BNA, INC.

# PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT



**France**

**Breach Notification**

Despite numerous data breaches, the French government has not announced new data security breach notification legislation. However, it is expected that such a legal framework will be enacted in order to implement the forthcoming amended ePrivacy Directive after its adoption by the European Parliament and the Council, writes Olivier Proust of Hunton & Williams LLP. In the meantime, Proust offers preventive measures that may help data controllers reduce the risk of a data security breach and its potential negative impact on a company, and says it may be advisable to notify affected individuals in the case of a breach after notifying the French data protection authority, the CNIL.

## Notification of Data Security Breaches in France

BY OLIVIER PROUST

In recent months, several data security breaches have occurred in various European countries, which has raised general awareness about personal data security in Europe. Currently, there is no harmonized legal framework for data security breach notification among the twenty-seven Member States of the European Union. This may change soon with the forthcoming amendment of EU Directive 2002/58[1] concerning the processing of personal data and the protection of privacy in the electronic communications sector. This directive, more commonly referred to as the ''ePrivacy Directive,'' is one of the five directives forming the ''telecom package,'' which is currently being amended by

*Olivier Proust, of Hunton & Williams LLP in Brussels, is a member of the Paris Bar. He can be reached at oproust@hunton.com.*

[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 (Directive on privacy and electronic communications).

 ISSN 1538-3423

the European Parliament and the Council of Ministers. The amended proposal for the ePrivacy Directive[2] imposes on providers of publicly available communication services the obligation to notify subscribers and the national data protection authority or the competent regulatory authority of a personal data breach.[3] Final approval of the amendments is expected in the course of 2009.

In France, security breaches are progressively reaching public attention, as illustrated by a recent security breach of the Web platform of the Paris public transportation system (RATP). In 2006, a user noticed that he could easily access the personal data of thousands of online subscribers when typing any subscriber's identification number in the online registration form. Following this incident, the RATP decided to shut down access to the platform. Recently, the French Internet service provider Orange had to shut down access to the Web pages on its website relating to online orders after noticing that the personal data of 400,000 subscribers could easily be accessed simply by changing the last numbers of an URL address. Such incidents raise the question of whether data controllers should notify the individuals affected or the governmental authorities of the breach, and what other action should be undertaken when a breach occurs in France.

## The data controller's security obligations

Under Article 34 of the French Data Protection Act,[4] data controllers must take all necessary measures with regard to the nature of the data and the risks of the processing, to preserve the security of the data. 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 ($382,964) fine.[5]

These security obligations equally apply to data processors, who must offer adequate guarantees to ensure the implementation of the security and confidentiality measures.[6] However, a data processor may process the data only upon the data controller's instructions. The data controller is not exempted from verifying that the security measures are properly implemented. Therefore, the security and confidentiality measures implemented by the data processor must be clearly stated in an agreement between the data controller and the data processor.

Currently, under French legislation, there is no explicit legal obligation for data controllers to disclose data security breaches to individuals or to governmental authorities. Nevertheless, according to Alex Türk, chairman of the French Data Protection Authority (CNIL)[7] and of the Working Party 29, ''the level of protection of data cannot be deemed satisfactory as revealed by the investigations carried out regularly by the CNIL in the field''.[8]

Since the early '80s, the CNIL has recommended that data controllers implement general security measures that are necessary to resist accidental or willful[9] breaches of security prior to carrying out data processing.[10] These security measures must be adapted to the purpose of the data processing, the amount of data processed, and the risk of a data breach.

In this respect, the CNIL recommends that the following measures be taken to secure the processing of personal data:

- systematically assessing the risks and analyzing the security measures prior to any new data processing;
- drafting a security and confidentiality policy, updating the security measures and applying them continuously;
- defining the liabilities of the persons who participate in the enforcement of the security measures.

Non-compliance with the above-mentioned obligations and recommendations can prompt the CNIL to carry out an investigation, which may ultimately result in administrative or criminal sanctions.

