Article

complinet

Data breach at HMRC: implications for the private sector

Dec 04 2007 Bridget C. Treacy

Bridget Treacy

On November 22, 2007, data protection came of age in the United Kingdom. That was the date on which the UK Government admitted that one of its departments, HM Customs & Revenue, had lost in the post two CDs containing the unencrypted personal details of 25 million UK residents. Unusually, data protection was the favourite topic of conversation, with everyone scrabbling to understand just what the implications of this might be. As the scale of the data breach became apparent, the cavalier attitude of HMRC in failing rather spectacularly to safeguard the personal data of millions came as a shock.

The true facts as to how the data came to be downloaded onto CDs and put into the post will take time to emerge. What is already apparent, however, is that a data breach of this magnitude severely dents the trust placed by individuals in organisations which process their data. That trust will not easily be regained, but the fact that our data supervisor, the Information Commissioner, has minimal power to act does not help to restore confidence. In this article we explore the nature of the data breach and what lessons can be learned by the private sector.

The facts

The facts are still under investigation but in response to a request by the National Audit Office, a junior member of HMRC's staff was apparently instructed to send details of child benefit recipients to the NAO. The details were downloaded onto two CDs, without encryption, and simply sent in the post. This was, apparently, an unremarkable procedure. It has been said that the NAO asked for the fields of data in which it was interested to be stripped out of the database before it was sent, but that HMRC decided it was too expensive to filter out information.

Data protection law

The UK Data Protection Act 1998 permits data to be sent by a data controller to another party for processing, subject to certain safeguards. Key among the safeguards is a requirement for the data to be protected by adequate technical and organisational security. The fact that an entire database could be downloaded onto an unencrypted CD by a junior staff member suggests wholly inadequate organisational security procedures within HMRC. Sending the CDs through the post adds to these failings.

In addition to responsibility for securing the data in its systems, HMRC, as data controller remains accountable at law for the data where it is processed by another party on its behalf. Further, the controller has a responsibility to ensure that when it (or its agent) processes personal data, the processing is "proportionate". Proportionality here means that the data must be relevant and not excessive for the purposes for which they are processed. There is little doubt that there was no need for the entire database to be shared with the NAO.

The data breach

Once the fact of the data loss became apparent, HMRC took the decision to investigate the breach, to try to find the lost CDs and to devise a plan to reassure individuals and contain any damage. The first 24 hours after the discovery of a data loss are crucial in terms of containing the breach, but also to put in place safeguards to minimise the risk of loss and damage to individuals, including identity theft. Unlike the US, there is no formal requirement in the UK to notify the Information Commissioner or affected individuals of the fact of a data breach. Nevertheless, the UK Information Commissioner regards it as best practice to notify a breach to his office, despite the absence of any formal requirement. It may also be good practice to notify individuals, particularly where bank account details have been compromised, to urge them to be vigilant in monitoring unauthorised activity on their accounts.

Enforcement

A key fact highlighted by this data breach incident is that the Information Commissioner has severely limited powers to take enforcement action following a breach of the DPA. He has a power to prosecute in limited circumstances, but there is an exemption from prosecution for a government department which breaches the DPA. There is no power to fine. The commissioner's power to conduct spot checks or audits on data controllers is subject to the controller consenting in advance. In light of the HMRC breach, the Prime Minister has agreed that the commissioner can audit data processing within government departments at will. A change in the law will be required before this is extended to the private sector but an extension to the commissioner's powers in this respect is now very likely. The CNIL, the French data protection regulator, has recently begun to use more actively its right to audit and to conduct spot checks on companies.

Longer-term impact

Data protection is a cultural value which depends on trust. If individuals do not trust a controller to safeguard their data, they are unlikely to hand it over for processing. Trust has certainly been lost by HMRC and this is threatening other government projects involving the processing of personal data, namely the ID cards scheme, the children's data base and the NHS records management project. Research published this month by the Information Commissioner before the HMRC breach suggests that 60 per cent of us feel that we have lost control over who processes our data, and that data protection is high on the list of concerns people have in the UK.

After the HMRC breach, we can expect to see the government move to restore trust, possibly by halting or at least delaying their other data projects, and also by granting additional enforcement powers to the regulator. The impact of all of this is that individuals, namely our clients, are now much more aware of data protection. They will demand better data protection practices from all of us. Those businesses which are already complaint will have a distinct advantage.

This article does not provide a complete statement of the law. It is intended merely to highlight issues which may be of general interest and does not constitute legal advice.

• ***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 December 04 2008. For a free trial of Complinet's services, please contact client support on* client.support@complinet.com *or* +44 (0) 870 042 6400.