# Using privacy impact assessments

***Data protection lawyer and consultant, Stephanie Pritchett, addresses the main questions surrounding the use of privacy impact assessments***

On 6th April 2010, the UK's Information Commissioner's Office ('ICO') was given new powers to issue penalties of up to £500,000 for serious contraventions of the Data Protection Act 1998 ('DPA') and to 'dawn raid' public sector bodies for compliance investigation.

Before the credit crunch dominated business reporting, data protection and data security breaches were mainstream news. It was rare to pick up a newspaper without a front page headline about sensitive information left in skips or missing laptops and memory sticks containing information about thousands of customers.

The recession undoubtedly meant a new media vocabulary and more 'exciting' headlines. It has also meant a greater temptation for organisations to cut corners, and a greater desire to exploit databases and information assets. Season with compliance cuts, and there is a recipe for unmanageable and dangerous business risks.

Privacy impact assessments ('PIA') can assist with the process of compliance by:

- providing a measure against which to assess staff compliance at a practical level;
- minimising the risk of a security breach occurring by taking appropriate preventative measures;
- impressing on the ICO and others that data protection obligations are being taken seriously, and that steps are being taken to minimise non-compliance; and
- ensuring that an organisation discovers about privacy problems itself rather than from regulators, critics or competitor organisations.

## What is a privacy impact assessment?

Usually a PIA is used by organisations that are in the process of deciding whether to process personal data in new ways, or using new technology for the first time.

They aim to help an organisation to:

- identify what processing is being carried out;
- identify the risks to individuals and the organisation of new data processing activities, particularly on projects with a wide ranging scope or using intrusive technologies, or involving sensitive or high risk information;
- identify the privacy risks beyond data protection law;
- identify problems that might occur before they actually happen, to avoid (in the ICO's words), "expensive, inadequate 'bolt-on' solutions" when the issue could have been more cheaply and effectively resolved at an earlier stage of the project;
- identify solutions to those risks and problems;
- prevent loss of public confidence and minimise reputation risk to corporations and public sector bodies if a data breach occurs. In the ICO's words, "experience shows that once an organisation's reputation is damaged and trust is lost, it is then very hard to regain that trust;"
- create a 'privacy friendly culture' in the organisation; and
- comply with legal and regulatory requirements, in addition to any relevant best practice guidelines.

## When to use a PIA

The process of carrying out a PIA is separate from carrying out a data protection audit or an information security assessment. Although a number of the same issues will be addressed, the other processes tend to focus only on the organisation and not on third parties who may be affected.

The aim of a PIA is to stop data protection and privacy problems arising in order to prevent any interruption and unnecessary expense later on. Therefore, they are best run on projects at the project design or early implementation stage. The ICO suggests that they should be carried out before (i) decisions are set in stone; (ii) systems are procured; (iii) contracts have been signed; and (iv) at a stage where the project can still change course. The PIA can always be

*(Continued on page 8)*

Stephanie Pritchett is the trainer for PDP's training session *Data Protection Essential Knowledge — Level 2,* which includes training on privacy impact assessments. 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 towards the Practitioner Certificate in Data Protection.

Please visit www.pdptraining.com for further information.

*(Continued from page 7)*
followed up with another PIA at the stage when changes are being made to the running of a particular project.

By comparison, more general data protection compliance or IT security checks are usually carried out on projects that have already been implemented and have been running for some time. They aim to evaluate whether data protection and privacy laws have been complied with, and if not, what steps need to be taken to address any deficiencies. Where problems do exist, they will usually be expensive to fix and cause irksome business interruption.

## Are we legally obliged to carry out a PIA?

Though there is no legal requirement to carry out a PIA, the Cabinet Office has instructed all central government departments and agencies that it is compulsory for them to carry out PIAs when developing new systems. The ICO has also opined that PIAs should be used more widely by all public and private sector organisations in line with the published strategy that preventative steps are far more effective in minimising risk at the early stages of projects rather than as an afterthought.

## Who is responsible for carrying out the PIA?

As a PIA is strategically important, the ICO advises that it should be managed by a senior person within the organisation, and points out that those people who already have responsibility for the organisation's risk management, audit or compliance, may be best placed to understand the nature of the work involved in carrying out a PIA. Other recommendations include:

- for a senior member of the relevant project team to be responsible for ensuring the outcomes of the PIA are implemented in the project;
- to avoid brining in someone from outside the team who may find it hard for their views to be taken seriously;
- for the recruitment of an external consultant, if an independent view, external resource or skills are needed. The problem with this is that the individual may be criticised for not understanding the organisation sufficiently, and so their recommendations not given appropriate weight;
- making a project steering committee responsible (where the project is a large one); or
- the organisation's Data Protection Officer — only to be involved where that person has authority to influence the design and development of a project and participate fully in the project design decisions.

***"As a PIA is strategically important, the ICO advises that it should be managed by a senior person within the organisation, and points out that those people who already have responsibility for the organisation's risk management, audit or compliance, may be best placed to understand the nature of the work involved in carrying out a PIA.***

The ICO has said that, while it may be able to consult on some large scale projects, the organisation would always be required to have first fully utilised the ICO PIA Handbook. It is fair to say though that, even where the ICO has cast its eye over a project, it would never totally sign off on its compliance, and legal advice may well be necessary.

