Help! I'm being investigated by the ICO

Data protection lawyer and consultant, Stephanie Pritchett, explains what it means to be investigated by the ICO, what to do when breaches occur, and gives her top ten tips for dealing with an investigation

Stephanie Pritchett is the trainer for PDP's training session *Data Protection Essential Knowledge — Level 2,* which includes training on the ICO's powers and other areas of detailed data protection law compliance. This session and *Data Protection Essential Knowledge — Level 1*, led by Peter Carey, provide a thorough grounding in data protection, and can be used as credit for the Practitioner Certificate in Data Protection.

Please visit www.pdptraining.com for further information.

Individuals have long had the right to ask the Information Commissioner's Office ('ICO') for an assessment of a data controller's compliance with the Data Protection Act 1998 ('the DPA'). The ICO can also proactively decide to investigate particular organisations, though historically, this has tended to happen where the ICO has become concerned about standards of compliance within a particular sector or organisation. These concerns may have arisen as a result of, for example, the ICO's general compliance or regulatory strategy, by complaints received from individuals, by media exposure to breaches, or suspected breach reporting from other regulators or industry watchdogs. However, data security breaches seem to remain one of the main reasons for the ICO deciding to carry out a data protection compliance investigation into an organisation.

As there is currently no mandatory requirement in the UK to report a data security breach to the ICO, it is difficult to say with any certainty how common breaches actually are. We do, however, have some indication of the minimum numbers of security breaches from a press release issued by the ICO on 28th May 2010. According to the press release, over 1000 data security breaches had been voluntarily reported to the ICO between November 2007 and May 2010, and that the majority of these breaches had occurred as a result of human or technical errors. The ICO had previously reported that between November 2007 and April 2009, 516 security breach incidents had been notified to the ICO — suggesting that the overall amount of voluntary breach reporting has doubled in the last year. With our next door neighbour, Ireland, publishing its proposal this month to introduce mandatory security breach notification for organisations that lose the data of more than 100 people, we have to question how long it will take for the UK to follow suit. Perhaps only then will the true extent of data security breaches properly come to light.

In May 2010, David Smith, Deputy Commissioner at the ICO, said "we all know that mistakes can happen, but, the fact is that human error is behind a high proportion of security breaches that have been reported to us. Extra vigilance is required so that people's personal information does not end up in the wrong hands. Organisations should have clear security and disclosure procedures that staff can understand, properly implement these, and ensure they are being followed by staff. Staff must be adequately trained not just in the value of personal information, but in how to protect it."

The Data Security Breach Management Guidance, published by the ICO in March 2008, highlighted a number of ways in which a data security breach can occur, including damage to loss or theft of equipment (e.g. a memory stick or laptop), inappropriate access controls, failure of systems, human error (e.g. non-compliance with policies), force majeure circumstances (e.g. fire, flood, etc.) as well as more obvious security breaches, such as hacking, blagging and so on.

What to do when a data breach occurs

If a data security breach occurs within your organisation, some steps to consider taking include:

Consider whether to voluntarily inform the ICO about the breach: The ICO guidance on voluntary notification of security breaches (which has just been updated — see page 1) states that the ICO expects to be informed of 'significant incidents', and suggests that when deciding whether to notify the ICO, organisations should consider:

- the potential harm to individuals affected;
- the volume of personal data lost, released or corrupted; and
- the sensitivity of the data lost, released or corrupted.

The guidance also sets out some of the key components to be included in reports made to the ICO about data security breaches, and recognises that organisations in the financial services sector will most likely also be required to report such incidents to the Financial Services Authority ('FSA'). In case of any future challenge, organisations should still carry out an impact assessment about the breach and, if it is decided not to voluntarily report the breach to the ICO, the reasons for arriving at this decision. David Smith, Deputy Commissioner at the ICO, has previously made public the ICO's view that organisations

(Continued on page 4)

(Continued from page 3)
reporting their data security breaches may find themselves subject to regulatory action, but "those that try to cover up breaches which we subsequently become aware of are likely to face tougher regulatory sanctions."

