Data Protection and Privacy

Is data loss a risk worth taking..?

Consider the Brighton and Sussex University Hospitals NHS Trust, fined £325,000 following the discovery of highly sensitive personal data belonging to tens of thousands of patients and staff on hard drives sold on an Internet auction site.

Control and protection of personal data has always been important. The protection of personal data in the UK is enforced by the Information Commissioner's Office (ICO) under the Data Protection Act 1998 (DPA).

The DPA protects the privacy and integrity of data held on individuals by businesses and other organisations. If you or your organisation processes personal information about individuals, you have a number of legal obligations and as such may need to review your information security. The review should entail the technical, physical and procedural protection offered to this type of data together with a close look at the personnel you employ to process it.

Relevant Definitions

Personal information means information which relates to a living individual who can be identified from that information.

Sensitive personal information is data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal record.

The **Data Subject** is the person about whom the data relates.

Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on that data. This processing could be IT-based (including CCTV) or structured manual filing.

Subject Access Request is the right of an individual to request a copy of their data under a formal process and payment of a fee.

A **Data Controller** is an organisation or body which uses personal data.

DPA Principles

The DPA comprises 8 Principles as follows:

1. Personal data shall be processed fairly and lawfully.

You must 'notify' the ICO that you are processing personal data. You must inform subjects that you are collecting their data and why. You must obtain individual's consent if you intend to send the data outside of the European Economic Area (EEA)[1]. With regard to CCTV, prominent notices should warn people that their images are being captured. CCTV images will be subject to Subject Access Requests if not overwritten within 40 days of their capture.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Do not collect data just in case it might be useful.

4. Personal data shall be accurate and, where necessary, kept up to date.

Allow individuals the ability to update their data or to have it updated. Ensure that these update requests are followed through.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Develop a retention policy for personal data and ensure it is enforced.

[1] UK, Iceland, Norway, Finland, Sweden, Ireland, Denmark, Germany, Netherlands, Belgium, Luxembourg, Austria, Portugal, Spain, France, Italy, Greece, Liechtenstein, Czech Republic, Estonia, Cyprus, Latvia, Lithuania, Hungary, Malta, Poland, Slovenia, Slovakia, Bulgaria and Romania.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

Ensure any requests from individuals for a copy of their data are responded to promptly and the data is provided within 40 days. You may request a fee of up to £10 for each Subject Access Request. Provide opt-in tick boxes for marketing communications.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Configure firewalls on your network perimeter. Provide access only to specific authorised individuals. Consider 'at rest' and 'in transit' encryption. Consider email protection. Develop a policy for handling personal data and establish regular staff training.

8. Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Notification Under DPA

All organisations should consider notifying the ICO of their requirement to process personal information, although they are first advised to conduct the 'Notification exemptions' self-assessment. Some exemption examples are:

- Data Controllers who only process personal information for staff administration, advertising, marketing and public relations.
- Some not-for-profit organisations.
- If personal data is processed for the prevention and detection of crime as long as a formal procedure is established to ensure collection is 'reasonable'.
- Journalistic exemption. There are certain exemptions relating to the processing of personal data in the media (photographs in newspapers, TV images, etc).
- Legal proceedings.
- Vital interests of the data subject.

Powers of the ICO

Powers of the Information Commissioner, currently Christopher Graham, were increased in 2010 to give his office the right to issue Civil Monetary Penalties (CMP) of up to £500,000 to organisations committing serious breaches of the DPA. He stated at the time that he would '*not hesitate to use these tough new sanctions for the most serious cases where organisations disregard the law.*' At the same time he was also given audit powers of organisations in significant risk of compromising personal data, but which refused to cooperate with the ICO.

In the 2011/12 Annual Report statement on 5th July 2012, which coincided with an imposed CMP fine of £150,000 to a consumer lender company, Mr Graham expressed concern over '*some truly shocking examples, with sensitive personal information, including health records and court documents, being lost or misplaced, causing considerable distress to those concerned.*'

In September 2011 Mr Graham commented, in response to a bank cashier's illegal access of her imprisoned husband's sex attack victim, that '*It beggars belief that – in an age where our personal information is being stored and*

accessed by more organisations than ever – the penalties for seriously abusing the system still do not include the possibility of a prison sentence'.

Mr Graham is actively (perhaps aggressively) seeking '*the need for a comprehensive approach to deterring information theft*'. He believes that '*We must not delay in getting a custodial sentence in place for section 55 offences under the Data Protection Act.*' These calls were echoed in July 2012 by the Home Secretary, and in response, the Home Affairs Committee have recommended that '*the Home Secretary exercise her power under section 77 of the Criminal Justice and Immigration Act 2008 to strengthen the penalties available for offences relating to the unlawful obtaining, disclosure and selling of personal data*'. Although this form of data misuse is undoubtedly not the intention of your organisation, where personal data is accessible to your employees, the head of the organisation, or at least the organisation's reputation, will not escape the wrath of the ICO if an employee chooses to use it for illicit gain.

Also in November of 2012, the ICO issued a warning to the financial sector, based on a CMP of £50,000 issued to Prudential and which did not '*relate to a significant data loss*', but rather to Principle 4 of the DPA: '*Personal data shall be accurate and, where necessary, kept up to date*' – and a mix up of customer account details resulting in an individual's retirement funds being transferred to another individual's bank account. The financial sector was accountable for 15% of all public claims made to the ICO in FY-2011/12.

Government / Public Sector

Of course Government departments and agencies are subject to DPA too. Where information systems are employed in these areas they must be seen to reach specific standards for the protection of information processed by these systems. This scrutiny is known as Accreditation, whereby an impartial 3rd party assessor formally agrees that the security controls in place are adequate to protect the information being processed.

Privacy Impact Assessment

As part of the Accreditation process, departments and agencies are required by law to carry out and submit a Privacy Impact Assessment (PIA). The PIA will highlight the risks to privacy within the system. The purpose of the PIA is to visibly demonstrate that an organisation acts responsibly in relation to privacy, and the ultimate focus is compliance with the DPA.

Freedom of Information Act and other Regulations

The ICO does not only administer the DPA, but also the Freedom of Information Act 2000 (FOIA) and other Regulations including the Privacy and Electronic Communications Regulations 2003 (PECR), the Environmental Information (EI) Regulations 2004, and the INSPIRE Regulations 2009.

FOIA, EI and INSPIRE Regulations give the 'public right of access' to government-processed, publicly-owned information. The Act requires that information be stored and made available to comply with any requests for information. The EI Regulations give you specific rights to obtain environmental information, and the INSPIRE Regulations give you the right to view spatial or geographic information.Requests for personal information, however, are completed through the use of Subject Access Requests through the DPA, not FOIA.

Regency IT Consulting

Regency IT Consulting consultants have the experience and expertise to provide assistance to both public and private sector organisations of all sizes to ensure that you have robust security measures, including technical, physical, procedural and personnel, in place to meet your legal obligations under DPA.

By working closely with your organisation our consultants are able to provide tailored advice to help you to identify current risks and advise you on how to reduce them. This assistance could include submission of a PIA, through to working with you to seek Accreditation or ICO/IEC 27001 Certification. In short, we can support you in taking all reasonable steps to protect the information, including personal, that you process.