When the ICO comes to call

Is your company ready?

Ann Bevitt of **Morrison & Foerster (UK) LLP** examines the enforcement activity of the Information Commissioner's Office and what organisations should do when faced with an audit process.

Artist: Andy Lovell

The UK's data protection authority, the Information Commissioner's Office (ICO), released its 2012 to 2013 annual report (the report) in June 2013, which confirmed that the general level of ICO enforcement activity is increasing in many areas. For example, between April 2012 and March 2013, the ICO:

- Levied a total of £2.6 million civil monetary penalties; more than double the amount levied in the previous 12 months.
- Conducted 58 audits of data protection practice; an increase of 38% on the previous 12 months.
- Looked at 1,300 cases through its civil enforcement team; a 45% increase on the number of cases looked at in the previous 12 months.
- Levied its first monetary penalty under the Privacy and Electronic Communications (EC Directive) Regulations 2003 (*SI 2426/2003*) (2003 Regulations) for sending unsolicited spam texts.

Although the ICO is keen to stress that enforcement is only one aspect of its approach, it is clear from the figures in the report that this is an increasing area of its focus and activity (*see box "The five Es"*). Accordingly, organisations would be well advised to ensure that they are ready for the ever more likely knock on the door from the ICO.

A number of types of enforcement action are available to the ICO, either individually or in combination, as the circumstances require (*see box "The ICO's enforcement options"*). This article reviews

This article first appeared in the August 2013 issue of PLC Magazine.

those actions, particularly focusing on the ICO's ability to conduct consensual audits, and looks at how organisations should respond to the ICO's request to audit their data processing and what factors they should be considering at each stage of the audit process.

INFORMATION NOTICES

The ICO has the power under section 43 of the Data Protection Act 1998 (DPA) to serve organisations with information notices, which require them to provide information about their processing operations unless the information is legally privileged or self-incriminating. This power can be exercised either in response to an individual's request for an assessment under section 42 of the DPA as to whether or not it is likely that processing affecting the individual has been, or is being, carried out in compliance with the DPA, or if the ICO reasonably requires any information to determine whether the organisation has complied, or is complying, with the principles in the DPA (DPA principles) (*see box "The data protection principles"*).

An organisation served with an information notice may appeal to the Information Tribunal (the tribunal). Failure to comply with an information notice is an offence under section 47 of the DPA.

UNDERTAKINGS AND ENFORCEMENT NOTICES

After an organisation has complied with an information notice, and based on the information provided by the organisation, the ICO may issue an undertaking requiring the organisation to take certain remedial actions. Alternatively, the ICO may serve an enforcement notice under section 40 of the DPA.

When deciding whether to serve an enforcement notice, the ICO is required to consider whether any contravention of the DPA principles has caused, or is likely to cause, any person damage or distress. An organisation served with an enforcement notice may appeal to the tribunal. Failure to comply with an enforcement notice is an offence under section 47 of the DPA.

The five Es

The Information Commissioner's Office has outlined its approach to the task of upholding information rights in the public interest as the following "five Es":

- Enforcing compliance with the law.
- Educating organisations about the right to privacy and the right to know.
- Empowering individuals to assert their rights.
- Enabling improvements in services to be developed.
- Engaging with developments in technology, business and policy.

Recent examples of the ICO's service of undertakings and enforcement notices include the following:

- On 21 June 2013, the ICO served an enforcement notice on Google Inc following a serious breach of the DPA relating to the collection of payload data by Google's Street View cars in the UK.

- On 12 June 2013, Bedford Borough Council signed an undertaking, issued by the ICO on 10 September 2012, to comply with the seventh data protection principle relating to the removal of legacy data from a social care database. Central Bedfordshire Council also signed an undertaking, issued by the ICO on 18 September 2012, to comply with the seventh data protection principle relating to the removal of legacy data from a social care database and in relation to the preparation of planning application documents for publication.

