

Data protection in government: a sensitive subject

15 June 2011

Martin Gibson, Data Protection Officer at Buckinghamshire County Council, looks at the need for new approaches to data security arising from recent advances



The Information Commissioner has begun to use the powers granted to him in the Criminal Justice and Immigration Act 2008 that came into force in April 2010. This allows the commissioner to impose fines of up to £500,000 for breaches of the Data Protection Act by organisations or data controllers. The first fines were a while coming and in November 2010 he fined Hertfordshire County Council £100,000 and an employment company named AE4 £60,000 for data protection breaches. In February of this year, the commissioner fined London Boroughs of Ealing and Hounslow £80,000 and £70,000 respectively.

In the case of three of the fines, those related to the loss of unencrypted laptops, and in the case of Hertfordshire, the fine was in relation to sensitive personal data being sent to the wrong addresses via fax, on two separate occasions. A glance down the list of undertakings on the commissioner's website, signed by the chief executives of offending authorities whose data breaches didn't warrant a monetary fine, indicates that apart from unencrypted laptops, unencrypted memory sticks are another high security risk.

The rise of mobile working and the accompanying rise in the use of mobile devices have increased the danger of the unauthorised disclosure of personal data. There is a tendency amongst users to treat private and work mobile devices in a similar, insecure way. Accessing work data via smart phones has an obvious business advantage but when the data controller insists on encryption and passwords, this can meet resistance from the users. The data controller decides how personal data will be processed either in-house or outsourced.

Typically, this will be the organisation that remains legally responsible for the data. The data controller can appoint a processor to process the data on their behalf, but will remain legally answerable for any data loss.

For this reason alone, the first flush of the commissioner's fines in November 2010 has been a useful tool to remind users of the dangers of losing data.

The implementation of secure laptops, smart phones and memory sticks comes at a cost, but for the first time public authorities have a figure to compare the cost of implementation against the cost to the authority of unauthorised disclosure of data. The effect of fines has been to accelerate the move towards greater security for personal data. For most public authorities, the way forward for enhanced security is via the tried and tested methods of greater awareness of the value of the data users process through training and increased security of electronic devices.

But, in an age of budget savings, training budgets are being cut and the drive to rationalise purchasing of expensive equipment is leading to the consideration of more economic solutions. Can these economic solutions deliver the required security? So far it is too early to tell but there are a number of initiatives being considered by Buckinghamshire County Council.

Training

We are moving towards the introduction of self-service through e-learning. In this way, users choose to learn about new technologies or courses by taking online sessions on various subjects.

There are obvious advantages with e-learning packages as users can choose when and what training modules they take. The public authority can make savings in personnel through the use of e-learning, and an electronic record can be kept on progress. It can also be made compulsory for staff to complete.

However, taking a course online is more impersonal and the interaction between pupil and teacher is missing. The delivery has got to be standard for all users. Different user requirements, such as social care and education, cannot be easily accommodated. The take up of non-compulsory courses can be low without managerial support.

Technological solutions

The nature of personal information held by public authorities and especially by local authorities is often very sensitive and high levels of security are required to avoid huge fines being levied by the Information Commissioner. This requires investment and expertise in areas such as encryption of data and security. Increasingly an organisation's most precious asset, their data will be processed in locations other than the local office. The time in which data is processed will also change as work flexibility moves out of the 9 to 5 timeframe.

The acceptable balance between usability and security will continue to be pushed by the requirement to save money by authorities on the one hand, and, on the other hand, the need to maintain robust security to protect clients and comply with our legal requirements. Many users are familiar with the use of mobile working and social networking. There is a danger that the freedom users apply to their social mobile habits will translate to their use of the organisation's data, and this needs to be addressed through training and explaining the consequences of such use.

Outsourcing and The Cloud

The future promises to be challenging. Already the concept of who owns the data – the classic data controller and data processor relationship – is being eroded with initiatives such as data sharing with other public authorities, and the device of legitimising processing through the issue of 'privacy' notices, where data collected for one purpose will increasingly be used to justify processing that data in other areas and for other purposes.

As more services become outsourced and 'back office' activity becomes more streamlined through merged resources, data ownership and ensuring compliance with the requirements of the law will become more difficult. The work may be given to other organisations but the responsibility for the data will remain with the data controller. With all this in mind, implementing the 'Big Society' agenda will be difficult where the responsibility for the data remains with the public authority.

The increasing use of cloud computing as a driver to cut costs will bring benefits and problems. To obtain the maximum benefit, the location where data will be processed will be dynamic, so it is entirely feasible for data to be processed in the Far East on one day and the in the USA on the following day, or indeed a combination of both. At present, a great deal of the processing plants are situated in the advanced economies, but as the drive to force down costs develops, there will undoubtedly be moves to locate in less advanced and perhaps less stable countries. The old comforting method of processing data in-house and ensuring its security will be a thing of the past. Great care will need to be taken, especially with sensitive personal data, when drawing up contracts for The Cloud. Data controllers will be seeking reassurances about the security and accessibility of their data.

Conclusion

The 1998 Data Protection Act is based on the 1995 EC Directive on data protection. At the time the directive was being drawn up, there was no social networking, mobile phones were not as widely available as they are now and the introduction of broadband was in its infancy. Legislative proposals for a new EC data protection directive are expected later in the year. This will take account of the advances in technology and any threats to privacy arising out of these advances. One thing is certain and that is that those working in the personal information field are in for busy and interesting times.

Article published in Public Service Review: Local Government and the Regions before the Information Commissioner's decision to issue a penalty of £120,000 to [Surrey County Council](#) for repeatedly emailing sensitive information to the wrong recipients