Follow the data security breach policy: Ideally, before a data breach occurs, organisations will have already prepared a management plan for security breaches, including information about, for example:

- how the organisation will deal with particular types and levels of breach;
- what security breach testing has been carried out previously, and the results of such testing; and
- who is in charge of security breach management within the organisation.

Organisations should also have carried out a data protection and data retention audit and relevant privacy impact assessments, so that they know what data are stored and, therefore, what the scale of the breach is. This will enable organisations to provide business continuity, both during the breach, and during any subsequent investigation or enforcement action.

Identify what the breach has been, and what needs to be done about it: Organisations should ensure that they have detailed information about, for example:

- what actual breach occurred;
- which individuals have been affected;
- what information was affected;
- which of the organisation's systems are affected;
- whether any third parties (e.g. other data controllers or data processors) were involved in the breach; and
- what business continuity measures are needed.

Consider informing affected data subjects and third parties: The ICO may either require organisations to inform related third parties this or advise them to do so as best practice, depending on the nature of the particular breach that has occurred. The ICO guidance states that notification should have a clear purpose, such as to enable individuals who have been affected to take steps to protect themselves, for example by cancelling a credit card. It may also be required to notify others depending on the contractual arrangements that are in place.

Take the necessary follow up actions: The ICO also recommends that organisations should:

- ensure that any organisational practices that have led to the breach are changed to ensure future compliance; and
- review data breach management to see if policies for handling breaches should be changed in the future.

What is an ICO investigation?

There are clearly a number of reasons why the ICO might choose to investigate an organisation, but how would an organisation know that it is being investigated?

The ICO can carry out investigations in a number of ways including:

Issuing an Information Notice: The ICO may issue an 'Information Notice' to require the data controller to give it information about its data processing activities. These are usually followed by formal enforcement action where the ICO finds that breach has occurred.

Making an informal voluntary information request: The ICO may also make an informal 'voluntary information request' which is usually backed by a formal Undertaking given by an organisation to the ICO in lieu of a formal Enforcement Notice. The Undertakings are posted on the ICO's website. Many organisations have been keen to go down this route because the 'Undertaking' implies that, despite being publicly "named and shamed", they accept the ICO's position and are trying to remedy the issue without being required to. Where an Undertaking is not agreed, or the organisation does not comply with it, the ICO usually proceeds quickly with a formal Enforcement Notice. Particularly where an Undertaking has been breached, the ICO will have a much easier task of bringing enforcement action to bear, not least because many of the facts will have already been established and agreed.

Public sector spot checks: Since 6th April 2010, the ICO's powers have been increased to give the regulator a right to enter and inspect the premises of public sector bodies, without notice or a court warrant, to perform spot checks or 'dawn raids' to assess the manner in which those bodies handle personal data. Those organisations are required to co-operate and supply necessary information.

Private sector investigations under warrant (for now): With a court warrant, the ICO may also exercise powers of entry and inspection, as well as the seizure of documents and equipment, from private sector bodies, provided it can first show the court that there is a reasonable suspicion of a data protection law breach. In December 2009, the ICO made public once again its desire for clear unconditional rights to also perform spot checks on private companies without a warrant. It will be interesting to see if the new Conservative/Liberal Democrat Coalition government responds positively to the ICO's request, as this has been an area of much debate given recent high profile security breaches in the private sector. Each party's election manifesto stated that, should it be elected, it would enhance the audit powers of the ICO and extend these to the private sector. It is therefore widely expected that private sector dawn raids will follow soon.

In any event, if the ICO does decide to investigate an organisation (whether by information request, spot check or under warrant), it may cost an organisation a lot of money putting its "house in order" quickly at a time it was unprepared for the financial outlay. In addition to this, organisations should consider (and plan for) the impact of adverse PR should the investigation lead to an agreed Undertaking or other enforcement action.

Investigations may also be carried out by other regulators and enforcement authorities in the UK and Europe.

