Bilsington Parish Council

What the Information Commissioners Office means by Privacy Impact Assessment

Privacy Impact Assessment is a process which helps an organisation to identify and reduce the privacy risks of a project. An effective Privacy Impact Assessment will be used throughout the development and implementation of a project, using existing project management processes. A Privacy Impact Assessment enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

The Information Commissioners Office uses the term project in a broad and flexible way – it means any plan or proposal in an organisation, and does not need to meet an organisation's formal or technical definition of a project, for example set out in a project management methodology.

Privacy Impact Assessments are often applied to new projects, because this allows greater scope for influencing how the project will be implemented. A Privacy Impact Assessment can also be useful when an organisation is planning changes to an existing system, but the organisation needs to ensure that there is a realistic opportunity for the process to implement necessary changes to the system.

The purpose of the Privacy Impact Assessment is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. This analysis can be tested by consulting with people who will be working on, or affected by, the project.

These can be risks to the individuals affected, in terms of the potential for damage or distress. There will also be corporate risks to the organisation carrying out the project, such as the financial and reputational impact of a data breach. Projects with higher risk levels and which are more intrusive are likely to have a higher impact on privacy.

Each organisation will be best placed to determine how it considers the issue of privacy risks. The steps in this code can be applied to a wide range of business processes. The Information Commissioners Office has designed its Privacy Impact Assessment methodology to be as flexible as possible so that it can be integrated with an organisation's existing ways of working.

Conducting a Privacy Impact Assessment does not have to be complex or time consuming but there must be a level of rigour in proportion to the privacy risks arising.

What do we mean by privacy?

Privacy, in its broadest sense, is about the right of an individual to be let alone. It can take two forms, and these can be subject to different types of intrusion:

- Physical privacy – the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.
- Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance

or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

This code is concerned primarily with informational privacy, but an organisation can use Privacy Impact Assessments to assess what they think are the most relevant aspects of privacy.

Privacy risk is the risk of harm arising though an intrusion into privacy. This code is concerned primarily with minimising the risk of informational privacy – the risk of harm through use or misuse of personal information. Some of the ways this risk can arise is through personal information being:

- Inaccurate, insufficient or out of date;
- Excessive or irrelevant;
- Kept far too long;
- Disclosed to those who the person it is about does not want to have it;
- Used in ways that are unacceptable to or unexpected by the person it is about; or
- Not kept securely.

Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job. At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of confidential or sensitive information. Sometimes harm might still be real even if it is not obvious, for example the fear of identity theft that comes from knowing that the security of information could be compromised. There is also harm which goes beyond the immediate impact on individuals. The harm arising from use of personal information may be imperceptible or inconsequential to individuals, but cumulative and substantial in its impact on society. It might for example contribute to a loss of personal autonomy or dignity or exacerbate fears of excessive surveillance.

The outcome of a Privacy Impact assessment should be a minimisation of privacy risk. An organisation will need to develop an understanding of how it will approach the broad topics of privacy and privacy risks. There is not a single set of features which will be relevant to all organisations and all types of project – a central government department planning a national crime prevention strategy will have a different set of issues to consider to an app developer programming a game which collects some information about users.

Understanding privacy risk in this context does though require an understanding of the relationship between an individual and an organisation. Factors that can have a bearing on this include:

- Reasonable expectations of how the activity of individuals will be monitored.
- Reasonable expectations of the level of interaction between an individual and an organisation.
- The level of understanding of how and why particular decisions are made about people.

Public bodies need to be aware of their obligations under the Human Rights Act. Article 8 of the European Convention on Human Rights guarantees a right to respect for private life which can only be interfered with when it is necessary to meet a legitimate social need. Organisations which are subject to the Human Rights Act can use a Privacy Impact Assessment to help ensure that any actions that interfere with the right to private life are necessary and proportionate.

The benefits of a Privacy Impact Assessment

Conducting a Privacy Impact Assessment is not a legal requirement of the Data Protection Act. The Information Commissioners Office promotes Privacy Impact Assessments as a tool which will help organisations to comply with their Data Protection Act obligations, as well as bringing further benefits. Carrying out an effective Privacy Impact Assessment should benefit the people affected by a project and also the organisation carrying out the project.

Whilst a Privacy Impact Assessment is not a legal requirement the Information Commissioners Office may often ask an organisation whether they have carried out a Privacy Impact Assessment. It is often the most effective way to demonstrate to the Information Commissioners Office how personal data processing complies with the Data Protection Act.

The first benefit to individuals will be that they can be reassured that the organisations which use their information have followed best practice. A project which has been subject to a Privacy Impact Assessment should be less privacy intrusive and therefore less likely to affect individuals in a negative way.

A second benefit to individuals is that a Privacy Impact Assessment should improve transparency and make it easier for them to understand how and why their information is being used.

Organisations that conduct effective Privacy Impact Assessments should also benefit. The process of conducting the assessment will improve how they use information which impacts on individual privacy. This should in turn reduce the likelihood of the organisation failing to meet its legal obligations under the Data Protection act and of a breach of the legislation occurring.

Conducting and publicising a Privacy Impact Assessment will help an organisation to build trust with the people using their services. The actions taken during and after the Privacy Impact Assessment process can improve an organisation's understanding of their customers.

There can be financial benefits to conducting a Privacy Impact Assessment. Identifying a problem early will generally require a simpler and less costly solution. A Privacy Impact Assessment can also reduce the ongoing costs of a project by minimising the amount of information being collected or used where this is possible, and devising more straightforward processes for staff.

More generally, consistent use of Privacy Impact Assessments will increase the awareness of privacy and data protection issues within an organisation and ensure that all relevant staff involved in designing projects think about privacy at the early stages of the project.

Projects which might require a Privacy Impact Assessment.

The core principles of Privacy Impact Assessments can be applied to any project which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals.

Privacy Impact Assessment terminology often refers to a project as the subject of a Privacy Impact Assessment and this should be widely construed. A Privacy Impact Assessment is suitable for a variety of situations:

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.

- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding Automatic number plate recognition capabilities to existing CCTV).
- A new database which consolidates information held by separate parts of an organisation.
- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.

A Privacy Impact Assessment should be used on specific projects and to be effective it should be applied at a time when it is possible to have an impact on the project. This means that Privacy Impact Assessments are more likely to be of use when applied to new projects or revisions of existing projects. Conducting a Privacy Impact Assessment of an existing project is less likely to make a positive difference unless it is possible for necessary changes to be implemented.

Organisations should develop the capability to identify the need for a Privacy Impact Assessment at an early stage and should consider building this into their project management or other business processes.

Responsibility for conducting a Privacy Impact Assessment.

Each organisation can decide who is best placed to coordinate and carry out the Privacy Impact Assessment process. Large organisations are more likely to have a dedicated Data Protection Officer. A Data Protection Officer is naturally well-placed to have a significant role in a Privacy Impact Assessment, and may also be able to design a set of Privacy Impact Assessment tools which mirror an organisation's existing processes. They may also maintain a log of all Privacy Impact Assessments carried out in the organisation.

Not all organisations have their own Data Protection Officer, or it may be difficult for a Data Protection Officer to conduct all the Privacy Impact Assessments – the general approach to Privacy Impact Assessments is also intended for use by non-experts. Project, risk or other managers without specialist data protection knowledge should be able to use the screening questions in Annex one to help them focus on privacy issues. An effective Privacy Impact Assessment will include some involvement from various people in an organisation, who will each be able to identify different privacy risks and solutions.