

Press Release

For immediate release

Date: 25 August 2010

DSG Retail customer credit agreements found in skip

Electronics retailer DSG has been found in breach of the Data Protection Act by the Information Commissioner's Office (ICO), following the discovery of customers' credit agreements in or near a skip at one of the company's PC World stores.

The discovery of eight completed credit agreements containing customers' personal and financial data was made by a local authority's environmental health department. The documents related to transactions made two years prior and had been kept beyond the period recommended by DSG's policies for holding personal data. The company's normal procedure for destroying sensitive documents should have meant that they were transported in sealed containers to a central facility for secure shredding, but this did not occur in this instance.

John Browett, Chief Executive of DSG Retail, has signed a [formal undertaking](#) agreeing to take a number of steps to prevent a similar breach happening again. These include conducting a review of security procedures and providing appropriate training for staff on complying with the company's security policies.

Mick Gorrill, Head of Enforcement at the ICO, said: "Any organisation collecting and holding personal information needs to ensure that

information is kept and disposed of safely and securely. This is an important principle of the Act. Making sure data is disposed of securely and not keeping information for longer than is necessary can help to prevent information falling into the wrong hands. Staff need to be aware of policies and it is essential they receive appropriate training to follow them."

A full copy of the Undertaking can be found here:

http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx

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

Notes to Editors

1. The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Fifth and Seventh Data Protection Principles in Part I of Schedule 1 to the Act, and in particular that:

The data controller shall:

- review its security measures and implement such other security and monitoring measures as it deems appropriate to ensure that credit agreements and their associated personal data are protected against unauthorised or unlawful processing, accidental loss, destruction or damage;
 - ensure that its staff who have access to such data are made aware of the data controller's policy and measures for the storage, use, retention and disposal of credit agreements and their associated personal data, and are appropriately trained how to follow these.
2. The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
 3. 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
6. The Data Protection Act (1998) does not cover the acts of interception of communications or 'hacking' of personal information. The interception of communications falls under the Regulation of Investigatory Powers Act (2000) which is regulated by the Interception of Communications Commissioner.
7. The ICO has legal powers to ensure that organisations comply with the requirements of the Data Protection Act. In using its regulatory powers, the ICO considers the nature and severity of the breach which has occurred. Dependent on circumstances, the powers the ICO has at its disposal include:
 - serving information notices requiring organisations to provide the ICO with specified information within a certain time period;
 - serving enforcement notices requiring organisations to take specified steps in order to ensure they comply with the law;
 - issuing monetary penalties of up to £500,000 for serious breaches of the Data Protection Act;
 - conducting audits to assess whether organisations are processing personal data in accordance with good practice;
 - reporting to Parliament on data protection issues of concern;
 - prosecuting those who commit criminal offences under the Act. The ICO prosecutes individuals and organisations for specific breaches of the Act such as the illegal trading of personal data and non-notification.