Article

complinet

Data security obligations: enforcement by the French, German and UK data protection authorities

Mar 26 2008 Bridget C. Treacy

Bridget Treacy

After recent data breaches, and against a background of persistent rumours of more active enforcement by data protection authorities companies are renewing their focus on compliance with data security obligations. This focus is particularly evident within the financial services sector, given that financial services regulators typically exercise co-extensive jurisdiction with DPAs over data security.

Basic data security requirements

Article 17 of the Data Protection Directive (Directive 95/46/EC) requires the data controller to "implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access". The directive thus requires the data controller to ensure an appropriate level of security relevant to the risk of processing particular data, but the specific measures to be implemented are not prescribed. Instead, the DPAs acknowledge that companies must undertake a risk-based approach to determining what security measures are required, and they adopt differing approaches to the enforcement of these requirements.

France

The French DPA, the CNIL, maintains a significant degree of control over the processing of personal data by requiring companies to seek authorisation for certain aspects of data processing. For example, each new database created by a data controller must be registered with the CNIL. The data controller must provide the CNIL with details of the purpose of the processing and of the categories of people who receive the information processed on the database. The CNIL has received more than 800,000 registrations to date.

The CNIL has the power to impose sanctions, including warnings, injunctions to stop processing which infringes these requirements, and financial sanctions for companies in breach. Further, the French Criminal Code provides that processing personal data without taking all relevant steps to preserve the confidentiality of such information and, in particular to prevent it from being damaged or disclosed, is punishable by a five year term of imprisonment and a fine of € 300,000. During the past year we have seen the CNIL initiate audits and undertake spot checks to verify how companies are processing personal data. This signals a more proactive, but targeted, approach to enforcement.

Germany

The BFDI, the German DPA, comprises 20 different federal and regional supervisory authorities, each of which has a degree of autonomy in establishing local best practice in the area of data protection. Generally, both criminal sanctions and administrative fines can be imposed on a data controller which breaches the

data protection legislation. Each regional supervisory authority acts independently in imposing sanctions and, until recently, the imposition of sanctions in individual cases has often not been widely reported. This position appears to be changing. In December 2007, the German federal DPA issued a press release highlighting two security breaches. One breach concerned customer data found dumped in a waste disposal unit and, in the other incident, employee HR files were found in an abandoned warehouse.

The German Commissioner's stance in publicising these incidents (albeit on an anonymised basis) marked a new practice and can perhaps be seen to echo the approach of the UK DPA in seeking to draw attention to its enforcement activities. Further, Germany's Spanish neighbour has a very active DPA which regularly publishes on its web site details of complaints which are investigated. The Spanish DPA has also imposed large fines in order to encourage compliance, including a fine of €30,001 on a Spanish law firm for misusing its marketing database.

United Kingdom

In the UK the Information Commissioner has begun, proactively, to name and shame companies which have failed to comply with the Data Protection Act, including those which have failed to apply adequate security measures to safeguard data. The UK commissioner has adopted a practice of investigating reported breaches and then negotiating legally binding undertakings from companies, requiring them to admit breach and to undertake to implement specific remedies. Typically these measures include a requirement to submit to audit by the Information Commissioner. These undertakings are then published on the commissioner's web site and accompanied by a press release.

Notably, the British retailer, Marks & Spencer was taken to task in January 2008 for failing to supervise a third party vendor which had downloaded Marks & Spencer's employee data onto a laptop which was then stolen. Data protection laws impose responsibility on controllers for data protection, even where the data is processed by third parties. Having been found to have breached the UK Data Protection Act, Marks & Spencer sought to negotiate a confidentiality provision with the commissioner as part of the agreed undertaking. The commissioner, however, made it clear that confidentiality would not be offered in these circumstances and, in the absence of agreement, unilaterally issued an enforcement notice, requiring Marks & Spencer to take remedial steps. The commissioner also issued a press release.

Financial services industry

For obvious reasons, the financial services sector has long focussed on data security. Data security in this sector is the preserve not just of the data protection authorities, but also the financial services regulators In Germany, the Federal Financial Supervisory Authority provides guidance to regulated companies on data security.

In France, the Autorité des Marchés Financiers regulates France's financial system. It has the power to conduct inspections and investigations, and its Enforcement Committee can impose sanctions and penalties.

In the UK, the Financial Services Authority adopts a "risk-based" approach to regulating the financial services industry, with a particular focus on the need to ensure that a regulated entity takes reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

In 2007 in the UK, the FSA fined the Nationwide Building Society £980,000 for failing to have effective systems and controls to manage its information security risks. The specific incident involved a stolen laptop but the underlying criticism was that the building society had inadequate internal procedures to inform staff what they needed to do in such circumstances. In late 2007, the FSA fined Norwich Union £1,260,000 for poor security in relation to its processing of telephone inquiries. These fines are significant and demonstrate that data security risks must be taken seriously.

Appropriate technical and organisational measures?

So, what does "appropriate technical and organisational security measures" require? Examples include improving IT systems themselves, carrying out privacy impact assessments, and appointing a data protection officer to implement policies. The French government, the Central Information Systems Security Division, has launched a separate web site dedicated to Information Systems Security to provide guidance to businesses. For many companies, the issue is much more fundamental. Many do not really know to what extent personal data are processed within the business, by which business units or for what purpose.

Without such basic information, it is impossible to assess whether existing systems and security measures are "appropriate" from a data protection perspective. Further, there is an increasing focus by regulators (as can be seen from Marks & Spencer's experience at the hands of the UK DPA) on how companies deal with data security requirements when the data is being processed on their behalf by third party vendors and contractors. Many companies are now taking steps to identify and review the terms of these third party contracts, mindful that, in the event of a data breach, the EU DPAs will still look to the controller as the responsible party.

In 2006 Peter Hustinx, the European Data Protection Supervisor, predicted that companies will attract new customers in the future by guaranteeing personal data protection so that "privacy will soon develop into a sales pitch". That position has not yet been reached, but there is growing evidence that data protection, including data security, matters to our clients. It should, therefore, matter to us.

• ***Bridget Treacy*** *is a partner in the Hunton & Williams Global Sourcing and Privacy practices. Tel: +44 (0)20 7220 5731*

This article first appeared on Complinet on www.complinet.com *on March 26 2008. For a free trial of Complinet's services, please contact client support on* client.support@complinet.com *or* +44 (0) 870 042 6400.