasonable measures to prevent data breaches. Below are some of the preventive measures that may limit the risk of a breach:

■ Develop an Information Security Policy

Before any breach occurs, the organisation may consider developing a comprehensive information policy. Drafting of the internal information policy should begin with identifying what types of breaches may occur. The definition of a breach incident should be as broad as possible and should encompass any situation in which the confidentiality of internal information may have been compromised (*e.g.*, disclosed to, accepted by, or acquired by someone who is not authorised to access or receive the information) or is at risk of being compromised. The policy should also identify the types of data that may be lost (*e.g.*, identification data, financial data, health data, sensitive data, *etc.*) and the categories of individuals who may be affected (*e.g.*, customers, employees, *etc.*).

■ Identify Possible Risks

There are numerous risks of a breach that each organisation should identify. This will usually depend on the field of operation. The types of risks to consider when evaluating and implementing security measures may include:

- collection of information over the internet;
- access to sensitive files by employees and independent contractors;
- use of security controls by employees;
- transmission, storage, and disposal of computerised data;
- outsourcing transactions that require transmission of data;
- insufficient physical security of the premises; or
- risk of unauthorised access.

Employees should be trained regarding such risks to ensure security controls and to ensure that all appropriate security measures are in place.

■ Create a Response Team

The next step should involve determining the personnel who will be responsible for dealing with the breach. Such a response team will usually depend on the size of an organisation, but typically it could include: IT security, physical security, legal counsel, human resources, risk and compliance, and management of the affected department. Each member of the team should be as-

   ISSN 1473-3579

signed a concrete task so that, when a breach occurs, each of them knows how to proceed. It may be helpful to draft rules of procedure describing the composition of the response team, their duties and responsibilities and any particular procedures that must be followed.

Ensure Appropriate Communication

Clear information concerning what actions must be taken when a breach occurs can save a lot of time and trouble. Internally, employees should be informed when and to whom they must report a breach, when a breach needs to be reported to management and when an investigation must be initiated. The language of the information should be clear and unambiguous. The methods of communication may vary from the existing methods used to contact employees (*e.g.*, email, information on the website, paper notice, *etc.*).

Organisations should also ensure that service providers are properly informed about the security policies and procedures. To this end, organisations should ensure that agreements with service providers include appropriate security measures and a duty to notify the organisation when a breach occurs on their side.

Dealing with a Data Breach

When an incident occurs, the organisation should be sufficiently prepared to deal with its consequences. The point of reference should be the Response Programme — a document which provides step-by-step guidance regarding the necessary procedures. Compliance with the Response Programme will minimise the risk of any additional negative consequences. A clear and well-written Response Programme can become an indispensible tool for dealing with data breaches effectively and quickly. The different steps of a Response Programme are described in more detail below:

Identify the Incident

The first step should be to identify an incident. The Response Programme should aim at describing the incidents as broadly as possible. Once the incident has been identified, the unit where the incident occurred should issue a report. The response team should then be notified of this incident. Once the response team determines that the event qualifies as an incident, a formal meeting should be convened where a decision on launching an investigation may be taken.

Gather Information

Gathering as much information as possible at the beginning may significantly increase the likelihood of success of the outcome. This should include:

- affected data types;
- affected information systems and sensitivity of data;
- number and identity of affected individuals and their contact details; and
- possible consequences of the breach.

Members of the response team should be tasked with the duty of gathering information, but any other competent personnel may also be useful.

Take Initial Steps

As soon as the breach occurrence is identified, access to data containing personal information should be blocked. The data should also be secured to prevent any additional exposure.

In some jurisdictions it may be necessary to launch an investigation by a third party or to inform the public authorities. If such obligations exist, the organisation should determine who to inform and when.

On the internal level, a thorough investigation should be launched. The Response Programme should be followed in detail and the response team members should execute their duties.

Ensure Proper Notification

One of the most crucial matters related to dealing with data breaches is ensuring that the notification obligations have been met. Organisations should verify which laws impose breach notification requirements and identify any applicable guidance from data protection authorities. Organisations should carefully assess who to notify (*e.g.*, the regulator and/or the individuals), when and how. Organisations should take into account the fact that notification may not be required in all cases, for example, when appropriate technological measures are implemented.

Think about the Future

Companies will benefit from carefully evaluating security incidents and incident responses. This will help them to avoid similar breach occurrences in the future, and will help reduce any potential costs. It will also maintain or improve the reputation of the organisation.

Following a security incident, organisations may find it useful to modify or improve their Response Programme. Remedial measures that are appropriate to prevent recurrence of the incident may be documented and implemented.

Finally, some laws may require records of security breaches to be maintained, including details and effects of breaches, and remedial actions taken. Even if there are no such requirements, it is good practice to document the handling of the breach.

NOTES

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July [2002] OJ L 201/37 amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November [2009] OJ L 337.

[2] The transposition deadline for the revised e-Privacy Directive was May 25, 2011.

[3] Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011 (COD), January 25, 2012.

[4] Ordonnance N° 2011-1012 du 24 août 2011 relative aux communications électroniques.

[5] See World Data Protection Report, "France's New Data Security Breach Notification Requirement For Electronic Communications Service Providers," September 2011, Volume 11, Number 9.

[6] Loi N° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (modifié par l'Ordonnance N° 2011-1012 du 24 août 2012).

[7] Décret N° 2012-436 du 30 mars 2012 portant transposition du nouveau cadre réglementaire européen des communications électroniques.

[8] Note: These conditions were inserted under newly added Articles 91-1 to 91-5 of the Decree N° 2005-1309 of October 20, 2005, implementing the Data Protection Act of January 6, 1978.

[9] See CNIL, "La notification des violations de données à caractère personnel," May 28, 2012, available at: http://www.cnil.fr.

[10] http://www.cnil.fr/dossiers/securite/.

[11] http://www.cnil.fr/la-cnil/actualite/article/article/deux-nouveaux-guides-securite-pour-gerer-les-risques-sur-la-vie-privee/.

[12] http://www.cnil.fr/la-cnil/actualite/article/article/deux-nouveaux-guides-securite-pour-gerer-les-risques-sur-la-vie-privee/.

[13] Autorité de Régulation des Communications Electroniques et des Postes (ARCEP).

[14] Article 226-17-1, Criminal Code.

[15] See CNIL, "Quel programme des contrôles pour 2012," April 19, 2012, available at: http://www.cnil.fr/la-cnil/actualite/article/article/quel-programme-des-controles-pour-2012/.

[16] See Comprehensive approach on personal data protection in the European Union, July 6, 2011, 2011/2025 (INI), available at: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2011/2025(INI)#documentGateway.

[17] See Report on critical information infrastructure protection — achievements and next steps: towards global cyber-security (2011/2284 (INI)), May 16, 2012, Committee on Industry, Research and Energy, available at: http://www.europarl.europa.eu/committees/en/itre/reports.html.

Olivier Proust is Of Counsel at Field Fisher Waterhouse LLP, Brussels, and a member of the Paris Bar. He may be contacted at olivier.proust@ffw.com.

  WDPR ISSN 1473-3579