Privacy Impact Assessments.

Aldington
&
Bonnington
Parish
Council

Privacy Impact Assessments

This guide is intended to help you determine quickly, whether a Privacy Impact Assessment is necessary and, if so, at what level.

If you decide a Privacy Impact Assessment is necessary, the guidance given later will help you complete the Privacy Impact Assessment Template.

What is a Privacy Impact Assessment?

A Privacy Impact Assessment:

- Is a process to identify and minimise the privacy risks associated with any new initiative or change. Consultation with stakeholders is a key part of this process.
    - Note: 'privacy risks' means – risks to the privacy of individuals whose personal information will be used on the system or affected by the change. High risks will normally result from inadequate security or poor system design.
- Aims to build privacy in from the outset, so it is not really suitable for checking existing systems.
- Is not designed to dictate specific outcomes or limit options. Decision makers will always need to weigh privacy risks against other risks.
- Is not intended to increase the administrative burden and is not about form filling. It is an active process and should, as far as possible, be integrated with the project to which it relates. A well planned approach will avoid duplication of work.
- Is a part of the overall risk assessment and risk management process, and should be done in a way that is proportionate to the risks.
- Involves checking compliance with the law, though that is only a part of what it's about.

What are the risks of not carry out a Privacy Impact Assessment?

The risks are:

- Need for re-design all or major parts of the system, which could be particularly costly if the risks are realised late in the development stage;
- Collapse of the project or the completed system as a result of adverse publicity and/or withdrawal of support by key participating organisations;
- Loss of credibility as the public perception is that the system does not protect their personal data adequately and safeguard their privacy;
- Subsequent imposition of regulatory conditions as a response to public concerns, with the inevitable cost that entails;
- Low adoption rates or poor participation in the implemented scheme;
- Breach of privacy law, with the possibility of litigation.

Under what circumstances should I carry out a Privacy Impact Assessment?

You should carry out a Privacy Impact Assessment whenever you are implementing or making a change to a process or system that could have an impact on the privacy of individuals. If you are sure that there are no privacy implications in what you are doing, there is no need to do a Privacy Impact Assessment, but the decision not to do one (and reasons) should be recorded in the project log. If you are not sure, then you should at least go through the screening process described below. If it turns out that a Privacy Impact Assessment is needed, the screening will also help you determine what resource you need to put into the Privacy Impact Assessment.

The Privacy Impact Assessment process is not designed for existing systems. The purpose of a Privacy Impact Assessment is to build privacy in from the outset. If you want to check an existing system you should carry out a privacy or data protection audit.

You will see the term “project” used throughout this guide. It should be interpreted loosely to cover any initiative or change that could have privacy implications, including policy development, databases, processes, data sharing (see below), services, schemes, outsourcing, reviews, etc.

Data sharing

A Privacy Impact Assessment should still be carried out even if the Council has a permissive power to share personal data with other public bodies. Whilst most legal gateways will provide for the sharing of personal information, they do not cover all aspects, e.g. they won’t state the level of security protection required for databases or the way data should be transferred.

When should I start?

Privacy protective features should be designed into a system, rather than bolted on later leading to delays in the project and escalating costs. The Privacy Impact Assessment should be started at project initiation phase, sustained throughout the project lifecycle and re-visited in each new project phase. The earlier you start, the more likely you are to “design-in” privacy considerations and the less likely you are to have to unpick what you’ve already done.

How should I do it?

The Privacy Impact Assessment process is explained in detail later in this document. If the Privacy Impact Assessment is being run as part of a project, every attempt should be made to integrate the Privacy Impact Assessment within that project. Privacy risks should not be considered in isolation from other types of risks – when determining priorities you need to weigh all the risks against one another.

