New powers give the Information Commissioner the right to levy fines of up to £500,000

The Information Commissioner has been granted new statutory powers to issue fines of up to £500,000 to data controllers who commit a serious breach of the Data Protection Act 1998 ("DPA") on or after the 6th of April 2010, when the new powers came into force.

The Information Commissioner, Christopher Graham, commented in a press statement issued January 2010 that the new penalties are designed as a deterrent to promote compliance with the DPA and that "…[he] will not hesitate to use these tough new sanctions for the most serious cases where organisations disregard the law." It is no secret that the Information Commissioner's Office (ICO) has been pushing for tougher sanctions for some time, so all that remains is to 'watch this space' and wait to see which organisation falls foul of the new regime and becomes the first to suffer from the resulting financial repercussions and bad publicity.

The Guidance

The ICO has issued guidance which sets out how the ICO proposes to use its new powers. The guidance makes it clear that the power to issue monetary penalties applies to all data controllers, irrespective of whether they are in the private or the public sector (with the exception of the Crown Estate Commissioners and certain limited bodies set out in section 63 (3) of the DPA including, for example, the Keeper of the Privy Purse). This means that everyone, from Government Departments to charities to large corporations, needs to step up compliance with the DPA. It also seems to indicate that some of the high profile losses of compact discs and lap tops containing personal data which have occurred in the last year or so would have resulted in high profile fines had the new legislative framework been in place.

The ICO has the right to impose a monetary penalty notice where the following 3 elements are satisfied:

1. The data controller has seriously contravened the data protection principles (set out in Schedule 1 of the DPA)

The first point to make is that the monetary penalty will only be applied in the most serious circumstances - for example, where a data controller deliberately or negligently disregards the DPA. However, the guidance makes it clear that a single breach might be sufficient to constitute a serious contravention and gives the example of the failure by a data controller to take adequate security measures, such as the use of encrypted files and devices etc resulting in the loss of a compact disc holding personal data.

2. The breach was likely to cause substantial damage OR substantial distress.

Damage would include any actual loss suffered by an individual and the guidance gives the example of an individual becoming the victim of identity fraud as a result of the loss of financial data. In the alternative, it is sufficient for the individual to have suffered distress - i.e. the individual does not suffer any actual harm but, as a result of the loss of data, the individual suffers worry and anxiety.

3. The breach was either deliberate OR the breach was negligent and the organisation failed to take reasonable steps to prevent it.

A deliberate breach is straightforward and the guidance gives the example of a marketing company which collects personal data supposedly for the purposes of a competition but in fact discloses that data to a tracing database for commercial purposes.

In circumstances where the breach occurred as a result of the organisation's negligence, the ICO will consider whether the data controller was aware, or should have been aware, of a risk that a breach would occur. The guidance goes on to consider the sort of reasonable steps the data controller should have taken. This includes, for example, the data controller having good governance arrangements in place to establish clear lines of responsibility for preventing contraventions. It is worth reading the guidance to take account of the sort of steps the ICO expects organisations to take to ensure that personal data is held in accordance with the data protection principles. This section of the guidance sets out the sort of good housekeeping measures the ICO expects organisations to have in place.

Assessment of the Penalty

The value of the penalty will be assessed on a case by case basis by the ICO. When publishing the guidance, the ICO commented that it would take the organisation's financial resources, sector and size into account when assessing what monetary penalty would be appropriate. It would also take the nature and the effect of the breach into account.

The ICO gives the first indication in the guidance that it fully intends to use the new powers when it says that it will issue further guidance on the value of fines that will be levied once actual cases have presented themselves. The ICO also indicates that it is more likely to issue a monetary penalty where a particular category of breach is prevalent amongst data controllers, in order to set an example.

The guidance goes into more detail about the sort of mitigating and aggravating factors that the ICO will take into account. For example, if a large number of individuals are actually or potentially affected, or if the data controller carried out a deliberate or premeditated breach, a monetary penalty will be more likely. By contrast, a monetary penalty is less likely where the breach was caused by circumstances outside the data controller's control and where the data controller had done all it reasonably could to comply with the DPA.

To access the full guidance, please see the following link:
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf

Best Practice

The key message to take away is that now is a good time to ensure that compliance with the DPA is an integral part of your business operations (if you do not do so already). Don't forget that the ICO will have to regard the way in which an offending organisation has handled its obligations under the DPA when deciding whether or not to levy a fine and the value of the fine itself. Therefore, it is not enough to pay lip service to your obligations under the DPA, and you should be ensuring that you have the processes and policies in place to make sure that your organisation and its staff comply with the DPA when carrying out business.

If your organisation routinely uses third party processors to handle personal information, it is important that not only do you select a reputable company, but that you enter into an appropriate data processing agreement and actively audit and manage the way in which data is handled during the life of the arrangement. This will assist your case in the event that your data processor commits a breach of the DPA which you could not have known about or prevented.

For further information, please contact:

Victoria Ferguson
T: +44 (0)1392 333970
v.ferguson@ashfords.co.uk

Garry Mackay
T: +44 (0)1392 333931
g.mackay@ashfords.co.uk

Ashfords
Solicitors

www.ashfords.co.uk