

Press release

Date: 8 October 2010

Consultation on the first ever UK code of practice on data sharing launched

The Information Commissioner's Office today launched a consultation on a new statutory code of practice on the sharing of personal data. The consultation will run for 12 weeks from today, ending on Wednesday 5 January 2011.

The draft code sets out a model of good practice for public, private and third sector organisations, and covers routine data sharing as well as one-off instances where a decision is made to release data to a third party.

Scenarios where data sharing might occur include a school passing information about a child to a social services department, a group of insurance companies pooling data about people making claims, GPs sending a patient's record to a hospital, or a retailer passing customer details to a debt collection company.

The code covers a number of areas including:

- what factors an organisation must take into account when coming to a decision about whether to share personal data;
- the point at which individuals should be told about their data being shared;
- the security and staff training measures that must be put in place;
- the rights of the individual to access their personal data; and

- when it's not acceptable to share personal data.

Information Commissioner, Christopher Graham said:

"Under the right circumstances and for the right reasons, data sharing across and between organisations can play a crucial role in providing a better, more efficient service to customers in a range of sectors – both public and private. But citizens' and consumers' rights under the Data Protection Act must be respected.

"Organisations that don't understand what can and cannot be done legally are as likely to disadvantage their clients through excessive caution as they are by carelessness. But when things go wrong this can cause serious harm. We want citizens and consumers to be able to benefit from the responsible sharing of information, confident that their personal data is being handled responsibly and securely.

"I would encourage all organisations who handle personal data to engage with the issue and offer their comments and suggestions on the draft code we've issued today. Only then can we make sure we've got a robust and adaptable code of practice that can be applied across the board."

If you need more information, please contact the ICO press office on 020 7025 7580 or visit the website at:

http://www.ico.gov.uk/about_us/consultations/our_consultations.aspx

ENDS

Notes to editors

1. The consultation on the code of practice on data sharing is available on the ICO website.

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.