## The investigatory powers of the CNIL

Following amendments to the French Data Protection Act in 2004,[11] the powers of the CNIL were reinforced to ensure that the processing of personal data is carried out in compliance with the provisions of the Data Protection Act.[12] In this respect, the CNIL can carry out an investigation on the premises of the data controller, examine any equipment used for the data processing, and access the electronic data processing programs and the data itself.[13] The CNIL can also impose sanctions (warning, fine, order to stop processing, withdrawal of an authorization)[14] if it considers that the data processing does not comply with the French Data Protection Act. The CNIL can decide to publish the warnings that it issues. It can also, in case of bad faith on the part of the data controller, order the publication of any sanctions imposed in any publication, newspaper or other media of its choice.[15]

Recently, the CNIL toughened its control over data controllers and decided on some occasions to announce publicly the sanctions imposed in case of a serious se-

[2] More information on the legislative proposals is available at: http://ec.europa.eu/information_society/policy/ecomm/library/proposals/index_en.htm

[3] Article 2(i) of the amended proposal for Directive 2002/58/EC defines a personal data breach as ''a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data, transmitted, stored or otherwise processed in connection with the provision of publicly available electronic communications services in the Community''.

[4] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[5] See Article 226-17 of the French Criminal Code.

[6] See Article 35 of the French Data Protection Act.

[7] Commission Nationale de l'Informatique et des Libertés.

[8] See ''C'est arrivé près de chez nous. . .!'', press release by the CNIL of 26 September 2008, available in French at: http://www.cnil.fr/index.php?id=2525http://www.cnil.fr/index.php?id=2525

[9] The CNIL defines willful breaches as those that are aimed at totally or partially destroying the data controller's equipment, or that have the purpose to divert, alter or destroy information.

[10] Délibération n°81-94 du 21 juillet 1981 portant adoption d'une recommandation relative aux mesures générales de sécurité des systèmes d'information.

[11] The French Data Protection Act of 1978 was amended by the Act of 6 August 2004, which implements Directive n°95/46/CE of 24 October 1995.

[12] See Article 11 of the French Data Protection Act.

[13] See Article 44 of the French Data Protection Act.

[14] See Article 45 of the French Data Protection Act.

[15] See Article 46 of the French Data Protection Act.

  PVLR ISSN 1538-3423

curity breach. For example, on 21 September 2006,[16] the CNIL issued a warning against Free SAS (a French Internet service provider) for disclosing the contact details of 120,000 ex-directory subscribers to telephone directories and directory enquiry service providers. Following numerous complaints from the subscribers, the CNIL carried out an investigation, which revealed that the disclosure of the confidential data was due to an error in the computer software used to transfer the data. The CNIL considered that Free SAS had breached its obligation under Article 34 of the French Data Protection Act, and ordered the company to take all organizational and technical measures necessary to avoid this type of security incident in the future. The CNIL also issued a public warning against Free SAS on the grounds that the breach was a particular threat to the privacy of the ex-directory subscribers.

On May 20, 2008,[17] the CNIL issued a public warning against a French website (''http://www.entreparticuliers.com/'') specialized in connecting real estate owners with real estate agents and potential buyers. The CNIL found out that a flaw in the Web platform's security system made it possible for anyone to access the personal page of advertisers, change the content of the advertisements, and access their personal data (name, contact information, bank information, invoices). The CNIL issued a public warning, which was published on its website and on the website of the Official Journal.

In a similar case that occurred in February 2008,[18] the CNIL found out that customer data (i.e., purchasing orders, transaction data, etc.) could easily be accessed via a merchant's Web platform specialized in the sale of furniture. In response to the data controller's bad faith and lack of cooperation, the CNIL imposed a €5,000 ($6,388) fine and ordered the publication of the sanction in a local newspaper.

## Specific notification requirements

Specific notification requirements apply to particular categories of data controllers. Under article D98-5 of the French Postal and Electronic Communications Code (''CPCE''), telecom operators[19] are required to:

- take adequate measures to ensure the protection, the integrity and the confidentiality of the personal data that they retain and process; and
- take all measures necessary to ensure the security of communications on their networks.

In this respect, telecom operators must comply with any technical requirements that the French Authority for Electronic Communications (ARCEP)[20] may prescribe in connection with security. Telecom operators must also inform their clients of existing services that enable them to reinforce the security of communications. If there is a particular risk of breach of the network security, telecom operators must inform the subscribers of this risk, of any possible measures designed to protect themselves against such a risk, and of the costs of such measures. At present, there is no legal obligation for telecom operators to notify a risk or actual security breach to the public authorities (such as the CNIL or ARCEP).

