January 2010

Review

Commercial & Dispute Resolutions

Avoiding the Information Commissioner's New Bite…

THE ICO GETS THE POWER TO FINE UP TO £500,000

It has recently been announced that the Information Commissioner's powers to impose fines on organisations that commit serious breaches of the Data Protection Act 1998 are to come into force on 6 April 2010.

The ICO is to have the power to impose fines of up to £500,000.

Although this does not match the level of the fines recently imposed by the Financial Services Authority (which can amount to £millions), a fine of this level will nevertheless have a significant impact on some organisations.

The good news is that a fine can only be imposed in restricted circumstances: There must have been a serious contravention of the Act which is of the kind which is likely to cause substantial damage or substantial distress.

The breach must have been deliberate or the data controller must either have known or ought to have known that there was a risk that the contravention would occur, and that it would be of a kind that was likely to cause substantial damage or distress. In addition, crucially, there must have been a failure to take reasonable steps to prevent the contravention.

This last factor is crucial, as it means that a significant way to minimise the risk of incurring a fine is to put reasonable measures in place to try to reduce the risk of a serious breach of the Act.

Fines can only be imposed in respect of breaches which occur on or after 6 April 2010, and so now is the time to assess the risks of a serious data protection breach occurring, and to ensure that the right procedures and policies are in place.

Organisations that ensure that reasonable measures are in place, not only reduce the risk of a fine being imposed in the event of a breach, but such measures could also reduce the level of any fine that is imposed in a worst case scenario. The ICO's Guidance specifically states that the ICO will take into account what steps had been taken, if any, to avoid the contravention, when deciding on the level of fine.

The ICO will also take into account what steps, if any, the organisation took after it became aware of the breach. Voluntarily reporting the breach to the ICO and/or taking prompt action to mitigate any damage caused, may reduce the level of fine imposed.

Keeping clear paper trails of all risk assessments carried out and all policies, procedures and practices put in place to try to avoid a contravention of the Act (or deal with it appropriately if it occurs) is vital, so that clear evidence of positive action can be produced if and when required.

Other factors which may be taken into account when deciding on the level of fine include, how serious the breach was, in terms of the nature of the data concerned and the number of individuals actually or potentially affected, whether the breach was a 'one-off' or part of a series of similar breaches and whether the data controller is willing to offer compensation to those affected.

‘A significant way to minimise the risk of incurring a fine is to put reasonable measures in place to try to reduce the risk of a serious breach.’

Only data controllers can be fined, not data processors. A data controller is generally responsible under the Act for breaches which occur as a result of the actions of its processors. However, the Guidance provides that one factor which could mitigate against the imposition of a fine, is that the breach was caused or exacerbated by circumstances outside the control of the data controller, who had done all that they could to prevent the breach. This makes it all the more important for data controllers to ensure that appropriate written contracts are in place with all of its processors and that their compliance with the contract is properly monitored.

When setting the level of a fine, the ICO will aim to eliminate any financial gain or benefit obtained as a result of the breach and will take into account the size and financial resources of the organisation. It will also take into account any proof of genuine financial hardship which is supplied - a fine could be reduced where the data controller made a loss in the previous year.

Before a fine is imposed, the ICO will issue a Notice of Intent setting out the amount of the fine and the reasons for it. There is then a period of time for the organisation to make representations to the ICO regarding the imposition of the fine and/or the amount. We are able to advise clients as to the appropriate content of such representations in the event that they are required.

Any fine which is imposed will be published on the ICO’s website, but the redaction of any confidential or commercially sensitive information can be requested. The organisation will have at least 28 days to pay the fine and if the fine is paid within this time, it will be reduced by 20%.

There is a right of appeal against a fine to the General Regulatory Chamber (First Tier Tribunal).

Finally, a word of warning. An express aim of the power to fine is to act as a deterrent to prevent similar serious breaches in the future. As a result, it is likely that some organisations will be unfortunate enough to be held up as examples to others.

The ICO’s Guidance can be found at www.ico.gov.uk/upload/documents/library/dataprotection/detailedspecialistguides/icoguidancemonetarypenalities.pdf.

For further information, advice or assistance, please contact Francesca Fellowes on DD: 0113 284 7459 or at francesca.fellowes@hammonds.com.

3493/1/10