



Information Commissioner's Office

Press Release

Date: 27 January 2010

Report data breaches or risk tougher sanctions, warns the ICO

Over 800 data security breaches have been reported to the Information Commissioner's Office (ICO) in just over two years, the privacy watchdog announces today. The ICO is warning that organisations may face tougher sanctions if they fail to report security breaches which subsequently come to light.

David Smith, Deputy Commissioner, said: "In just over two months a further 100 organisations have reported data security breaches to us. We are keen to work with organisations to prevent breaches occurring in the first place and to help put things right when things do go wrong. Talking to us may of course result in regulatory action. However, organisations must act responsibly; those that try to cover up breaches which we subsequently become aware of are likely to face tougher regulatory sanctions."

Mistakes account for 195 of the 818 data security breaches reported to the ICO since November 2007. 262 breaches are the result of theft, often where the personal information was held on an unencrypted portable device. The ICO provides free advice to organisations to help them comply with the Data Protection Act. Organisations can minimise the risks of security breaches involving personal information by ensuring that all portable media devices containing personal information are encrypted. Staff must be adequately trained and organisations should give proper consideration to restricting staff from downloading large volumes of data on to memory sticks and other portable devices. All personal information held within buildings and offices should be protected by adequate security arrangements to prevent theft or the loss of the data. The loss of personal information can cause

harm and distress for individuals, and can lead to reputational damage and loss of customer trust for organisations.

New powers, designed to deter data 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 power to impose a monetary penalty is designed to deal with the most serious personal data breaches 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.

The ICO has produced a plain English [Guide to Data Protection](#) to provide businesses and organisations with practical advice about the Data Protection Act. The guide is intended to help organisations safeguard people's personal details and comply with the law. The guide takes a straight-forward look at the principles of the Data Protection Act and uses practical, business-based examples.

ENDS

A copy of the breach table is available here:

http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/breach_notification_spreadsheet_jan09.pdf

If you would like more information, please contact the ICO press office on 020 7025 7580 or visit the website at: www.ico.gov.uk

Notes to Editors

1. Whitehall departments and many NHS organisations are obliged to inform the ICO when a data breach occurs.
2. The guidance on monetary penalties 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
3. The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
2. 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

4. For more information about the Information Commissioner's Office subscribe to our e-newsletter at www.ico.gov.uk. Alternatively, you can find us on Twitter at www.twitter.com/ICOnews
5. 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