European security rules lack harmonisation

The varying patchwork of security regulations across Europe is making it difficult for businesses to adopt a standard compliance strategy. Report by **Robert Waixel**.

Speaking at Privacy Laws & Business's Annual conference in July, Christopher Millard, Partner at law firm Linklaters, explained that while the EU Data Protection Directive was intended to implement 'a level playing field' across member states, this goal has only been partially realised.

In particular, the directive's security provisions have been interpreted in a number of different ways throughout the EU. Millard stressed the importance of the security requirements as it is a key issue in today's outsourcing negotiations. The consequences of security incidents are high, with organisations facing business disruption, regulatory enforcement action, financial penalties and, in extreme cases, prison sentences. Security incidents can damage the corporate brand and leave companies susceptible to civil actions.

Security law study

In April 2004, Linklaters conducted a study of EU data protection laws which highlighted the lack of harmonisation between member states' rules on data security.

While Article 17 of the EU directive addresses the security requirements member states must implement, Millard said that in reality the standard position set out by the directive, is not so standard. In fact, Linklaters' study found that only four countries - Denmark, Finland, the Netherlands and the UK - have stuck closely to the directive's language. Other member states, said Millard, "have all gone further and decided they want to have additional security obligations." In some cases, he added, these obligations are "extraordinarily detailed."

Data categories

In Portugal, a specific distinction has been made between the security requirements for sensitive and non-sensitive data. Similarly in Spain, different security measures are required according to the category of data being processed. Three security risk levels (basic, medium and high) have been established, with the high risk level applying to more sensitive information such as medical data.

Staff education

In some member states, companies are obliged to inform staff about their security responsibilities (for example, in Ireland, Spain, Belgium, and Austria). The Italian law goes further by including a specific legal obligation for companies to train their staff on data security. "It is vital, if you want to manage your compliance risk in relation to data security, that you explain to all of your staff the obligations both you and they have," explained Millard.

Security plans

The development of security plans or documentation have become mandatory in Greece, Spain and Italy (see next page). Typically, these plans will involve drafting a 'security roadmap' for the organisation, which, among other issues, may require employees to be informed of their obligations within the organisation.

Access controls

Some countries (Ireland, Austria, Belgium) favour logistical controls such as identifying categories of staff that have authorisation to access data, segmenting data and keeping computer screens hidden from casual visitors.

Others (Italy, Ireland, Norway, Spain, Portugal), require specific technical measures such as password controls (Italy, for example, even specifies the minimum password length and format), and digital authentication.

Transfer Controls

Some counties specify that encryption must be used both when transferring data over public networks and when there is physical delivery of personal data on digital media.

Security reviews

In Spain, security reviews are a requirement for all data that falls under the medium and high security categories. The reviews can be carried out by either internal or external auditors, and should be carried out at least every two years, and perhaps more often.

Conclusions

The variations between member states' security rules, explained Millard, does not provide much help for organisations trying to implement a standard policy for data security. He added that these variations conflict with the purpose of the EU directive, which was promote the single European market by enabling free movement of personal data within EU borders. "These kinds of divergences can result in quite unnecessary barriers being re-erected within the single market," he said.

There are a number of initiatives to develop an international standard for data security, some of which have been examined by the EU Article 29 Data Protection Working Party. If the Working Party does eventually decide to endorse a reasonable standard, concluded Millard, "then in the course of time, it may be possible to achieve a level of harmonsiation that we don't have today."

AUTHOR:

Robert Waixel, Senior Lecturer in Computer Science, Anglia Polytechnic University, UK