- On 7 June 2013, the ICO served an enforcement notice on Glasgow City Council following a serious breach of the DPA that led to the loss of two unencrypted laptops, one of which contained the personal information of 20,143 people.

CONSENSUAL AUDITS

The ICO has the power to assess, with the agreement of the organisation, whether any organisation's processing of personal data follows "good practice" (*section 51(7), DPA*). Audits are therefore voluntary and are designed to assist companies with compliance and to promote best practice (*see box "The benefits of a consensual audit"*). Between April 2012 and March 2013 the ICO conducted 58 audits of organisations, which represented a 58% increase on the previous 12 months. Most of the organisations audited were local government authorities and criminal justice organisations.

The ICO's approach

The ICO adopts a risk-based approach to identifying which companies it requests to audit. Risk factors include the number of complaints that the ICO receives about an organisation and the nature of the data it processes. Companies can invite the ICO to audit them but unless they satisfy the ICO that there are sufficient risk factors associated with their processing of data, the ICO will decline to audit.

An audit will typically assess an organisation's procedures, systems, records and activities in order to:

- Ensure that the appropriate policies and procedures are in place.
- Verify that those policies and procedures are being followed.
- Test the adequacy controls in place.
- Detect breaches or potential breaches of compliance.

- Recommend any indicated changes in control, policy and procedure.

An audit comprises both an off-site check of policies and an on-site review of procedures in practice. The ICO provides audited organisations with a report that outlines good practice and any areas of improvement required, and makes recommendations to help organisations address these. The ICO publishes, with an organisation's consent, the executive summary of the report on its website and usually carries out a follow-up review approximately six months after the initial audit.

Consent

On receipt of a request from the ICO to conduct an audit, a company will need to decide whether to consent. Factors which may incline an organisation towards agreeing to, or declining, an audit include:

- The perceived level of existing compliance within the organisation generally, or within parts of the organisation.

- The potential negative publicity and possible damage to brand and/or reputation arising out of a refusal to agree to an audit.

- The positive publicity and enhancement of brand and/or reputation arising out of a positive audit.

- The raising of the profile and awareness of data protection within the organisation as a result of the audit process (and this may also be useful in supporting requests for more budget for data protection issues).

If an organisation agrees, in principle, to an audit, it will then need to consider the appropriate scope and timing of the audit, preparation for the audit, and how best to manage any potential risks associated with the audit.

Scope of the audit

The scope of the audit will be agreed before the audit takes place. The ICO's guidance on audits (the audit guidance) lists six potential areas to be covered by an audit, although any audit will cover a maximum of only three of these areas (*www.ico.org.uk/what_we_cover/audits_advisory_visits_and_self_assessments/~/media/documents/library/Data_Protection/Detailed_specialist_guides/auditing_data_protection.pdf*):

- Data protection governance.

- Training and awareness.

- Records management.

- Security of personal data.

- Requests for personal data.

- Data sharing.

For those organisations subject to the Freedom of Information Act 2000, which came into force in 2005 and gives any individual access to information held by public authorities, the handling of freedom of information requests is another potential area to be covered (*for more information, see feature article "Freedom of Information Act: business risk or opportunity?", www.practicallaw.com/0-103-2420*).

Companies need to consider the scope of the proposed audit carefully. On the one hand, for the audit to be meaningful, the scope should not be too narrow; on the other hand, given the risks associated with any audit, and the time and downtime costs involved in engaging in the audit process, companies will want to minimise potential hazards and costs by ensuring that the scope is sufficiently narrow that they feel comfortable that they are maximising their chances of a positive outcome.

Factors that will guide the decision regarding scope include: the size of the business; the amount and type of personal data being processed; and the nature of any complaints received to date. For example, a business with a large retail customer database may want an audit to deal with this aspect of its data processing, whereas a business with a purely business-to-business focus may decide that an internal focus would be more valuable; for example, on its handling of employee data. Very large organisations should bear in mind that the ICO has a limited supply of auditors and therefore too large a scope could put pressure on ICO resources.

