



Information Commissioner's Office

Press Release

12 February 2010

ICO launches new consultation on auditing notices

The Information Commissioner's Office (ICO) has launched a [consultation](#) on a new draft code of practice which sets out the privacy watchdog's proposed approach to using its new auditing powers due to come into effect in April 2010.

The ICO will take a proportionate and risk-based approach to auditing, based on a range of intelligence including complaints received, business and media reports and annual statements issued by the organisation. The auditing process allows the ICO to assess whether organisations are processing personal information in line with the Data Protection Act (DPA) and to advise on best practice. The ICO will continue to request consent for an audit to be carried out where it is identified that personal information may be at risk.

However, where an organisation refuses to work with the auditing team, but is considered as being at significant risk of compromising personal data, the ICO will be able to serve an Assessment Notice - a compulsory audit notice. Initially the ICO will only be able to conduct these compulsory audits on central government departments. It will though be able to make a case to the Government for the power of compulsion to be available more widely. The draft code of practice has been designed to provide advice on the ICO's auditing framework to all public and private sector organisations and will be relevant whether an audit is to be carried out by consent or with compulsion.

David Smith, Deputy Commissioner at the ICO, said: "Auditing plays a key role in educating and assisting organisations to meet their obligations under the Data Protection Act. We will work with organisations that want to get it right and are keen to follow best practice. However, those government departments less willing to work

with us will face an Assessment Notice if there is evidence to suggest they are putting personal information at risk. Whilst our auditing powers are restricted to central government departments initially, we will, where we can make a good case, seek to extend our powers to undertake compulsory audits in the rest of the public and private sectors.”

The draft code includes information on the factors considered before issuing an Assessment Notice, the ICO’s approach to compulsory audits and the Information Commissioner’s considerations regarding further action following an audit.

Extract from the draft code

4.1 Factors to be considered before issuing notices

Assessment Notices will only be served where it is deemed necessary by the Information Commissioner because:

- a risk assessment has been conducted and indicates a high probability that personal data is not being processed in compliance with the Act with a significant likelihood of damage and distress to individuals, and
- the data controller has failed to respond to a written request from the Information Commissioner to undertake an audit or has refused consent to such an audit, without adequate reasons.

The consultation launched on 11 February 2010 and closes on 24 March 2010. The draft code is available on the ICO’s website at

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

Comments and suggestions can be sent to Chris Turner at

Chris.turner@ico.gsi.gov.uk, or by post to Chris Turner, Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF.

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 Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
2. The ICO is an independent body with 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.
3. 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
4. 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