



Information Commissioner's Office

## Press Release

Date: 12 January 2010

### **Data breaches to incur up to £500,000 penalty**

New powers, designed to deter personal data security breaches, are expected to come into force on 6 April 2010. The Information Commissioner's Office (ICO) will be able to order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act. The ICO has produced [statutory guidance](#) about how it proposes to use this new power, which has been approved by the Secretary of State for Justice, and has been laid before Parliament today.

When serving monetary penalties, the Information Commissioner will carefully consider the circumstances, including the seriousness of the data breach; the likelihood of substantial damage and distress to individuals; whether the breach was deliberate or negligent and what reasonable steps the organisation has taken to prevent breaches.

Information Commissioner, Christopher Graham, said: "Getting data protection right has never been more important than it is today. As citizens, we are increasingly asked to complete transactions online, with the state, banks and other organisations using huge databases to store our personal details. When things go wrong, a security breach can cause real harm and great distress to thousands of people. These penalties are designed to act as a deterrent and to promote compliance with the Data Protection Act. I remain committed to working with voluntary, public and private bodies to help them stick to the rules and comply with the Act. But I will not hesitate to use these tough new sanctions for the most serious cases where organisations disregard the law."

The Information Commissioner will take a pragmatic and proportionate approach to issuing an organisation with a monetary penalty. Factors will be taken into account including an organisation's financial resources, sector, size and the severity of the data breach, to ensure that undue financial hardship is not imposed on an organisation.

The power to impose a monetary penalty notice is designed to deal with serious breaches of the Data Protection Act and is part of the ICO's overall regulatory toolkit which includes the power to serve an enforcement notice and the power to prosecute those involved in the unlawful trade in confidential personal data.

**Box out**

For a data breach to attract a monetary penalty the Information Commissioner must be satisfied that there has been a serious breach that was likely to cause damage or distress and it was either deliberate or negligent and the organisation failed to take reasonable steps to prevent it.

***Example – damage***

Following a security breach by a data controller financial data is lost and an individual becomes the victim of identity fraud.

***Example - distress***

Following a security breach by a data controller medical details are stolen and an individual suffers worry and anxiety that his sensitive personal data will be made public even if his concerns do not materialise.

***Example - deliberate***

A marketing company collects personal data stating it is for the purpose of a competition and then, without consent, knowingly discloses the data to populate a tracing database for commercial purposes without informing the individuals concerned.

The guidance can be downloaded from the ICO website at

[http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/ico\\_guidance\\_monetary\\_penalties.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf)

## ENDS

If you need more information, please contact the ICO press office on 020 7025 7580 or visit the website at: [www.ico.gov.uk](http://www.ico.gov.uk)

### Notes to Editors

1. The amount of the penalty must not exceed £500k. The amounts may vary widely depending on the circumstances of each case.
2. If the Information Commissioner receives full payment of the monetary penalty within 28 calendar days of the notice being served, the Information Commissioner will reduce the penalty by 20%.
3. The money is not kept by the Commissioner but must be paid to the Consolidated Fund owned by HM Treasury.
4. The penalties don't apply to PECR.
5. The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
6. The ICO has specific responsibilities set out in the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003
7. Organisations can now sign the Personal Information Promise to demonstrate their commitment to protecting people's personal information by visiting the website at [www.ico.gov.uk](http://www.ico.gov.uk)
8. For more information about the Information Commissioner's Office subscribe to our e-newsletter at [www.ico.gov.uk](http://www.ico.gov.uk). Alternatively, you can find us on Twitter at [www.twitter.com/ICOnews](https://www.twitter.com/ICOnews)
9. Anyone who processes personal information must comply with eight principles, which make sure that personal information is:
  - Fairly and lawfully processed
  - Processed for limited purposes
  - Adequate, relevant and not excessive
  - Accurate and up to date
  - Not kept for longer than is necessary
  - Processed in line with your rights
  - Secure
  - Not transferred to other countries without adequate protection