Geography may also be an important consideration: does the organisation

The ICO's enforcement options

The Information Commissioner's Office (ICO) may:

- Serve an information notice requiring an organisation to provide the ICO with specified information within a certain time period.

- Serve an enforcement notice where there has been a breach, requiring an organisation to take (or refrain from taking) specified steps to ensure compliance with the law.

- Issue an undertaking committing an organisation to a particular course of action in order to improve its compliance.

- Conduct a consensual audit to assess compliance with the law.

- Serve an assessment notice to conduct a compulsory audit.

- Issue a monetary penalty notice requiring an organisation to pay up to £500,000.

- Prosecute those who commit criminal offences under the Data Protection Act 1998.

feel comfortable with the ICO being in its headquarters, and potentially in contact with areas of the business outside the agreed scope, or is it able to locate the audit within a standalone business function only dealing with that part of the business which is in scope? Once the organisation has determined a scope that is acceptable to it, it will need to agree that scope with the ICO. The ICO is likely to take the view that if the scope is reduced too much, the experience will not be valuable.

As well as agreeing the scope of the audit with the ICO, organisations will need to sign a letter of engagement. A sample letter of engagement can be found at Appendix 2 of the audit guidance. Issues that organisations may need to consider when finalising the letter of engagement include:

- What the audit will not cover.
- The size of the audit team.
- The timeframe for the various activities, including the audit visit itself, the ICO's production of the draft report, the organisation's review of the draft and its agreement to it, and the ICO's publication of the executive summary of the audit on its website.
- The type of follow-up that the organisation is happy for the ICO to undertake.

Having agreed the basic terms of engagement on which the ICO will undertake the audit, organisations may also wish to discuss with the ICO a number of other, more practical, matters before the audit; for example, the number and names of ICO staff who will be undertaking the audit (so that appropriate security access can be arranged for them), and the methodology to be used during the audit process.

Preparing the business

A key step in the audit process is preparing the business for audit. Whereas the ICO may prefer to be free to interview whomever it wants during the audit process, most, if not all, organisations will want to choose with whom the ICO will speak, and make sure that these individuals are properly prepared. Preparation for those employees directly involved in the audit process may include:

- Describing the role of the ICO and the purpose of the audit.
- Explaining the scope of the audit and what will happen during the audit process.
- Undertaking a mock audit with the help of an external third party, such as a law firm or consultant.

The focus of the ICO's interviews with individuals and the evidence gathered by the ICO will depend on the agreed scope of the audit. However, Appendix 1 of the audit guidance contains some generic areas that the ICO normally covers within each scope area.

The data protection principles

When personal data are being processed, the eight data protection principles set out in Part I of Schedule 1 to the Data Protection Act 1998 must be complied with. The principles can be summarised as requiring personal data to be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate and up to date.
- Not kept for longer than necessary.
- Processed in line with data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

At the beginning of the audit visit, the ICO will usually meet with senior managers to explain the audit process to them and answer any questions they have. The ICO will then conduct a series of interviews with individual employees. Organisations may want to ensure that the person with overall responsibility for data protection within the organisation is also present at these interviews, to assist with any questions that individuals are unable to answer. The ICO may also wish to undertake inspections of the workplace and key data processing systems. Organisations should ensure that during the audit process the ICO keeps to the agreed scope and that there is no "mission creep". At the end of the audit visit, the ICO will meet again with senior management and highlight any major concerns identified by the audit team.

The report

The ICO will issue a draft report within ten working days of the site visit, which defines and grades risks, and details the findings and issues identified against those risks. Organisations are given the opportunity to comment on the draft report and the ICO will then produce a second report that will include recommendations mitigating the risks of non-compliance, and reducing the chance of damage or distress to individuals and of regulatory action being taken by the ICO. The ICO will issue this report with a draft executive summary, which organisations will be given ten working days to agree.

