EU plans to harmonise notification rules

Notifying your data processing activities with national regulators is a burdensome task, one that is made demonstrably harder considering the inconsistent approach taken by EU member states. **Laura Linkomies** looks at the efforts being made to simplify the process.

Differences in member states' notification systems are placing a significant burden on data protection managers' workload. Time spent on filling in forms and checking out what is required in each country could be spent more effectively on other aspects of compliance.

Additionally, data protection authorities in many countries are forced to dedicate much of their workforce just for the purpose of administering their notification systems. It is a problem that has recently been acknowledged by the European Commission, and a subgroup of the EU Article 29 Data Protection Working Party has launched an initiative to examine how notification rules could be simplified and harmonised.

A European Commission official explained to *PL&B International*: "Most Data Protection Commissioners are very supportive of this initiative, and we expect a substantial outcome. In order to achieve this, there is no need to amend the [EU] directive itself, but explore the flexibility of the current systems, and possibly amend national laws. Whereas there are some traditional systems as in France and Spain, as opposed to the more flexible ones such as Sweden, for example, there is no preferred country."

Difficulties in creating a harmonised approach to notification can be expected, especially as some national authorities do not even agree on the basic definitions of data protection terminology. However, as the issue has been listed in the European Commission's action programme for 2004, it is hoped that the work will be completed this year. But, if the Working Group does not produce the results, the Commission has indicated it is prepared to take over and carry on the work.

IDENTIFYING THE PROBLEMS

The European Commission has voiced a number of serious concerns about the implementation of the EU Data Protection Directive. Its 2003 report on the status of implementation across the EU included recommendations for simplifying the notification process. The Commission recommends a wider use of the exemptions for notification - for example, organisation that appoint a data protection officer are not required to notify. The Commission's report also calls for the Data Protection Working Party to examine opportunities to facilitate notification, especially for multinational businesses that operate in several different EU countries.

The report, which is based on feedback from business and data protection authorities, states that:

> "many submissions argue for the need to simplify and approximate the requirements in member states as regards the notification of processing operations by data controllers. The Commission shares this view, but recalls that the [EU] directive already offers the member states the possibility to provide for wide exemptions from notification in cases where low risk is involved or when the controller has appointed a data protection official. These exemptions allow for sufficient flexibility while not affecting the level of protection guaranteed. Regrettably, some member states have not availed themselves of these possibilities. However, the

What is data protection notification?

Under the EU Data Protection Directive (see Articles 18-21), organisations are required to register their data processing activities with the privacy regulators in each EU country in which they operate. The categories of information that organisations are required to notify include:

- Name and address of organisation (or its representative).
- Why the data it holds is being used or processed.
- Who the information relates to (eg. customers, employees).
- Who the data is disclosed to.
- Whether the data is transferred outside the EU/EEA.
- A general description of security measures.

Notification registers are generally updated on an annual basis with entries made freely available to the public.

The directive does provide a number of exemptions to the notification process. For example, an organisation which appoints a data protection officer or only processes 'low risk' data is exempt from the notification process.

In cases where data protection authorities consider the use of personal data to be a 'high risk' (for example, where an organisation processes sensitive information such as genetic or other health-related data), they can require organisations to obtain prior authorisation before carrying out the processing activity.

> Commission agrees that, in addition to wider use of the existent exemptions, some further simplification would be useful and should be possible without amending the existing Articles."

Currently, differences between the EU countries' notification systems are significant, especially with regard to prior checking - eg. in cases of high risk data the data protection authority can require prior authorisation - the use of in-house data protection officials, and the categories of information that organisations are required to include in their notification entries.

What organisations are faced with

A study on the implementation of the EU directive by Professor Douwe Korff of London Metropolitan University provides a useful summary on the main differences in EU notification systems. For example, in the case of prior checking, the situation varies from one extreme to another. Whereas in the UK no processing is subject to prior authorisation, in France all public sector processing must be subjected to the data protection authority's approval. Most other countries require prior checking for the processing of sensitive data. However again, the specific details on this are different.

The directive provides for wide exemptions in cases where low risk data is involved, or where the organisation has appointed a internal data protection officer. This is the case in Sweden and Luxembourg, while Germany's data protection law also provides a similar exemption, although it is more limited in its scope. The use of this exemption is to be discussed further at the EU level, as it is recognised that it would allow data protection authorities to devote more of their resources to other tasks.

"In each country, we have a data protection representative who takes care of notification as part of their jobs in IT, human resources or finance."

- David Trower, chief privacy officer, IMS Health

There are also major differences in how manual filing systems are treated. While Denmark, Greece, Italy and Luxembourg require notification of both automated and manual processing operations, some countries extend notification only to some manual systems, while others provide wide exemptions.

There are also differences in publicising the processing operations. Whereas all countries require the details mentioned in the Data Protection Directive (Art 19), some also expect to be informed of additional notifiable particulars. For example, in Austria, data controllers have to define the legal basis for any processing. Denmark requests dates for when the processing starts and finishes, and in Finland, data controllers must inform the authority of the logic behind any fully automated "significant" decisions. The French and German laws, on the other hand, require notification of the retention periods of the data.

Too much effort, very little benefit

Experts question what value notification schemes have in promoting privacy compliance. It is a well-known fact that notification is widely ignored by organisations and according to Korff, many data protection authorities would prefer to spend their resources on more effective compliance measures. There is the view that notification may even have a negative effect on compliance, as companies could easily come to the conclusion that once they have notified, they are complying with the law. However, some data protection authorities regard notification as having an educational role, as it forces companies to examine their data processing operations against their legal obligations.

many data protection authorities would prefer to spend their resources on other measures which could contribute more effectively to compliance.

Managing notification across the EU

IMS Health, an information and analysis provider for the healthcare sector, is a good example of a multinational that processes personal data across many European jurisdictions. "Notification is just one of the issues that is difficult to manage," says David Trower, chief privacy officer at IMS Health. "IMS has operations in all EU countries apart from Denmark and Luxembourg, and we have chosen to deal with notification locally in each country. It would just be too difficult to handle all notifications centrally."

"In each country, we have a data protection representative who takes care of notification as part of their jobs in IT, human resources or finance. There is a company procedure to follow, and if representatives have any queries, they can contact myself, or a local lawyer. The common procedures include ready-prepared forms for assessing compliance needs against the notification rules."

Trower welcomes the intention to harmonise notification rules, but is doubtful about how much common ground can actually be found. He adds that the system IMS has adopted has worked well, but he would prefer notification systems with less bureaucracy. "The notification rules in France, in particular, always seem to cause some concern, as there are very few exemptions in the French rules."

AUTHOR: Laura Linkomies is a contributing editor to *PL&B* newsletters.

FURTHER INFORMATION: For a copy of Professor Douwe Korff's *Study on Implementation of Data Protection Directive*: http://europa.eu.int/comm/internal_market/privacy/studies_en.htm