It is important to remember that a Privacy Impact Assessment is a process to ensure privacy risks are addressed throughout the lifecycle of the project – it is not about ticking boxes and producing documentation. Nevertheless, you also need to have a record – usually in the form of a Privacy Impact Assessment report – of the measures that were taken to address the privacy issues in the project. This is so that there is:

- Accountability and transparency – the report is likely to be published under the Council's Freedom of Information Publication Scheme;
- A basis for the post implementation review;
- A basis for audit;
- A record to be called up for future Privacy Impact Assessments. Privacy Impact Assessments can be re-used subject to appropriate review for subsequent substantially similar projects.

The Trafford Privacy Impact Assessment Template, when completed fully, is designed to provide a suitable freestanding record of a Privacy Impact Assessment.

How the Privacy Impact Assessment process aligns with the Project/programme lifecycle

The Privacy Impact Assessment should be initiated at the start of the project and re-visited at each new phase in the project life-cycle. There is no precise guidance on how the Privacy Impact Assessment process links to the project/programme lifecycle, but it is reasonable to expect that most of the work on the Privacy Impact Assessment, including all the important consultation and risk analysis, will be done in the early stages so that it can inform the options put forward in the Outline Business Case. For this reason, work should begin once the project mandate has been drafted and a business case has started to develop.

What if the project is already up and running?

The core of a Privacy Impact Assessment is consultation, so unless there is a genuine opportunity for the design or implementation of the project to be altered as a result of the views expressed by stakeholders, you should not carry out a Privacy Impact Assessment on a project that is already up and running. Such projects should instead be submitted to a compliance check or data protection audit.

What are the outcomes of an effective Privacy Impact Assessment?

The outcomes of an effective Privacy Impact Assessment will be:

- Identification of a project's privacy impacts;
- An appreciation of those impacts from the point of view of each group of stakeholders;
- Understanding of the acceptability of the project from those affected by it;
- Identification of ways to avoid negative impacts on privacy;
- Identification and assessment of less privacy-invasive alternatives;
- Where negative impacts on privacy are unavoidable, clarification of the business needs that justify them;
- Documented and published outcomes.

The Privacy Impact Assessment Process

Preparation for the screening process

The purpose of the screening process is to work out whether a Privacy Impact Assessment is necessary and if so, how it should be scaled. It should ensure that the time and effort you put into carrying out a Privacy Impact Assessment is proportionate to the risks. If you conclude that a Privacy Impact Assessment is not necessary, the screening process will also help you determine whether you should at least, check compliance with privacy laws, including the Data Protection Act.

Before you start the screening process you need to gather the information set out below. You can record these details on the Privacy Impact Assessment Template,

- State the purpose and objectives of the project or process in the Project Outline. As well as providing a clear and well-argued case for the project as a whole, it should also highlight those features that may have the potential for the biggest impact upon privacy. You should use the project mandate, your knowledge of the scope of the initiative, and/or advice from key stakeholders to inform the Project Outline.
- Make a preliminary assessment of the data usage, so that you have a clear understanding of who will have access to data affecting privacy, how, when and why. Gather information on the proposed security measures.
- Undertake a preliminary stakeholder analysis by identifying the organisations directly involved in the project, as well as those who will benefit or be affected by it and those that provide the technology or services to enable it. Also identify the internal stakeholders.
- Look at what else is out there (also known as an environmental scan). Look around – both within and outside the organisation – to gather information from previous projects of a similar nature (particularly where the same or similar technology has been used) to see whether there are any lessons you can draw upon.

Your approach to the above should be proportionate to the project or initiative you are addressing. If it is of a minor nature where there is no formal project – for example a new request to share data – the information can probably be gathered and documented with minimal effort.

You should now have all the information you need to carry out the screening process, which will enable you to decide whether a Privacy Impact Assessment is necessary.

Carrying out the screening process

The scale of a Privacy Impact Assessment should flow naturally from the number and severity of the privacy risks and range of stakeholders that need to be consulted, but the process to be followed is essentially the same at any scale. The screening process consists of answering a number of questions. These are set out in the Privacy Impact Assessment Template and cover the following areas:

- Technology;
- Identification methods;
- Involvement of multiple organisations;
- Changes to the way data is handled;
- Changes to data handling procedures;
- Statutory exemptions/protection;

- Justification.

