

Data Protection – Half a million reasons to comply

Fines up to £500,000 for serious data protection law breaches

On 6th April 2010, the Information Commissioner was given new powers to fine data users found guilty of serious contraventions of the Data Protection Principles as laid out in the Data Protection Act 1998. Now serious contraventions could result in fines of up to £500,000.

This change is in response to the number of high profile data security incidents, which made headline news across the UK. Amongst others, the MOD, the CSA and the NHS all ‘misaid’ large amounts of sensitive personal data, leading to a public outcry and calls for heads to roll.

These high profile security breaches highlighted the Information Commissioner’s inadequate powers to punish Data Controllers* who failed to meet the standards. Previously, the Commissioner had extremely limited powers to impose fines, even for very serious breaches of Data Protection law. This was thought to be wrong and so the Data Protection Act was amended to allow fines to be levied for serious breaches of law, up to a maximum amount of £500,000. *A Data Controller is a person who decides why and how any personal data is processed.

These new powers emphasise, that for businesses and organisations, the lawful gathering, use and protection of personal data must form both an integral part of an organisation’s everyday policies and procedures as well as part of its compliance framework. Data protection can no longer to be considered an optional extra with lip service paid to the requirements of the Data Protection Act. And it doesn’t matter what size your organisation is – whether you are a sole trader, a charity or a substantial business – if you process personal data, this law applies to you!

It is expected that the Information Commission will only fine to the maximum £500,000 in the most serious situations and/or where deliberate or negligent breaches of the Principles have taken place.

However lesser fines may be levied for less serious breaches and organisations should use this change to review their own situations, even though the new fines regime is only applied to contraventions occurring after 6th April 2010.

It is vital that you ensure any personal information you hold about clients, customers, contacts and employees is collected, managed and processed in accordance with the Principles of the Data Protection Act.

Continued . . .

.../continued

The Data Protection Principles set out that a Data Controller must ensure that all personal data being held is:

- kept securely;
- processed fairly and lawfully;
- adequate, relevant and not excessive;
- processed in line with the rights of individuals;
- accurate and, where necessary, kept up to date;
- processed for one or more specified and lawful purposes;
- kept no longer than is necessary for the purpose for which it is being used;
- not transferred out side the European Economic Area unless adequately protected.

Where a Data Controller has seriously contravened the Data Protection Principles and, where the contravention was of a kind likely to cause substantial damage or distress, the Commissioner now has enforcement powers to issue a Monetary Penalty Notice.

To attract the maximum penalty of £500,000, the contravention must have been deliberate or where the Data Controller knew, or ought to have known, that there was a risk that contravention would occur and that he or she failed to take reasonable steps to prevent it.

Guidance from the Information Commissioners office makes it clear that the intention is not to impose undue financial hardship on an otherwise responsible Data Controller, where a genuine mistake has been made.

So long as your Data Controller takes appropriate steps in line with the Principles to keep personal data secure, it is not likely that you will be subject to one of these fines. However, more minor contraventions may be subject to other enforcement provisions under the Act.

The Information Commissioner has prepared a detailed guidance note which sets out the full extent of the powers and also the Commissioner's interpretation of what sort of actions will be liable to attract a monetary penalty. The document can be found at

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf

For more information in relation to the Information Commissioner's new powers or your obligations under the Data Protection Act, or advice on how to update your compliance procedures or your everyday processes, policies and procedures, please contact Angus MacLeod at agm@wjm.co.uk.

More information from: Angus MacLeod: agm@wjm.co.uk

The information contained in this newsletter is for general guidance only and represents our understanding of relevant law and practice as April 2010. Wright, Johnston & Mackenzie LLP cannot be held responsible for any action or inaction taken in reliance upon the contents. Specific advice should be taken on any individual matter. Transmissions to or from our email system and calls to or from our offices may be monitored and/or recorded for regulatory purposes. Authorised and regulated by the Financial Services Authority. Registered office: 302 St Vincent Street, Glasgow, G2 5RZ. A limited liability partnership registered in Scotland, number SO 30033

