Crowell

CLIENT ALERT

Privacy & Data Protection

September 9, 2008

Other sections of this issue:
Privacy & Data Protection | ISP-Liability & Media Law | Contracts & E-Commerce | Electronic Communications & IT

Belgian Privacy Commission's takes a hard stance on direct marketing

The Belgian Privacy Commission (BPC) recently published a non-binding note on the data protection aspects of direct marketing. In this note, the BPC defends a very strict interpretation of the data protection legislation, which is sometimes in contrast with current industry practices.

Introduction
Over the last years, the BPC received many complaints with regard to direct marketing. With its note, which is not binding, the BPC applies analyzes direct marketing in light of the current legal framework and thereby provides a useful checklist. As usual however, the BPC adopts a very strict view which may go beyond the law's requirements.

Legitimacy
One welcomes the BPC accepting that a direct marketer may have a balanced interest to process personal data. This legitimacy ground will be of particular importance when the data subject's prior informed consent has not been obtained or when the data subject is not a client or prospect.

However, the BPC lists many exceptions, some of which are nothing more than the result of a strict interpretation of the legal framework. For example, the BPC states that when personal data are obtained via viral marketing (a technique whereby participants to a campaign are induced to provide the contact details of friends who are then sent advertising messages) or from a trader in personal data, a direct marketer would have to obtain the data subject's consent prior to sending advertising messages.

Data retention
Although the BPC states that personal data must be deleted from a database when the direct marketer did not recently contact the data subject, no specific data retention term is suggested. Rather, the BPC calls for the industry to determine such a term.

Provision of information to the data subject
Pursuant to the Belgian Data Protection Act, certain information must be provided proactively to the data subject. A template for the provision of this information is included in the note.

In addition to the information which must be provided pursuant to the Belgian Data Protection Act, the BPC considers that the source of the personal data must also be provided to the data subject in case the data are not obtained directly from the subject.

Industry initiatives
Various industry initiatives, such as the Belgian Direct Marketing Association's code of conduct and the Robinson-lists (a list of data subjects who have opted out of receiving direct marketing) are discussed in the note. The BPC welcomes such initiatives, but stresses that they cannot override the data protection legislation.

Conclusion
With its note, the BPC wanted to clarify the data protection aspects of direct marketing. However, by adopting a strict view direct marketers are now left with a new question: should one follow the BPC's guidelines?

French Data Protection Authority actively examines employee data processing

The French Data Protection Authority "CNIL," recently announced that it is actively examining the processing of personal data by French employers. CNIL has found that many of these employers are in violation of French privacy legislation. CNIL's findings are very interesting since they contain a list of the most frequently occurring privacy violations. Employers interested in data protection compliance may therefore be interested in this list. CNIL's recent action is also an illustration of the increased enforcement activity of the national data protection authorities throughout Europe. To learn more about the CNIL's findings, click here.

Introduction
The French Data Protection Authority (the *"Commission Nationale de l' Informatique et des Libertés"* or *"CNIL"*) recently announced that it has been actively examining (and will continue to do so) the processing of personal data of employees by French employers. CNIL has found that many employers are in violation of French privacy legislation.

CNIL's findings
CNIL noted that following violations occurred most frequently:

- Providing insufficient or inadequate information to the employees with respect to their rights under applicable data protection laws;
- Weakness of security measures destined to protect the personal data, especially in situations where such personal data are transferred abroad;
- Absence of policies for updating personal data and removing information that has become obsolete;
- Limited use by French employees of whistle-blow systems;

- Lack of knowledge on French legal requirements relating to whistle-blow systems.

With respect to *whistle-blow systems* (which are mandatory for listed companies in the United States under the Sarbanes-Oxley Act), CNIL made two observations.

The first finding is that French workers do not make much use of such systems. In addition, whistle-blow mechanisms that are set up by parent companies headquartered abroad often appear to be incompatible with local practices within French companies, with the French labor legislation and with the traditional ways of resorting to the normal management line to report any malfunctions.

The second finding concerns the poor understanding by employers of the French data protection legislation when implementing whistle-blow systems. In many cases, employers do not notify the existence of their whistle-blow system to CNIL, whereas this is legally required. In addition, when companies do make a notification, they often refer to CNIL's *"Single Authorization No. 4"* (*i.e.* a document of CNIL setting forth the conditions under which whistle-blowing is allowed), even though very few whistle-blow systems currently in place are actually in compliance with this document.

With respect to the *trans-border data flows*, CNIL has noted an important increase of such data flows, especially in large multinational companies. However, this increase has not resulted in an increased attention to applicable data protection rules. This is rather surprising since violations of these rules are punished severely (up to 5 years of prison and penalties amounting up to 300.000 Euro). The violations established in this respect by CNIL include the absence of information to data subjects, unacceptably long data retention periods once the personal data has been transferred, and the absence of prior notifications to CNIL.

Conclusion
CNIL's particular attention towards the processing of HR personal data should incite French employers to make sure that they are compliant with French data protection legislation.

But the importance of CNIL's recent action goes further: it is illustrative of the increased activity of all national data protection authorities in Europe altogether. There is a tendency amongst these authorities towards actively enforcing compliance with data protection law. In doing so, the authorities are not hesitating to impose sanctions.

Employers therefore have a real interest in setting up good data protection practices and adequately notifying their activities to the relevant authorities.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Thomas De Meese
Partner – Brussels
Phone: +32.2.282.1842
Email: tdemeese@crowell.com