Outcome of the screening process

Having worked through the screening questions you should now have a clear idea about what the main privacy risks are. These should be recorded in section 7.1. this will help to clarify the basis of your decision and help to inform the planning you do in the next stage, and it should ensure the framework and resourcing for any Privacy Impact Assessment are in proportion to the perceived risks. If a Privacy Impact Assessment follows this preliminary identification of the risks should be treated very much as work in progress – the whole purpose of the consultation phase of the Privacy Impact Assessment is to find ways to avoid or reduce the effects of these risks, as well as to surface any other risks that may exist. It is of course important to consider privacy risks alongside other project risks.

A decision must then be made based on this as to whether you need to do a Privacy Impact Assessment, or whether a privacy law compliance check is sufficient (see checking compliance with privacy law below). This cannot be a scoring exercise but must involve a judgement about any risks identified. It is possible that a single ‘yes’ in the screening exercise is sufficient to justify a Privacy Impact Assessment on one project, but several ‘yeses’ do not justify a Privacy Impact Assessment on another.

Preparation for consultation and analysis

Having concluded that a Privacy Impact Assessment is warranted, the next stage is to make the preparations for the all important consultation and risk analysis stages. These stages are at the core of any Privacy Impact Assessment and are what distinguishes it from a straightforward legal compliance check.

1. ***How is it going to be managed and who’s going to be involved?***

The governance framework you put in place for this work will be determined by the scale of the Privacy Impact Assessment. In most cases, the Privacy Impact Assessment will be an integral part of the project or programme to which it relates, and not a separate process. The project manager should be responsible for the conduct of the Privacy Impact Assessment and will take ownership of the privacy risks in the same way as other project risks. It is important to keep clear oversight of the privacy risks.

2. ***Privacy Impact Assessments in terms of the overall project***

In your project documentation you will want to make clear what the objectives of the Privacy Impact Assessment are. The following are appropriate executive level objectives for a Privacy Impact Assessment:

- Ensure effective management of the privacy impacts arising from the project;
- Ensure effective management of the privacy risks arising from the project;

- Avoid expensive re-work and retro-fitting of features, by discovering issues early, devising solutions at an early stage in the project life-cycle, and ensuring that they are implemented.

3. *A closer look at who the stakeholders are*

Once you've decided who is going to be involved in the remaining stages of the Privacy Impact Assessment, one of the first actions to complete as a team is to look back at the preliminary analysis of stakeholders.

This builds on the work you did during the preparation for the screening stage. You now need to consider in more detail what the interest of the various stakeholders are and the level of involvement they will have in the Privacy Impact Assessment. You need to:

- Agree whether all the stakeholders have been identified;
- Make a distinction between internal and external stakeholders;
- Decide whether you can carry out the consultation with representatives of, or advocates for, some stakeholder groups;
- Agree what the perspective, or interests, of all the stakeholders are;
- Decide <u>how</u> you will consult them e.g. face to face meetings, phone calls, correspondence, workshops etc.

4. *Consultation plan*

It is important that the time and effort spent consulting each stakeholder is proportionate to the seriousness of the risks they are helping you address – as with the management of all risks proportionality should be the watchword. Form the work you have completed so far, you should have an initial view of the privacy risks which you can use to guide you in drawing up a consultation plan.

Pointers for effective consultation are set out below.

5. *Resources*

Form the above work you should be able to estimate the resources required for the consultation process and risk analysis work, and will want to make sure those resources are secured before the consultation starts.

The consultation

You should now be ready to start consulting stakeholders. This stage, with the legal compliance check, is closely linked with the risk analysis stage. You should treat them as a cyclical process, surfacing risks and going back to stakeholders to explore acceptable ways to avoid or mitigate those risks. If you are conducting a large Privacy Impact Assessment and the consultation is particularly in depth or widespread, you may wish to produce a consultation report and use this to inform the risk analysis stage.