Examples of these authorities include the Office of Fair Trading, the Advertising Standards Authority, the Financial Services Authority, the Competition Commission, the Health & Safety Executive, the Environment Agency, the European Commission, and further bodies. By way of illustration, in July 2009 the FSA fined three HSBC firms over £3 million for not having adequate systems and controls in place to protect their customers' confidential details, which were lost in the post on two occasions. In a speech to the British Bankers Association in November 2009, Margaret Cole, Director of the Enforcement and Financial Crime Division at the FSA, said that "data security is [an] area where we can, and will, use enforcement action...we expect firms to consider how their actions or failures leave others open to the threat of fraud. We continue to learn of data security lapses that put customers' personal information at risk."

Top ten tips on how to deal with an investigation

Consider the powers under which the ICO has requested information, and confirm whether you are obliged to disclose the information: The ICO has a fair, open and proportionate approach to what it is doing. Staff will be happy to explain why they wish to carry out an investigation and what powers they are exercising. This can provide the organisation with some comfort that it is disclosing the information will be for a legitimate, legal or regulatory reason.

However, organisations should be careful about responding to voluntary disclosure requests (for example, after a security breach), as providing information to the ICO voluntarily may mean breach of confidentiality owed to third parties and data subjects. Organisations will be required to protect their position, whilst also being helpful to the ICO.

Have a process in place to deal with ICO actions: These may include:

- ensuring that someone within the organisation with appropriate authority (e.g. in house counsel, Compliance Officer, Data Protection Officer) "heads up" the process;
- knowing who the key stakeholders will be (e.g. representatives from the firm's IT, legal, compliance, audit & PR functions, as well as relevant third parties), and ensuring this team remains consistent throughout the investigation;
- checking the results of any previous risk assessments to know what the impact of ICO enforcement action will be;
- ensuring there is Board level support of the process;
- being able to respond speedily, accurately and in a focused manner to ICO requests; and
- taking external legal advice from specialist data protection lawyers, as required.

Ensure that key stakeholders are aware of the investigation and know their responsibilities: Data protection officers should consider arranging a key stakeholder meeting to ensure stakeholders are aware of the allegations made, and also to collect facts and to start preparing the organisation's response. It should be ensured that all those involved know that confidentiality is important at this stage.

Carry out an internal investigation into the allegations made by the ICO: Information should be gathered with the help of key stakeholders. Any relevant privacy impact assessments, risk assessments or data protection compliance audits should be reviewed to see what has already been prepared in relation to this. Similarly, the results of the investigation should be reviewed, and the complaint's merit considered — is it based on incorrect facts or assumptions? Data Protection Officers should consider if any other parties are involved and need to be informed (see tips on dealing with a breach as set out above). They should also consider if any other regulators are involved, and need to be informed (for example, the FSA, ASA, etc.). If the organisation has signed up to the ICO's Personal Information Promise, any potential impact from that should be considered.

Prepare a response to the ICO: Before sending any response, data protection officers should seek legal advice as necessary from the organisation's in-house counsel or external advisors about the implications of the information it is imparting and agree on a 'strategy' going forward.

Consider speaking to the ICO 'offline' to see if you can agree a compromise: The ICO is keen to help find practical solutions, and may, depending on the severity of the breach, agree to an informal investigation or Undertaking rather than further formal enforcement action. However, it should be remembered that where an organisation agrees to an Undertaking and then breaches it, the ICO will have a clearer and more direct route to enforcement.

Be aware that all information provided to the ICO could be disclosed under FOIA: Where relevant, make it clear in any response to the ICO that the information being provided is commercially sensitive, and request that it be kept confidential and not disclosed under the Freedom of Information Act.

Keep a copy of all information provided to the ICO: This may be needed in case of future challenge.

Prepare any necessary PR: It should be decided how information about the investigation or breach should be presented, if any press releases are necessary, and how to deal with any further media requests for information. Organisations should consider issuing an internal response so that all staff are 'singing from the same hymn sheet' if third parties make enquiries.

Follow up actions: Organisations should undertake whatever remedial action it and/or the ICO have deemed necessary. They should also carry out any necessary staff disciplinary action, staff awareness training, and change their policies to try to prevent reoccurring breaches. Organisations should then carry out follow up privacy impact assessments, risk assessments or data protection compliance audits, to ensure future compliance.

Stephanie Pritchett
Pritchett's Law
stephanie@pritchettslaw.com