REFORM OF DATA PROTECTION NOTIFICATION REQUIREMENTS

Article 29 Working Party
2 October 2003

Introduction

Covington & Burling regularly advises clients on compliance with European privacy legislation, with a particular emphasis on notification requirements, online privacy issues, direct marketing, compliance audits, human resources, and health privacy issues. We have assisted many clients with inter-company data transfers and transborder data flows, as well as with the data protection implications of corporate transactions and business restructurings. In addition, Covington has helped clients to adhere to Member State information security rules.

At the request of the European Commission, we provide herein some suggestions, based on our experience, regarding how to streamline and simplify notification requirements in EU Member States consistent the objective of ensuring a high level of data protection.

Purpose of Notification

Although Article 18 of the EU Data Protection Directive (95/46/EC) requires Member States to establish notification systems, it does not state the purpose notification of data processing operations is meant to serve. Indeed, our experience with clients is that they generally have no idea why notifications are required, and view them as an administrative cost and a burden. While clients recognize the need to protect privacy – whether that of employees or other persons – they do not see how this objective connects with the notification forms they must fill out.

In our view, there are three potential purposes for notifications:

1. Notifications could serve as a source of information for national data protection authorities regarding which companies process personal data, and thus guide enforcement efforts.
2. Notifications could raise awareness among data controllers of the requirements of privacy law.
3. Notifications could be a means to inform data subjects regarding which entities are processing personal data.

As currently structured, however, the notification system fulfils none of these purposes. Currently, there are not many enforcement matters – a result, most likely, of inadequate funding of national data protection authorities. As a result, enforcement matters tend to be drawn from complaints, rather than checking on notified processing operations.

Likewise, our experience is that notification forms do not raise awareness among controllers about data protection requirements. In general, companies seek to complete the administrative filing task quickly, and do not reflect on their broader privacy practices. And, as many notification databases are not online, individuals do not have easy access to the notification information to learn what entities are processing data in their country.

This result, while unfortunate, is not surprising. There are other examples in Community law where the notification process failed to achieve the hoped-for results. Most notably, in the competition field, the notification system had to be abandoned because of its inefficiency.

Problems with the Notification Process

Compliance with notification requirements throughout Europe is frustrating to companies both small and large. Four problems in particular exist:

Lack of consistency among data protection laws. In the EU, countries have different interpretations regarding basic aspects of data protection law that are essential to filing a notification. For example, on the same facts, countries differ regarding whether data are personal and, if so, who is the controller. To take just one example, some countries treat coded clinical trial data as personal data, while others consider it anonymous. And, in a clinical trial, countries differ regarding whether the controller is the pharmaceutical company that drafted the trial protocol, or the physician/investigator who collects the data from the patient. In some countries, the protocol is deemed to define the purposes and means of processing, while in others the physician's duty to the patient means that he or she cannot be a data processor.

Consequently, companies have to go to significant trouble and expense to determine whether they are deemed to process personal data in a particular country and, if so, whether they are a controller that must file a notification – even though, from a business perspective, they are doing the same thing in the different Member States. This analysis can be expensive (tens of thousands of Euro for a sophisticated company with establishments in multiple Member States). In sum, this lack of consistency introduces an element of uncertainty even if a company diligently tries to comply with data protection law.

Different information requirements. Once a company determines that it must file notifications in several Member States, it is confronted with an array of totally different notifications forms that ask for different types of information. Needless to say, this increases the time and expense involved in completing the

forms. As notifications are supposed to serve the same purpose across Europe, it is difficult to understand why the forms ask for different information.

Systems Issues. Once companies have gathered all of the information needed to complete the notification form, they often face systems issues, unless their notifications are limited to the Netherlands and the UK, where have implemented user-friendly systems. For example, Spain allows companies to indicate only one data processor on its notification form, even though a company may use several. In Belgium, the computer program used for notification is designed in such a way that once a notification is filed, one cannot use the program to file a second, as the information for the first appears and cannot be deleted.

Inconsistent exemptions. Exemptions from notification are not harmonized across EU Member States, and those that exist are often too restrictive. For example, in Belgium controllers do not have to notify processing of human resources data unless the company conducts performance evaluations or processes health data. As virtually every company evaluates its employees, and every company is legally obliged to collect some health data (e.g., information about accidents at work), this exemption is useless. In Italy, the data protection code has established a system under which controllers do not have to file notifications unless they processes certain types of data. However, companies must file a notification if they monitor employees' use of electronic communications – again, a common practice.

Possible Reforms

Following the Commission's data protection conference of September 2002, which highlighted several issues with the notification process, companies expect real, practical reforms to simplify and streamline notification. These measures should be aimed at making notification less burdensome and costly, while still fulfilling its purposes.

We believe that two reforms in particular should be pursued. First, exemptions from notification should be made broader, and should reflect common business practices. Data processing of which the data protection authorities and data subjects should be aware – for example, because it is mandated by law or is a general business practice (e.g., processing of employee data) – should not have to be notified, even if sensitive data are involved.

Second, a system of mutual recognition should be established for notifications related to databases used by controllers established in more than one Member State. For example, many controllers may operate one HR database for all of their European operations. Under a mutual recognition system, the company would file a detailed notification in one EU Member State. This notification would identify the relevant entities in other Member States that also act as controllers of the database. As part of this notification, companies should be allowed to indicate a single contact point for data subjects and authorities throughout the relevant

EU countries, as long as it provides an assurance that answers will be provided in the subject's/authority's language.

Under this system, the "lead" data protection authority would inform the other relevant data protection authorities of the notification. This would be accomplished by distribution of a standardized summary sheet completed by the controller. This summary sheet should be a template that can easily be translated, so that it will be available in all of the required languages. To the extent possible, check boxes should be used in preference to free text fields, in order to avoid the need for multiple translations of descriptions. Moreover, these summary sheets could be placed online by data protection authorities to ensure that data subjects are informed about what companies are processing data in their country. In case of complaints or suspected violations of data protection laws, a data protection authority could ask the lead authority for more information on a particular notification, and, if necessary, ask the controller to provide a translation of the detailed notification.

Of course, it would be necessary to determine in which country the detailed notification would be filed. This could be the European headquarters of the company, if it has one. But some companies do not have a head European office, or that office may be located in a country in which there is an applicable exemption from notification. In such cases, companies should be able to designate a particular "lead" subsidiary, in a manner similar to that proposed in the Article 29 Working Party's recent paper on binding corporate rules. Alternatively, if there is a transfer only out of one country, the country out of which this transfer takes place may be the appropriate country to file the detailed notification.