Organisations are required to agree the recommendations and produce an action plan detailing how, when and by whom those recommendations will be implemented. The ICO will, with the organisation's consent, publish the executive summary on its website. If an organisation does not consent, the ICO will publish the fact that an audit took place and the organisation refused to agree to the executive summary being published. The executive summaries of audits undertaken in the previous 12 months are published on the ICO's website (*www.ico.org.uk/what_we_cover/audits_advisory_visits_and_self_assessments/audits*).

Assurance ratings

The ICO awards an overall "assurance rating" to indicate the extent to which an organisation has in place effective controls.

There are four assurance ratings:

- High assurance indicates that there is limited scope for improving existing arrangements and significant action is unlikely to be required.
- Reasonable assurance indicates that there is some scope for improvement in existing arrangements.
- Limited assurance indicates that there is scope for improvement in existing arrangements.
- Very limited assurance indicates that there is a substantial risk of non-compliance with the DPA, and immediate remedial action is required.

In the calendar years 2011 and 2012, the ICO audited 21 private sector organisations, 13 of which received a high assurance rating, seven a reasonable assurance rating and one a limited assurance rating. The ICO also awards assurance ratings for each scope area.

In the private sector audits undertaken in 2011 and 2012, the ICO observed good practice particularly in data protection governance, training and awareness and security of personal data, whereas records management was a common area for improvement, usually as a result of a lack of controls or process for the disposal of electronic and/or manual records, and the absence of effective controls to log and track the secure movement of manual records.

The ICO has published helpful details of its findings and observations of good practice in these audits in a guidance note (*www.ico.org.uk/for_organisations/data_protection/working_with_the_ico/~/media/documents/library/Data_Protection/Research_and_reports/outcomes_report_private_sector.ashx*).

Remedies

The ICO does not have the power to impose a monetary penalty following an audit. However, if major breaches of the DPA are identified in an audit, and these are not remedied, the ICO can take further action and issue a recommendation that remedial steps be taken. If the organisation fails to take the necessary action, the ICO can issue an enforcement notice. However, to date, the ICO has not issued any enforcement notices, even where companies have not implemented all of its recommendations.

Advisory visits

In addition to auditing larger organisations with their consent, the ICO can conduct advisory visits on small to medium-sized businesses, charities, not-for-profit organisations and public authorities. The ICO completed its first full year of its advisory visit programme in 2012 to 2013, during which time it visited 78 smaller organisations, including those in the charitable and voluntary sectors. The purpose of an advisory visit is to assist and educate organisations to comply with data protection requirements. Organisations may request an advisory visit and the ICO will prioritise those that will benefit most from a visit.

The purpose of the visit, which takes a day, is to:

- Identify good practice.
- Ensure that appropriate procedures are in place, and that those procedures are being followed.
- Help raise awareness of data protection.
- Provide organisations with an opportunity to use the ICO's resources at no expense.
- Help identify data protection risks and provide practical and pragmatic advice.

The visit focuses on three main areas:

- Security, including physical security, IT network security, access to IT systems, training and reporting incidents.
- Records management, including how records containing personal data are created, maintained and destroyed, and how personal data are collected and kept up to date.
- Requests for personal data, including subject access requests, and how routine and one-off disclosures to other organisations are handled.

The ICO provides an information sheet and a short questionnaire for organisations to complete before an advisory visit. The visit starts with a discussion regarding the completed questionnaire, and then meetings with staff to discuss their work and how they process

The benefits of a consensual audit

The Information Commissioner's Office (ICO) is engaged in a proactive campaign to extend its consensual audit programme. It believes that the benefits of a consensual audit include:

- Helping to raise awareness of data protection.
- Showing an organisation's commitment to, and recognition of, the importance of data protection.
- The opportunity to use the ICO's resources at no expense.
- Independent assurance of the effectiveness of an organisation's data protection policies and practices.
- Identification of data protection risks and practical, pragmatic, organisation-specific recommendations.
- The sharing of knowledge with trained, experienced, qualified staff and an improved working relationship with the ICO.

personal data. The organisation has the chance to ask questions about its processing of personal data.

