February 2010

Review

Commercial & Dispute Resolution

A fine time to review your data protection procedures?

From April, a business that breaches the Data Protection Act 1998 (DPA) may be fined up to £500,000. Now is the time for businesses to review the adequacy of their data management procedures.

From April this year the Information Commissioner can fine up to £500,000 for data breaches

THE CURRENT POSITION – A TOOTHLESS TIGER?

The role of the Information Commissioner (IC) has to date been criticised for its weak enforcement powers. Except in limited circumstances (for example, failing to notify processing), the IC currently has no power to fine data controllers for breaches – even flagrant breaches - of DPA principles. The only sanction which has been available to him is to issue an 'enforcement notice' which requires a business not complying with the DPA to take steps to remedy the position.

There has been sustained criticism at EU level about wide variations in the enforcement powers of data protection authorities in different Member States. At the end of last year, the Article 29 Working Party (Europe's advisory body on data protection and privacy) called on the European Commission to change the EU data protection framework to require each Member State to enhance the enforcement powers of their data protection authority. It said that these authorities should be "strong and bold, strategic on intervention and enforcement". It asked particularly that Member States be required to empower their data protection authorities to impose financial sanctions for data breaches.

WHAT IS CHANGING?

From 6 April this year, the IC will be able to impose fines of up to £500,000 for breaches of the data protection principles. A 'monetary penalty notice' (MPN) can be imposed where the breach is:

- serious and likely to cause substantial damage or distress

and the breach was either

- deliberate or

- the data controller knew or ought to have known that there was a risk that the breach would occur and that it would be likely to cause substantial damage or distress but failed to take reasonable steps to prevent it.

A breach is likely to be regarded as 'serious and substantial' where the data concerned is of a particularly sensitive nature, a large number of individuals are affected and there is high likelihood of damage (financially quantifiable loss) or distress (injury to feelings). However, the IC has indicated that he will look at all of the circumstances of the breach to determine whether it is a serious one. In making the decision, he will "aim to reflect the reasonable expectations of individuals and society".

Examples of possible 'serious and substantial' breaches are:

- Medical records containing sensitive personal data are lost following a security breach by a data controller during an office move. An individual suffers worry and anxiety that his sensitive personal data will be made public.
- Following a security breach by a data controller, data is lost and an individual becomes the victim of identity fraud.
- Inaccurate personal data held by an ex-employer is disclosed by way of an employment reference resulting in the loss of a job opportunity for an individual.
- A data controller is warned by its IT department that employees are accessing sensitive personal data but fails to carry out a risk assessment or implement a policy of encrypting all laptops.

WHO DECIDES HOW MUCH THE FINE WILL BE?

The IC sets the level of the fine in each case. He will look at all the circumstances of the breach, including the size and financial resources of the data controller, and impose a "reasonable and proportionate" fine. The fine acts as both a sanction for the breach and deterrence against future breaches. The IC also intends the fines to be substantial enough to send a warning to other organisations of what will happen if they breach the DPA.

MONETARY PENALTY NOTICE PROCEDURE

Before serving a MPN, the IC must carry out an investigation and be satisfied that the breach is 'serious and substantial'. He must then serve a 'notice of intent' on the data controller concerned. This tells the data controller that the IC is considering serving a MPN, provides full details of the alleged breach and specifies the level of the proposed fine. The data controller then has 21 days in which to make representations to the IC. The IC will consider these and, when the 21 days has elapsed, serve a MPN on the data controller if he still considers it appropriate to do so. He can vary the level of the fine from that set out in the notice of intent. The recipient of a MPN may appeal to the First Tier Tribunal seeking a reduction in the level of the fine or the lifting of the MPN altogether.

A data controller has 21 days in which to pay the fine. The fine will be reduced by 20% if paid in full within the 21 day period.

All MPN's will be published on the IC's website meaning that all organisations served with an MPN will be publicly named and shamed.

INFORMATION COMMISSIONER'S GUIDANCE

The IC is more likely to issue a MPN for a serious breach of the DPA where the data controller:

- has not followed codes of practice or guidance issued by the IC and others from time to time on compliance with the DPA (for example, the organisation

- cannot demonstrate compliance with ISO/IEC 27001 standard on information security management);
- has failed to take reasonable steps to prevent the breach by putting basic DPA compliance procedures in place;
- has failed to carry out a DPA risk assessment;
- does not have good corporate governance and/or audit arrangements in place establishing clear lines of responsibility for DPA compliance; or
- does not have in place plans for dealing promptly and effectively with a DPA breach if and when it occurs.

The greater the failures listed above, the higher the fine. The IC will look particularly at the behaviour of senior managers in the organisation concerned from whom a "high standard of behaviour" in relation to DPA matters is expected.

WHAT DOES THIS MEAN FOR MY BUSINESS?

The new powers for the IC will result in DPA going higher up the compliance agenda. For most businesses, this will result in treating DPA with same attention as they do for other compliance activities (whether that be Sarbannes-Oxley, competition law or financial services). For many multi-national businesses, this will be a case more of adjusting training programmes and governance procedures, rather than anything more radical. Businesses operating in mainland Europe are already well-alive to issues of ignoring data protection matters.

For those businesses which have sought to take a particularly "light-touch" approach to the DPA or are US businesses entering the EU market for the first time through the UK, it is time to take note. At the outset, such businesses need to engage with DPA compliance and seek to appoint an internal employee with responsibility for DPA issues with appropriate board support. That person can then look to set practical guidelines for the business. It need not be a burden but it does need to be addressed.

FURTHER INFORMATION

For further information please contact:

Mike Butler
Partner, London
T: +44 (0)20 7655 1239
M: +44 (0) 7973 287504
E: mike.butler@hammonds.com