Anti-bribery law — reconciling the Act with data protection

Bridget Treacy, Partner at Hunton & Williams, explains why the UK's anti-bribery law could mean trouble for data protection compliance

The UK Bribery Act 2010 (the 'Bribery Act') came into force on 1st July 2011. Its wide-ranging provisions and criminal sanctions for breaches have prompted considerable debate and discussion, not least because of initial concerns that corporate hospitality would be caught by its provisions. Organisations should by now have implemented procedures to prevent bribery. However, what some organisations may have overlooked is the need to ensure that their anti-bribery procedures comply with the Data Protection Act 1998 (the 'DPA').

What does the Bribery Act require?

The Bribery Act is broader in scope than the equivalent US legislation, the Foreign Corrupt Practices Act of 1977. It covers both the payment and receipt of bribes, and it extends to acts involving private organisations, even where no foreign official is involved (unlike in the US where a government official must be involved in order for their to be an offence). There is also an offence of failure to prevent bribery under the Bribery Act.

Organisations may have a defence under the Act where they have implemented 'adequate procedures' to prevent bribery by employees, suppliers and associated persons. It is the availability of this defence that has focused the minds of organisations on establishing procedures to prevent bribery.

To assist organisations with preparations for compliance with the Bribery Act, the Ministry of Justice ('MoJ') published guidance that recommends that organisations base their bribery prevention programme around six principles:

- proportionate procedures;
- top level commitment;
- risk assessment;
- due diligence;
- communication of policies and procedures (including training); and
- monitoring and review.

However, the due diligence and monitoring activities recommended by the MoJ have particular data protection implications. Organisations that do not focus on those implications risk either breaching the DPA or finding themselves unable to rely on evidence which has been gathered in breach of the DPA.

Due diligence activities

Principle 4 of the MoJ's guidance encourages organisations to conduct due diligence on persons who will perform services for or on behalf of the organisation. This due diligence may be conducted internally, or by external consultants. It may involve the examination of information from a variety of public sources, and may also involve the commissioning of reports on specific individuals. These diligence activities raise data protection concerns, because an individual may not be aware that they are the subject of such investigations.

To some extent, the data protection issues that arise during due diligence are the same as those that arise in the context of employee background checks. Preferably, individuals will be told about the diligence checks and will be asked to provide their consent. Obtaining consent poses challenges in an employment context where it can be difficult to demonstrate that an employee's consent has been freely given. Works councils may need to be consulted before such diligence procedures are established in the workplace. The need to perform diligence checks on vendors or agents also complicates matters. For example, difficulties would arise where a UK organisation requires a diligence check to be performed on an individual in another jurisdiction that prohibits or restricts the types of search that may be undertaken (the MoJ guidance contains a case study on this, see page 38 of the document which is available for download at www.pdpjournals.com/docs/87979).

In addition, consideration needs to be given to whether the organisation commissioning the background report is a data controller or a data processor in relation to that report. The answer may depend on whether the report is independently commissioned and researched, or whether it is produced from a generic database. If a UK organisation

(Continued on page 14)

(Continued from page 13)

is the controller, it will be responsible for complying with the DPA, including the eight Data Protection Principles. Care will be needed to ensure that the organisation can satisfy the principle of fair and lawful processing (Principle 1), particularly if the diligence (or parts of it) are covert or involve sensitive personal data. In the absence of consent, the Schedule 2 conditions that a UK organisation may seek to rely on in processing the data are 'compliance with law' or the 'legitimate interests' ground.

Where the data are sensitive, for example where prior convictions are involved, the absence of consent may make it difficult to comply with a Schedule 3 condition. These issues currently arise in the context of anti-money laundering checks, many of which are challenging to conduct in compliance with data protection laws.

There is likely to be an increase in the number of organisations that offer background verification and diligence services on an outsourced basis. The challenge for organisations using those services will be to ensure that such checks are conducted appropriately. A key challenge will be to determine, in those cases, which entity is the data controller. Is it the organisation requesting the background check? Or is it the organisation with the extensive databases that conducts the search? The answer may turn on fine distinctions, yet may be crucial, particularly given the sensitivity of some of the data that will be processed. Appropriate contractual safeguards, particularly on liability, will have an important role in managing these risks.

Monitoring and review

The MoJ guidance anticipates that organisations will implement monitoring procedures that cover their global activities. Such monitoring activities may well have data protection implications for staff, but also for third parties. Not only may the monitoring be subject to the UK DPA, but it may also be subject to the laws of other jurisdictions, which are perhaps more stringent than those of the UK.

Generally, covert monitoring is permitted only in the most limited of circumstances in Europe. Any monitoring of employees must be consistent with their employment rights. It is illegal to utilise CCTV to monitor employees in the workplace in a number of European jurisdictions.

'Speak up' or whistleblower hotlines

Compared to many European jurisdictions, the UK has a light-touch approach to whistleblower procedures. Many UK organisations have somewhat informal whistleblower arrangements in place.

In its guidance on the Bribery Act, the MoJ encourages organisations to have a "confidential means for staff and external business contacts to air any suspicions of the use of bribery". European subsidiaries of US regulated companies will be familiar with the whistleblower requirements of the Sarbanes-Oxley Act, and the complexities of establishing compliant hotlines in countries such as France and Germany.

Under the Bribery Act, many more companies will need to set up whistleblower hotlines, and will need to ensure that they take into account the sometimes stringent requirements imposed by other European Member States.

Conclusion

In preparing for the Bribery Act, organisations may not have focused on the data protection implications of their planned due diligence and monitoring activities. As with many aspects of data protection compliance, the DPA will not necessarily act as a bar to data processing activities, but does require that organisations structure these activities thoughtfully.

The need for transparency and proportionality underpins much of what is expected under the DPA. The due diligence and monitoring activities that organisations will conduct as part their Bribery Act compliance are not necessarily prohibited, but the way in which the data processing takes place will be all important.

Bridget Treacy
Hunton & Williams
btreacy@hunton.com

Bridget Treacy is chairing the 11th Annual Data Protection Compliance Conference. The 2 day event will take place in London on 18th and 19th October 2012.

For further information, see www.pdpconferences.com