After the visit, the ICO sends the organisation a short report within three working days, which covers the background to the visit, the areas the ICO reviewed, a summary of findings identifying good practice and areas for improvement, and detailed observations and recommendations. The ICO publishes on its website that it has conducted an advisory visit, and asks the organisation permission to include a short summary of the visit, which includes the first three sections of the report, but not the detailed observations and recommendations. This information is kept on the ICO's website for one year.

COMPULSORY AUDITS

The ICO is able to serve government departments and designated public authorities with a notice under section 41A of the DPA (an assessment notice), which imposes specific requirements on the organisation to enable the ICO to determine whether the organisation has complied, or is complying, with the DPA principles. This process is known as a compulsory audit.

The ICO also has the power to conduct compulsory audits of service providers to assess their compliance with the personal data breach notification requirements in the 2003 Regulations and to audit the measures taken by providers of public electronic communications services to safeguard the security of those services. Although the ICO has the ability to perform a compulsory audit, it will usually seek an organisation's consent, in line with the approach to consensual audits.

Whereas the objective of a consensual audit extends to an organisation's general following of good practice, the primary objective of a compulsory audit is limited to determining the organisation's compliance with the DPA principles. The ICO adopts a risk-based approach to compulsory audit activities, identifying high-risk organisations and sectors by using:

Complaints to the ICO

Most action by the Information Commissioner's Office (ICO) is triggered by complaints. Between April 2012 and March 2013, the ICO received 13,803 complaints, about 1,000 more than it received in the previous 12 months. Most of the complaints received related to organisations failing to respond appropriately to subject access requests. Other complaints related to: disclosures of data; inaccurate data; a lack of data security; the fair processing of data; the right to prevent processing of data; the unfair collection of data; and the collection and retention of excessive or irrelevant data.

The organisations that were the subject of complaints break down as follows: lending institutions (17%); local government (11%); general business (9%); health businesses (9%); central government (6%); policing and criminal records (5%); telecoms (4%); education (4%); insurance (3%); internet (2%); and retail concerns (2%).

According to the ICO's complaints data, spam texts are one of the biggest concerns to consumers. Texts about personal injury or accident claims and PPI claims remain the most common subjects, but there has been a recent rise in spam texts about pension reviewing or reclaiming. Given the number of complaints received regarding spam texts and cold-calling, the ICO has developed a simple online tool to report unwanted marketing by telephone, email or text (*www.ico.org.uk/complaints/marketing/2*).

The ICO investigates all complaints received and, in each case, issues an assessment of whether an organisation is appropriately handling personal data. These assessments are not routinely published. If the ICO determines that further action is required to change the way an organisation collects, uses and/or keeps personal data, there are a number of different steps it can take, depending on the particular facts, including the type and severity of the organisation's failings and whether any action has previously been taken.

- Business intelligence, such as news items.
- Organisations' annual statements on control.
- Organisations' information security maturity models.
- Information received from other regulators.
- The number and nature of complaints received by the Information Commissioner (*see box "Complaints to the ICO"*).
- Other relevant information.

The ICO may issue an assessment notice when:

- An organisation does not consent to a consensual audit within six weeks of being asked to do so.
- The ICO wishes to be assured that an organisation has taken appropriate measures to comply with a formal undertaking or enforcement notice.

Compulsory audits are conducted in two phases: an adequacy audit and a compliance audit.

The adequacy audit is usually conducted off site and consists of a review of relevant policies, procedures, guidance and training material. These documents and the output from their review provide the framework for the compliance audit, which is focused on the agreed scope and conducted on the organisation's site(s) over a number of days. The ICO will meet with staff and observe personal data handling processes to gather evidence of compliance with the DPA principles, and of adherence to the organisation's policies.

