NEWSSTAND

Once More Unto the Breach: the UK Data Protection Regime and Action in the Event of a Data Breach

June 2010
Richard Spiller, Theo Godfrey

Any breach of the UK data protection regime can be very damaging to the business and reputation of the organisation concerned. The strength of enforcement of data protection laws and regulation is increasing, and regulated financial services firms and their executives face the threat of significant penalties from two regulators following a breach.

This article looks at the current regime and action that can be taken to minimise the business costs and risk of enforcement action following a data breach. Compliance, and action in the event of a data breach, is of particular significance for UK (re)insurance companies, brokers and Lloyd's managing agents because of the quantities of personal data regarding policyholders that they are likely to manage in the course of their business. For health, life and other types of insurance, personal data may include medical and other types of sensitive data regarding policyholders, in respect of which stricter rules apply and the consequences of a breach may be taken more seriously by regulators.

The UK Data Protection Regime
The Data Protection Act 1998 (DPA), which implemented the EU Data Protection Directive, established a framework of rights and duties designed to safeguard information (personal data) relating to identifiable individuals (data subjects). Under the DPA, any firm that determines the purposes for which and the manner in which any personal data are to be processed (a data controller) must comply with eight data protection principles (DP Principles).

Of particular importance to data controllers, because of the potential consequences of its breach, is the seventh DP Principle, which requires them to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. This also includes ensuring such measures are in place at any third-party processor. Other DP Principles include ensuring that personal data are not excessive in relation to the purposes for which they are processed, keeping personal data accurate and up to date and not retaining personal data for longer than is necessary. The Information Commissioner's Office (ICO) is responsible for ensuring compliance with, and bringing enforcement action for breaches of, the DPA.

Regulated financial services firms, such as banks and insurance companies and brokers, must also comply with the relevant rules prescribed by the Financial Services Authority (FSA). The FSA requires a firm to make appropriate assessments of the risks of financial crime in relation to

the customer data it holds in line with its Principles for Businesses (FSA Principles), in particular, FSA Principle 2 (requiring a firm to conduct its business with due skill, care and diligence) and FSA Principle 3 (requiring a firm to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems). In addition, SYSC 3.2.6R of the FSA Handbook requires firms to take reasonable care to establish and maintain effective systems and controls for countering the risk that the firm might be used to further financial crime.

Enforcement

In the past, the ICO's enforcement powers were limited to issuing enforcement notices requiring the data controller to take specific action or, in the most serious of cases, to refrain from processing personal data, and to imposing fines of up to £5,000. Likely to have been of greater concern to regulated firms were the FSA's enforcement powers, which include private censure, removal of authorisation, withdrawal of approved person status and potentially large fines. In the future, firms will need to pay greater attention to the ICO: from 6 April 2010 it has had a new power to impose fines of up to £500,000 where there has been a serious contravention of the DP Principles and where certain other requirements are met.

Given the overlapping jurisdiction of the ICO and FSA, there is a risk of regulated firms being subject to enforcement proceedings, including fines, by both bodies following a data breach. In reality, the two bodies will likely work together to avoid this and ensure a consistency of approach. In other cases where the roles of the FSA or ICO and another regulator coincide, the relevant regulators have often put in place a memorandum of understanding governing their relationship.

Dealing With Regulators

According to guidance issued by the ICO, if a large number of people are affected by or there are very serious consequences of a breach, the data controller should immediately inform the ICO and seek its advice on appropriate remedial actions. In such circumstances, regulated firms should also notify the FSA. The ICO has warned that organisations may face tougher sanctions if they fail to report security breaches which subsequently come to light. Whilst notifying data subjects is not an absolute legal requirement, the ICO regards it to be best practice where, amongst other factors, it helps such individuals to manage their risk following a breach.