Effective consultation depends on all stakeholders being sufficiently well-informed about the project, having the opportunity to convey their perspectives and their concerns, and developing confidence that their perspectives are being reflected in the design.

Some useful ways of ensuring effective consultation include:

- Priming of discussions by providing some initial information about the project;
- Making sure there is ongoing dialogue with consultees throughout the Privacy Impact Assessment process;
- Participation of representatives of, and advocates for, stakeholder consultation groups who have appropriate background in the technologies, systems and privacy impacts involved;
- Facilitated interactions among the participants;
- Making sure that there is sufficient diversity among those groups or individuals being consulted, to ensure that all relevant perspectives are represented, and all relevant information is gathered;
- Making sure that each group has the opportunity to provide information and comment, even including multiple rounds of consultation where necessary;
- Making sure that the method of consultation suits the consultation group, for example using workshops or focus groups as an alternative to, or even as well as, formal written consultation;
- Making sure that the information provided by all parties to the consultation is fed into the subsequent rounds of design and implementation activities; and
- Ensuring that the perspectives, concerns and issues raised during the consultation process are seen to be reflected in the outcomes of the Privacy Impact Assessment process.

You will save time by involving the right *internal* stakeholders in your meetings with *external* stakeholders. For example, what an external stakeholder might think is a good solution might not be so if it is not technically feasible. Remember, your aim all the way through is to find ways to enhance privacy.

A Privacy Impact Assessment should be undertaken in as open a manner as possible. Where there are sensitive security considerations, however, you should consider holding discussions in closed sessions and recording the information in confidential appendices.

Compliance with privacy law (including Data Protection Act)

A privacy law compliance check will be carried out either as part of a Privacy Impact Assessment, or as a stand alone process when a Privacy Impact Assessment is unnecessary. Although the process can be run in parallel with the consultation and risk analysis stages, it cannot be finalised until late in the project life-cycle when the design is complete. This is why we revisit the compliance immediately before implementation.

The privacy laws that could be relevant – and briefly what they do – are as follows.

Data Protection Act 1998 – regulates, through its 8 principles, the processing or personal data – i.e. information about living identifiable individuals.

Article 8 of the Human Rights Act – states that everyone has the right to respect for their private and family life, their home and correspondence. This right is qualified, and exceptions relate to national security, public safety or economic wellbeing of the country, prevention of disorder or crime, protection of health or morals, or of the rights and freedoms of others.

Privacy and Electronic Communications Regulations – regulates electronic direct marketing e.g. email and text messages.

Regulatory and Investigatory Powers Act – regulates the interception of communications data (e.g. phone calls, emails and postal letter), their acquisition and disclosure, the carrying out of covert surveillance etc.

Common law duty of confidence – points to consider are whether;

- The information has the necessary quality of confidence;
- The information will be given in circumstances under an obligation of confidence; and
- There could be an unauthorised use of the information to the detriment of the confider (although detriment does not always need to exist for a breach of confidence to be actionable)

The Privacy Impact Assessment Template includes a separate template for checking Data Protection Act compliance (see Privacy Impact Assessment Template, Appendix A).

Compliance checking will be particularly relevant in the context of data sharing.

Risk analysis

It is recommended that you progressively record the issues raised by each of the stakeholder groups in an issues register, or use the Privacy Impact Assessment Template. From this you should start to form a clear picture about how significant the risks you previously identified are, and whether there are previously unseen risks. This work and the stakeholder consultation are a cyclical process. As you clarify what the risks mean you should work with stakeholders – both internal and external – to find ways to avoid or mitigate those risks.

Risks – avoidance and mitigation

There are two types of solutions to privacy risks – avoidance measures and mitigation measures.