Under the provisions of the Public Health Code, personal health data collected by health professionals or health institutions for the purposes of preventive medicine, medical diagnosis, and the administration of care and treatment can be stored with a data hosting provider[21] who has received a prior accreditation from the Ministry of Health.[22] In this context, the data hosting provider must demonstrate that he has implemented technical and organizational measures as well as control procedures to ensure the security, protection, preservation and restitution of the health data.[23] The data hosting provider must also enforce a security and confidentiality policy that implements adequate security measures allowing him to monitor any access to data, and to track security breach attempts or unauthorized access to data.[24] This security and confidentiality policy must enable the data hosting provider to report serious incidents, such as the alteration or unauthorized disclosure of personal health data.

## General recommendations

Despite numerous cases of data breach, so far the French government has not announced any new piece of legislation in relation to data security breach notification. However, we can expect such a legal framework to be enacted in order to implement the forthcoming amended ePrivacy Directive after its adoption by the European Parliament and the Council.

In the meantime, the following preventive measures may help data controllers reduce the risk of a data security breach and its potential negative impact on the company:[25]

- implementing state-of-the-art security measures in order to protect personal data and preserve their confidentiality;
- drafting a security and confidentiality policy which states the obligations and responsibilities of the individuals in charge of the data and network security;
- appointing a data protection officer within the organization and registering this appointment with the CNIL;

[16] Délibération n°2006-208 du 21 septembre 2006 prononçant un avertissement à l'encontre de la société Free SAS, available in French at: http://op.bna.com/pl.nsf/r?Open=byul-7q8usm

[17] Délibération n°2008-118 du 20 mai 2008 prononçant un avertissement à l'encontre de la société Entreparticuliers.com, available in French at: http://op.bna.com/pl.nsf/r?Open=byul-7q8uu7

[18] Délibération n°2008-053 du 21 février 2008 prononçant une sanction à l'encontre de la société VPC KHADR, available in French at: http://op.bna.com/pl.nsf/r?Open=byul-7q8uvk

[19] Article L.32-15° of the French Postal and Electronic Communications Code defines an operator as any natural or legal person who runs an electronic communications network that is open to the public or provides an electronic communications service to the public (telecom operators, ISPs, etc.).

[20] Autorité de Régulation des Communications Electroniques et des Postes.

[21] The data hosting provider can be either a natural or a legal person.

[22] See Article L. 1111-8 of the French Public Health Code.

[23] See Article R. 1111-9 of the French Public Health Code.

[24] See Article R. 1111-14 of the French Public Health Code.

[25] These steps are purely indicative and are in no way meant to be comprehensive. In particular, it must be noted that some measures commonly implemented in other countries (such as the U.S.A.) in case of a security breach do not yet exist in France (e.g., providing information to individuals on credit monitoring).

- assessing the seriousness of a data breach as soon as it occurs and reporting it immediately to the data protection officer.

Data controllers may also choose to voluntarily disclose data security breaches to the CNIL so as to avoid investigations and possible sanctions. Although such notification is not legally required, the CNIL values the transparency and cooperation of data controllers with regard to their data processing, and is less likely to launch an investigation on an organization that has voluntarily come forth following a data breach. While there is no particular form for this type of notification, its content may include the following information:

– the nature of the data breach (theft or loss of data, alteration or destruction of data, unauthorized access, etc.);
– the type of personal data concerned;
– the consequences of the data breach;
– the measures being considered to address the data breach.

It may also be advisable to notify the affected individuals of the breach after notifying the CNIL. Again, this is not required under French data protection law but it may be viewed by the CNIL as ''good practice.'' In particular, when a data breach concerns the data of individuals or entities in multiple countries (as is often the case when the security of a database is breached), it can be difficult from the point of view of customer or public relations to notify the breach in one country but not in another one. Any notification of a security breach to individuals in France should be coordinated as much as possible with the notification to individuals in other countries. Ultimately, notifying the data subjects of a data security breach adds trust and transparency to a company's data processing.

  PVLR ISSN 1538-3423