## The ICO's PIA Handbook

Following an international study by the ICO into the use of PIAs in other countries (for instance, in Canada, New Zealand and Australia), the ICO published the first UK PIA handbook in December 2007. Between its publication and June 2009, the ICO worked closely with both public and private sector organisations who had used the PIA handbook before re-launching a revised handbook which benefited from feedback received concerning practical PIA experience.

The PIA Handbook sets out practical advice and checklists on how to carry out the following key parts of a PIA:

**Initial assessment** — Organisations should carry out an initial assessment at the project design stage to consider the following:

- what the project involves and whether there are likely to be privacy risks;
- who internally and externally is involved with, or affected by, the project;
- where there have been similar projects before, and if so, whether there are previous PIAs that could impact on or be relevant to this project;
- what technologies are involved and what would be the nature of their impact; and
- whether a full scale or a small scale PIA should be carried out.

The ICO Handbook contains helpful screening questions to assist with this process and ensure that the PIA carried out is proportionate to the risks involved. As the ICO has said, "it can be very expensive for an organisation to discover too late that a project has substantial privacy impacts. On the other hand, it would be a waste of resources to unnecessarily carry out a PIA, or complete a full scale PIA where only a small-scale PIA is needed. It is therefore worth doing some preliminary evaluation to determine whether a PIA is necessary and what level of PIA is required."

**Full scale or small scale PIA** — When carrying out a full scale or small scale PIA, organisations

should:

- consider who to consult about the project;
- carry out interview, consultation or focus group sessions to gather information;
- carry out an audit to determine the privacy and data protection risks;
- consider the audit results and stakeholder responses;
- identify problems with the project and how to eradicate or minimise them;
- make a project plan setting out key milestones and dates for project implementation and for addressing the privacy issues by each milestone;
- prepare guidelines for circulation, highlighting compliance issues and practical guidance on how the issues has been or will be resolved;
- train appropriate stakeholders in the organisation's privacy practices as well as data protection and privacy laws generally to ensure continued compliance on a practical level;
- set a date to review the project at the post-implementation stage to see if the solutions have worked, or if any further changes are needed to address privacy risks.

Small scale PIA's need not be as formal or time intensive as the wider PIA. Also, the right stakeholders should be approached for information. It is important to get this right, and the ICO describes the risk thus: "there is...a danger that too much full-scale public consultation may lead to fatigue among stakeholder groups, who themselves do not have the resources to devote to providing so many consultation responses. As a result, stakeholders may begin to channel resources into higher profile projects. This can lead to the PIA process not achieving one of its core aims of representing the privacy concerns from all perspectives, particularly in more limited projects."

Finally, the risks identified via the small scale PIA may justify scaling the PIA up to a full scale PIA.

The ICO sets out numerous examples of projects where a small scale PIA will most likely be appropriate. These include the following:

- before the replacement of existing personal data IT systems;
- when collecting items of personal data from a new third party source;
- before carrying out revisions to data disclosure or staff communications policies;
- when there has been a change in data protection or privacy law;
- before the application of a new technology to an existing purpose;
- before drafting new customer verification procedures;
- when re-designing data collection web-forms;
- before outsourcing or off-shoring business processes involving personal data;
- before the application of existing personal data to a new purpose;
- before enacting changes to data retention policies; and
- before making amendments to the organisation's privacy policy statement.

## Privacy and data protection law compliance checks

Aside from a PIA, when carrying out an audit to determine what the privacy and data protection risks and liabilities are likely to be on the project, organisations should consider and document the organisation's legal compliance with 'privacy' laws including:

- the Human Rights Act 1998;
- the Regulation of Investigatory Powers Act 2000;
- the Privacy and Electronic Communications Regulations 2003 ('PECR');
- the law of confidence;
- torts of negligence and passing off;
- the emerging tort of privacy; and provisions within statutes relating to public health, education, family law, etc.

## The Data Protection Act 1998

The ICO Handbook contains some helpful templates to assist checking the compliance of a design against the DPA and PECR. These should provide some assistance when considering the issues that need to be addressed. Organisations will then need to consider whether the risks identified are acceptable. If they are not, the ICO recommends that it is decided:

i) what the business need is that justifies taking those risks; and

ii) what steps might be taken to eradicate or minimise those risks.

## The Commissioner — a toothless tiger?

In the past, the Information Commissioner has been the subject of substantial criticism over his lack of enforcement powers. The proactive stance of new UK Commissioner, Christopher Graham, together with increased powers to fine, rights to spot check public sector bodies (with similar 'dawn raid' powers for the private sector bodies likely to follow), personal criminal liability for directors (under section 61 of the DPA) and increased funding, mean that enforcement action is undoubtedly set to increase.

Prevention is better than a painful cure, and PIAs provide a structured way to take a timely look at the preventative steps which may be necessary.

**Stephanie Pritchett**
Pritchett's Law
stephanie@pritchettslaw.com