

Keeping your trade association legal

The introduction of a myriad of new legislation in 2011 will bring many challenges to your organisation. These changes will impact on the way your trade association is run and will also put your organisation at risk of facing punitive action if it does not comply with the new legislation.

Bribery Act

The new Bribery Act 2010 was due to come into force in April 2011, though the UK Government announced that it is reviewing the Act's likely impact on business and economic growth so detailed guidance will be available in September. However, there is some doubt that the Government review will result in any material change and so all organisations should ensure they have practical procedures in place to comply with the act as soon as possible.

"Corrupt" transactions, defined as "bribery", include the payment in money or in kind that is given or taken in a corrupt relationship. It can also involve "the abuse of entrusted power for private gain", "an inducement to show favour", "the perversion or destruction of integrity in the discharge of public duties by bribery of favour" and "the use or existence of corrupt practices especially in a state or public corporation".

The most controversial provision in the Act is the strict liability obligation placed on businesses for failing to prevent bribery. This means that organisations can be held liable for the actions of employees and agents who offer bribes to obtain a commercial advantage, even if the organisation is oblivious to the fact that this is taking place.

A failure to have anti-bribery processes is "a failure at board level" and the penalties can be severe. The maximum penalty will be ten years' imprisonment and/or a fine.



However the fine is unlimited for a corporate body and can lead to director disqualifications, not being allowed to tender for public contracts and the confiscation of assets.

How can your organisation prepare?

The Act allows for the defence of failure to "prevent a bribe being paid" by way of demonstrating that adequate procedures are in place. However, "adequate procedures" have not been defined in the Act and so it is left to organisations to draft these using the guidance to be published by the Secretary of State early this year.

Any organisation doing business in the UK should start considering now what procedures they must have in place. This should include:

- Communication of the commitment to the prevention of bribery from the most senior level of management.
- Undertaking a comprehensive assessment of the bribery risks faced.
- Monitoring and reviewing the effectiveness and compliance with policies and procedures.

- Updating contracts of employment and staff handbooks to ensure these contain clear rules regarding the giving of gifts or corporate hospitality as well as expenses.
- A comprehensive compliance and ethics training programme to ensure that your staff are better trained to recognise bribery.
- Clear disciplinary procedures and sanctions for employees who breach the rules.

Ultimately, it will be up to the judicial process to determine whether an entity's procedures are both effective and adequate. Producing "adequate procedures" will also take time to create and refine, and implement.

Organisations have a few short months to ensure that their policies to prevent corruption within their organisation meet the strict standards of corporate ethics imposed by the new Bribery Act 2010. Ignorance of the law will not be a defence!

Contact us if you are concerned about the new Bribery Act 2010 and its implications for your organisation.

Data protection

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.

Contact us

More information about Kingston Smith LLP and our services can be found at www.kingstonsmith.co.uk

Kingston Smith LLP
Devonshire House
60 Goswell Road
London EC1M 7AD
T 020 7566 4000

Nick Brooks – City
nbrooks@kingstonsmith.co.uk

Janice Riches – City
jriches@kingstonsmith.co.uk

Ashley Whittaker – Macclesfield
awhittaker@kingstonsmith.co.uk

Gordon Follows – St Albans
gfollows@kingstonsmith.co.uk

Sandra de Lord – City
sdelord@kingstonsmith.co.uk

Offices in Hayes, West End, Romford, St Albans, Redhill, Macclesfield