The ICO may refrain from issuing an enforcement notice in view of remedial measures taken by a data controller following a breach and in consideration of undertakings given by a data controller regarding its future data management. Firms giving undertakings will need to ensure that they and their sub-contractors are capable of fully complying with all of the ICO's terms of such undertakings. If necessary and appropriate, adaptations can be sought to the terms.

Most data breach cases handled by the FSA do not result in enforcement notices and fines, suggesting that the FSA will generally utilise other enforcement measures available to it, such as private censure and undertakings from firms. However, the position may be different where a firm has committed prior breaches or received warnings from the FSA.

The HSBC Case

In July 2009, the FSA fined an insurer, insurance broker and actuarial consultancy in the HSBC Group a total of £3.19m for information security failings, including sending unencrypted customer details through the post to third parties, leaving confidential information about customers in unlocked cabinets and not giving staff sufficient training on how to identify and manage risks like identity theft.

According to the FSA, key to the severity of its enforcement action in this case was a failure to respond to earlier breaches, that the breaches occurred following a period of heightened awareness, and an FSA campaign, regarding the risks of financial crime within the financial services sector and that the firms were aware of such risks but failed to act.

To ensure that similarly severe action by regulators is not warranted, firms should ensure that they have robust security policies in place and that, following a data breach, they promptly take appropriate remedial action.

Other Jurisdictions

Consideration must be given to any other jurisdictions in which a breach may have occurred, for example where a number of group companies use the same third-party processor, at which there has been a loss of personal data. In addition, if affected data subjects are located outside the UK, a UK data controller may have to notify regulators in these countries. The requirements relating to notification of regulators and affected data subjects following a data breach vary widely by jurisdiction, including within the EU, notwithstanding the degree of common approach introduced by the EU Data Protection Directive.

Practical Action Following a Data Breach

Measures that can be taken following a breach to minimise the possibility of damage to data subjects and enforcement action by regulatory authorities include:

- communicating promptly with affected data subjects, providing practical guidance on steps for them to take to limit their risk of loss and dealing with their queries in a timely manner, such as by setting up a dedicated hotline for questions;
- implementing technical measures to improve data security and prevent unauthorised access, such as encryption and secure means of physical transfer of media containing personal data;
- adopting written procedures on managing data security and effective risk assessment and compliance monitoring;
- introducing or improving training programmes, such as making data protection training mandatory at staff induction; and
- taking appropriate disciplinary action in respect of employees, and other actions in respect of third-party processors, involved in the breach.

Notification to data subjects and regulators should only be taken following careful consideration as to an organisation's planned response to a breach. It may be appropriate to engage public relations advisers to help reduce the risk of negative publicity.

Business Cost
In addition to any fines levied, a study published in January 2010 by the Ponemon Institute, a US-based organisation which conducts independent research and advises organisations on privacy, data protection and information security, put the average business cost for UK-based companies of a data breach at £1.68 million. This included costs incurred in relation to detecting and reporting breaches, notifying affected data subjects, implementing special measures following a breach, legal costs and, representing the greatest component of such costs, the cost of lost business associated with the diminished trust and confidence of customers. According to the Ponemon study, data breaches involving third-party processors were common and tended to be more costly. Organisations that notified affected data subjects quickly experienced lower costs associated with a breach.

Conclusion
All firms should already have in place appropriate technical measures to ensure data security and prevent unauthorised access, as well as organisational measures, such as effective risk assessment and compliance monitoring, data security training programmes for staff and written procedures on the secure storage and transfer of data. Compliance officers should bear in mind that implementing measures to ensure compliance prior to a data breach will be considerably less costly, hurried and stressful than implementing them after one.

If a data breach does occur, a quick but considered reaction is needed to manage the consequences, including minimising business costs and the risk of enforcement proceedings. Following a breach, the ICO and, for regulated financial services firms, the FSA, will want to see a commitment to improving technical and organisational measures to ensure data security in the future. Enforcement action may be severe should a firm fail to make such improvements and another breach occur.

EAPD have an International Privacy and Data Protection Group – see www.eapdlaw.com.