

KSAM Briefing Note

February 2011

DATA PROTECTION ISSUES FOR TRADE ASSOCIATIONS

Contact: Rob Johnson (Operations Director) rjohnson@kingstonsmith.co.uk

Since April 2010 the penalties from failing to have controls surrounding the collection, management and use of personal data have increased. From this date the Information Commissioner's Office (ICO), has the power to fine organisations up to £500,000 for serious contraventions of the Data Protection Act.

In a world where little is sacrosanct from Government cuts, a revenue raising opportunity like this could prove irresistible! So is everyone taking it seriously? The regulators are!!!

In October 2010, the ICO used its new powers to impose data-breach fines for the first time. Hertfordshire County Council was given a penalty of £100,000 for faxing sensitive personal information to the wrong recipients. In another case, A4e were fined £60,000 for losing an unencrypted laptop containing personal information.

As trade associations collecting personal data about living identifiable individuals, such as members, customers, suppliers or employees, you should review your policies and procedures to ensure you are fully compliant with the Act.

How can your organisation prepare?

To get your data security into shape your organisation should consider the following:

Governance

- Establish a policy for dealing with data protection issues including the appointment of a board member/senior employee to be responsible for ensuring business wide compliance with the Act.
- The right people at the right level of seniority need to be involved.
- A risk assessment of the whole business should be carried out, using outside expert help if necessary.

Training and awareness

- Contracts of employment and staff handbooks should be updated to ensure these contain clear rules regarding the collection, recording and passing on of personal data.
- Make sure that your staff understand the policies and procedures and can work with them. Don't assume that your staff know what they have to do.
- Conduct checks to ensure staff are implementing the procedures in practice.
- Focus on high risk areas.

Controls

- Access rights – generally speaking, too many people have too much access to too much information! All access should be granted on a need-to-know basis.
- Is your website secure? Are there adequate controls in place over staff accessing the organisation's IT systems when working at home?
- Risk-based monitoring of access to relevant data should be considered.
- Portable media including USB devices, CDs and smart phones need good management to mitigate against data security risks.

Disposal of data

- Many organisations are quite good at disposal of hard copy, paper based data records. However, when was the last time you checked the procedures at your outsourced offsite storage facility?
- Are hard drives and computers/laptops securely destroyed before disposal of the hardware?
- Ensure internal procedures exist to securely delete and destroy personal data which is no longer required.

Management of third party suppliers e.g. outsourced payroll

- How does the third party manage and secure your data?
- Who has access to it?
- How is it transferred between the two organisations?
- Don't rely on the contract to absolve you of responsibility in the event of a breach.

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 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 organisation – not IT – that is responsible for the protection of their information.

We can help you ensure that your policies and procedures satisfy the Act's requirements. Contact us if you would like to discuss how we can assist.