An avoidance measure is a means of dissipating a risk. It refers to the exclusion of technologies, processes, data or decision criteria, in order to avoid particular privacy issues arising. Examples include:

- Minimisation of personal data collection;
- Non-collection of contentious data-items;
- Active measures to preclude the use of particular data-items in the making of particular decisions;
- Active measures to preclude the disclosure of particular data-items.

A mitigation measure is a feature that compensates for other, privacy intrusive aspects of a design. A mitigation measure may compensate partially or wholly for a negative impact. Examples include:

- Minimisation of personal data retention by not recording it, or destroying it as soon as the transaction for which it is needed is completed;
- Destruction schedules for personal information, which are audited and enforced;
- Limits on use of information for a very specific purpose, with strong legal, organisational and technical safeguards preventing its application to any other purpose;
- Design, implementation and resourcing of a responsive complaints-handling system, backed by serious sanctions and enforcement powers.

Under some circumstances it may be appropriate to recognise and accept the privacy risk where the likelihood of it being realised or the impact would be low. However, this must be carefully considered, and must not be done simply as an alternative to taking action.

Recommendation and approval

Having completed the consultation, legal compliance checks and risk analysis, you should be in a position to clearly set out the options and to make a recommendation about how best to proceed. If significant risks remain, you should explain what the problems are and why the stakeholder consultation failed to resolve them. In extreme cases, your recommendation may be that the project needs to be re-thought because there is no viable solution that does not present an unacceptably high risk to the privacy of individuals.

If the Privacy Impact Assessment is part of a project, it is likely that the recommended way forward will be set out for approval in the Outline Business Case. For Privacy Impact Assessments not linked to projects, approval is likely to rest with the Information Custodian.

Implementation and readiness for service

Once the Business Case has been approved you should be ready to implement the agreed solution. This stage may involve procurement of an IT system and the subsequent detailed design and build stages. It is important to ensure throughout these stages that the mitigating and/or avoiding measures that were worked up during the Privacy Impact Assessment are carried through into implementation.

And finally, before going live, you should double-check that these measures are working in the way intended, and that the final system or process does still comply with privacy laws. If not, you may need to go back a stage to see whether the approved solution has been implemented correctly.

Review or audit

As you close the Privacy Impact Assessment you should consider when it will be reviewed and how the review will be carried out.

The purpose of a review or audit is to ensure that the measures introduced as part of the Privacy Impact Assessment are working effectively. It is expected that such a review, particularly in the case of major Privacy Impact Assessments, will be carried out as part of the wider review into the effectiveness of the project or programme deliverables. For smaller Privacy Impact Assessments, the review or audit may be carried out as a stand alone process and be undertaken by internal audit. Either way, upon completion of the Privacy Impact Assessment you should record how this review will be carried out, by whom, and when.

Publication

Where to publish

If the privacy issues relates to Members of the public/service users it is expected that the Privacy Impact Assessment will be published in accordance with the Council's Freedom of Information Act publication scheme. Publication does not necessarily mean the full document – see 'what to publish' below.

When it relates only to information about staff it should be published internally – with the same constraints.

When to publish

As the Privacy Impact Assessment remains 'live' throughout the lifecycle of the project, it won't be complete until the project is closed. Therefore, the time to publish the report is shortly after project closure. Prompt publication will feed the public appetite for the information while the issue is still topical, and reduce subsequent Freedom of Information requests.

What to publish

There may be parts of a Privacy Impact Assessment report that should not be published. This could be because they would disclose information that:

- Could prejudice security;
- Contains legal advice;
- Was provided by a third party in confidence;
- Is personal information about staff and stakeholders who would not expect their information to be made public.

In determining what should not be published, you should apply the "Freedom of Information test". This means considering whether the information would be subject to exemptions if a request was made for it under Freedom of Information, and, if those exemptions are subject to a public interest test, whether it would be in the public interest to disclose the information. The presumption should always be in favour of openness. If no Freedom of Information exemptions are relevant then the Privacy Impact Assessment can be published in full.