The ICO documents its findings in an audit report, which contains its recommendations. The organisation will be given an opportunity to comment on accuracy and respond to the recommendations contained in the audit report. Recommendations are risk-rated, on the ground of impact and probability, to identify those needing immediate or urgent action. Basic details of the audit and executive summaries of the audit reports are made available for a year on the ICO's website.

Further details of the ICO's practice regarding assessment notices and compulsory audits is contained in the ICO's guidance on assessment notices (*www.ico.org.uk/what_we_cover/taking_action/~/media/documents/library/Corporate/Detailed_specialist_guides/assessment_notices_code_of_practice_2012.pdf*).

Related information

Links from www.practicallaw.com

This article is at www.practicallaw.com/8-534-3225

Topics

Data protection	www.practicallaw.com/8-103-1271

Practice notes

Data protection toolkit	www.practicallaw.com/6-517-4600
Data subject access requests	www.practicallaw.com/4-200-2161
Employer obligations under the Data Protection Act 1998	www.practicallaw.com/3-200-2213
Overview of UK data protection regime	www.practicallaw.com/7-107-4765

Previous articles

Compliance for UK cookies: the deadline approaches (2012)	www.practicallaw.com/3-518-9542
Employee data: when to share (2011)	www.practicallaw.com/5-509-0012
Information governance: surfing the wave or drowning? (2009)	www.practicallaw.com/7-386-1696

For subscription enquiries to PLC web materials please call +44 207 202 1200

CIVIL MONETARY PENALTIES

The ICO has had the power to levy civil monetary penalties of up to £500,000 for breaches of the DPA since 6 April 2010, and for breaches of the 2003 Regulations since 26 May 2011 (*see News brief "Data protection fines: how to avoid them", www.practicallaw.com/5-501-5230*).

Until recently, all of the penalties imposed by the ICO were for failing to keep personal information secure as required by the DPA. However, 2012 to 2013 saw the ICO's first monetary penalty for a breach of the DPA that did not relate to keeping personal information secure: on 6 November 2012, Prudential Assurance Company was issued with a penalty of £50,000 for repeatedly confusing two customers' accounts with the same name.

In addition, the ICO has now levied civil monetary penalties under the 2003 Regulations: on 28 November 2012, the owners of Tetrus Telecoms were issued with civil monetary penalties totalling £440,000 for sending spam text messages claiming that recipients were owed compensation for accident claims and PPI mis-selling and, when recipients responded, Tetrus Telecoms sold their details as sales leads. The ICO also issued DM Design Bedroom Limited with a civil monetary penalty for £90,000 on 20 March 2013 for failing to check whether individuals had opted out of receiving marketing calls by registering with the Telephone Preference Service before cold-calling them to sell fitted kitchens.

The ICO has indicated that it will be taking further action to combat unlawful marketing texts and calls. The ICO has also issued guidance on its ability to levy civil monetary penalties and a framework document on determining monetary penalties (*www.ico.org.uk/what_we_cover/taking_action/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ico_guidance_on_monetary_penalties.pdf; www.ico.org.uk/enforcement/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ico_framework_to_determine_amount_penalty.ashx*).

CRIMINAL PROSECUTIONS

Individuals committing criminal breaches of the DPA face fines of up to £5,000 in the Magistrates' Court, and more than £5,000 in the Crown Court, although fines are usually much lower than that. Failing to notify the ICO of data processing is a criminal offence and the ICO has prosecuted a number of organisations for such a failure, including most recently Tetrus Telecoms, which was fined £5,000. Stealing or illegally acquiring personal data is also a criminal offence and, in March 2013, the ICO prosecuted a GP's receptionist who accessed sensitive information regarding her ex-husband's new wife, about which she then texted the new wife; she was fined £1,165. In light of the generally low level of fines for this type of offence, the ICO is pushing for tougher penalties.

Ann Bevitt is a partner and head of the Privacy and Data Security Group in London at Morrison & Foerster (UK) LLP.