

Extended Audit Powers for the ICO

From April 2010, extended data protection audit powers will be available to the Information Commissioner's Office (ICO) under the Coroners and Justice Act 2009.

The auditing process allows the ICO to assess whether organisations are processing personal information in accordance with the Data Protection Act 1998 (DPA). Where it has been identified that personal data is at risk, the ICO will continue to request consent to carry out an audit. However, where an organisation refuses to cooperate with the auditing team and there is a significant risk of compromising personal information, the ICO will have the power to serve a compulsory audit notice or an Assessment Notice.

The ICO has developed a Code of Practice for Assessment Notices, which sets out the framework for how audits will be conducted when an Assessment Notice has been served on an organisation.

Initially, the ICO will only be able to conduct compulsory data protection audits on central government departments but will, where it can make a good case, seek to extend its powers to undertake compulsory audits in the rest of the public and private sectors. The Code contains advice on the ICO's auditing framework relevant to all public and private sector organisations and will apply whether an audit is carried out with consent or not.

The ICO does not intend that 'consensual' and 'compulsory' audits will lead to formal enforcement action. Follow up may be by way of obtaining written assurances from the data controller that remedial action has been taken, or a further audit. The Code states that the Information Commissioner will not impose a monetary penalty on a data controller where a breach of the DPA is discovered in the course of carrying out an audit. However, the Commissioner reserves the right to use any of his powers in the case of any identified major non-compliance where the data controller refuses to address a recommendation within an acceptable timescale.