

The Data Protection time bomb and how to save money by getting it right

The Data Protection Act 1998 has been around for a number of years now and frankly has probably not been treated as seriously as it should by many organisations; be they commercial, not for profit, private or public sector. Recent research undertaken by the British Standards Institute (BSI) resulted in 1 in 5 organisations admitting that they may have unwittingly committed a breach, not simply by failing to hold personal information securely but by neglect of other legal obligations.

Since 6 April 2010 the risks surrounding the collection, management and use of personal data have increased. From this date the Information Commissioner's Office (ICO), the entity charged with overseeing and enforcing the Act, has the power to fine organisations up to £500,000 for serious contraventions of the Act. The ICO has stated that it will have no hesitation in using these powers. In a world where little is sacrosanct from Government cuts, a revenue raising opportunity like this could prove irresistible!

So, all individuals and organisations who "process" personal information for their own business purposes, relating to such individuals as customers, suppliers or employees, are well advised to take another look at policies and procedures to ensure

they are fully compliant with the Act. Securing information assets should be a top priority for all organisations; no-one can afford the damage to reputation that is caused by loss of personal data. Information security is something that needs to be embraced by the whole organisation; it is not a dry technology subject. In fact it is the business – not IT – that is responsible for the protection of their information.

What do you need to do?

You need to have the correct governance framework in place. This means having a nominated Data Protection Officer and the relevant business policies in place to support the Act. These might include:

- Information Protection Policy
- Information Classification Policy
- Information Security Policy
- Information Retention and Archive Policy
- Starters, Movers and Leavers Policy
- Access Control Policy
- Change Control Policy
- Email Policy
- Internet Access and Usage Policy
- Encryption Policy
- Network Security Policy
- Mobile Computing Policy
- Physical Security Policy

Out of this governance structure there needs to be a clear classification of information eg Confidential, Internal Use Only, Public, etc. An understanding of the lifecycle of information within the organisation including acquisition, storage, retention and disposal is essential.

You should also consider appointing information owners within the business; where possible these should *not* be from IT.

Finally you are required to ensure that all staff are made aware of the Act and are regularly provided with training and awareness on the importance of keeping information secure.

Some typical weak points

- Information security governance and architecture
- Access controls
- Mobile computing
- Information retention and archiving
- Ownership and classification
- Encryption
- Change control
- Legacy systems
- Physical storage
- Website security
- End user computing eg uncontrolled spreadsheets and databases
- Third party management

What should you do now?

- Carry out a gap analysis between the requirements of the Act and your control environment.
- Initiate a remediation plan and implement appropriate action.
- Test to ensure that remedial action has had the desired effect.
- Ensure control governance is maintained.

Why you should do something?

There are clear benefits to taking this Act seriously.

Notwithstanding the fact that compliance with the Act will mean that you will not run the risk of fines from the ICO there are many instances where more disciplined control over information has resulted in more effective processes and reduced storage costs.

Remember this Act applies to physically held information as well as electronic/digital information. It clearly states that personal information must be relevant, adequate and not excessive, be accurate and up-to-date and not retained for any longer than is necessary. In many organisations we typically find data that fails to meet

these pre-requisites and as such immediately puts them in breach of the Act.

A few words from the Information Commissioner

The Information Commissioner Christopher Graham said: "Getting data protection right has never been more important than it is today. As citizens we are increasingly asked to complete transactions online, with the state, banks and other organisations using huge databases to store our details. When things go wrong, a security breach can cause real harm and great distress to thousands of people. The penalties are designed to act as a deterrent and promote compliance with the Data Protection Act."

Observations from Kingston Smith Consulting

It is fair to say that most organisations we have worked with have had some of the policies and controls in place; however, these are generally not comprehensive or enforced. In particular the workforce is generally unaware of their obligations under the Act.

The process of getting to a compliant state does not need to be onerous, but the driver must come

from the top of the organisation. We work with the client to help them achieve compliance.

There is an upside, over and above complying with the Act. In most organisations we have found that information storage (either electronic or in hard copy) is excessive and has the potential to breach the Act. In many cases becoming compliant has enabled significant savings.

We **deliver solutions**, defining and agreeing the outcome you require and charging a fee which achieves that end, so that you will always understand the cost and benefit of our services.

We focus on achieving **return on investment**; we measure our success on the value you realise – this means solutions delivered to your specific needs and not someone else's template.

We **bring expertise** and experience to every engagement; every consultant in our team has a strong record of successful delivery in their field of expertise.

For further information please contact:

Mark Child on 020 7566 3731 or at mchild@kscllp.co.uk.

About Kingston Smith Consulting LLP

Kingston Smith Consulting is the specialist consulting practice associated with the top 20 accountancy firm Kingston Smith LLP. Kingston Smith was originally formed in 1923 and the firm has grown to its current position through organic growth and mergers. Kingston Smith is a member of KS International which is an association of independent accounting firms in over 50 countries around the world.

Kingston Smith Consulting LLP

Devonshire House, 60 Goswell Road, London EC1M 7AD, UK Telephone +44 (0)20 7566 4000 Fax +44 (0)20 7566 4010
info@kscllp.co.uk www.kscllp.co.uk

A list of partners is available for inspection at the above address.

Registered in England and Wales as a Limited Liability Partnership: No OC341786 Registered office: Devonshire House, 60 Goswell Road, London EC1M 7AD