About The Author

Cécile Martin is an Associate in the Labor and Employment Law department of Proskauer's Paris office. Prior to joining Proskauer, Cécile served as in-house counsel for the legal department of the French Data Protection Agency (CNIL). She is a member of the International Labor and Employment Group and the Privacy and Data Security Group.

Cécile has experience with all employment law aspects of corporate restructurings (including transfer of undertakings and due diligence), redundancy procedures, including dismissing protected employees, settlement negotiations, negotiations with employee representative bodies (personnel delegates, works councils, health and safety committees, unions) and French Labor Authorities (Labor Inspector, Ministry of Employment).

Cécile also has extensive experience in data privacy law and is generally responsible for cases involving privacy issues at the crossroads of employment law and the law of new technologies, particularly issues concerning the cyber-surveillance of employees and the dismissal of employees for abusing technologies put at their disposal during their work time.

E-mail: cmartin@proskauer.com

Data Security (France)

Cécile Martin

10 February 2011

The legal requirements

The French Data Protection Act dated 6 January 1978 strictly regulates the protection of personal data. According to Article 34 of the Act, data controllers must take all useful precautions with regards to the nature of the data and the risks to data processing in order to maintain its security and, in particular, to prevent its alteration and damage, or access by unauthorised third parties.

Article 35 of the Act specifies that if the data controller subcontracts the data processing activity, the subcontractor must offer adequate guarantees that it will ensure the implementation of the security and confidentiality requirements mentioned in Article 34. However, such a requirement does not exempt data controllers from their obligation to supervise the subcontractor's compliance with such measures. Consequently, the contract between the subcontractor and the data controller must specify the obligations incumbent upon the subcontractor with respect to the protection of the security and confidentiality of the data, and provide that the subcontractor must only act upon the instruction of the data controller.

Failure to comply with the data security duty can be detrimental to a company, given that pursuant to Article 226-17 of the French Criminal Code, any breach is punishable by up to five years imprisonment and a fine of up to €300,000. Furthermore, the French Data Protection Agency (CNIL) can order the destruction of the personal data processed by the data controller.

The strengthened data security duty

If data controllers are obliged to implement the above steps to guarantee the security of data they process within the EU, they have to be especially cautious if they decide to transfer or outsource data to a country outside of the EU.

According to Article 68 of the Data Protection Act, companies are not entitled to transfer personal data to a country which is not a member of the EU, if that state does not provide a sufficient level of protection of individuals' privacy, liberties and fundamental rights with respect to the actual or potential processing of their personal data. The EU Commission notably considers the security measures adopted by the country when making an assessment of the adequacy of its data protection regulations.

So far, countries identified by the EU as offering an adequate level of protection are limited to Argentina, Canada, Guernsey, Isle of Man, Jersey, Switzerland, Faroe Islands and in some ways, the US - provided that US companies comply with the Safe Harbor Principles.

If the country does not offer an adequate level of protection, the data controller may only transfer personal data outside of the EU through the following ways.

- The data controller can agree to use model contractual clauses in respect of transfers to the non-EU based data controller or subcontractor. In this respect, it is worth noting that the EU Commission recently drafted a set of contractual clauses, which takes into consideration the existence of a

further subcontractor outside the EU. According to the new clauses, a subcontractor who wishes to subcontract personal data must obtain the prior, written agreement of the data exporter. Furthermore, the agreement concluded between the initial subcontractor and the second subcontractor must contain a requirement that the latter comply with the same obligations - notably in terms of security - as the ones which the initial subcontractor is subject to.
- The data controller can use Binding Corporate Rules (BCRs) if the non-EU based data controller or subcontractor belongs to the same group of companies.
- The data controller can apply one of the very restricted exceptions listed under Article 69 of the French Data Protection Act. However the CNIL considers that those exceptions cannot apply to repetitive and massive transfers of data, because they need to be precisely regulated.

Given that French legislation is currently silent on the subcontractor's duty of security, the CNIL is considering the creation of a legal status of subcontractors so that notably they may be held criminal liable if they fail to comply with legal duties of security and confidentiality.

Practical recommendations for securing data

The CNIL recently published guidelines to ensure that companies adopt an appropriate level of security, as required by the French Data Protection Act.

The CNIL recommends in particular:

- Implementing a password policy - according to the CNIL, the password should be unique, difficult to guess, and should remain confidential. It should contain at least eight characters including figures, letters and symbols, and modified frequently, such as every three months.
- Implementing a user account process - the CNIL recommends that companies organise access to workstations through personal users' accounts and track actions made on a file to give a sense of responsibility to the users. The CNIL further recommends that any logs of user data be stored for a maximum of six months. Furthermore, the CNIL considers that to maximise the security of the network, it is necessary to anticipate the issues which could arise from the termination of employment of some employees by implementing a specific process of deletion of the users' accounts when the employees leave the company.
- Securing the workstations - it is recommended that workstations log off automatically after 10 minutes of inactivity, and that companies urge their employees to log off when leaving their office to limit the risks of fraud.
- Identifying who may access the files - the access to personal data should be restricted to employees who have a legitimate interest to access the data. The CNIL considers that users should only have access to data, which they need to carry out their duties. This means that access rights should be modified each time employees are transferred to another service of the company so that their access rights match with their new role.
- Checking the confidentiality of the data vis-à-vis third parties - subcontracting agreements should provide for a security and confidentiality duty with respect to personal data they may have access to. If sensitive data is involved, it is preferable that it is encrypted.
- Securing the local network - the CNIL recommends implementing measures to avoid viruses and fraudulent intrusions, and to secure remote access through the internet. As a consequence, the network should be secured against external attacks through firewalls, tunneling and encryption.

- Securing access to the premises - access to rooms where servers are located should be restricted.
- Anticipating the risk of disclosure or loss of data - it is recommended that back-ups in separate premises be implemented. Laptops, USBs and phones should be secured by encryption. Unused computers should be destroyed before being thrown out.
- Increasing users awareness on the security - it is necessary to notify the employees of the security duties in a document which is easily accessible. Companies may consider implementing training sessions for employees with respect to security duties, or to provide them with guidelines regarding risks, which may occur in case of a breach of security, and how to limit them.