Office of the Information Commissioner
Queensland

Applying the legislation

GUIDELINE *Information Privacy Act 2009*

Undertaking a Privacy Impact Assessment

A Privacy Impact Assessment (**PIA**) is a scalable tool agencies can use to:

- identify the impact that a project[1] might have on the privacy of an individual's personal information; and
- make recommendations on how to manage any negative impacts.

This guideline[2] sets out the key steps involved in a PIA and what each of those steps involves. A PIA report template is also available for agencies and health agencies to tailor as necessary to meet the needs of the project and the agency. A one page summary[3] of the key steps is also available.

Tip: Integrating a PIA process with project management

The PIA process can be easily integrated with an agency's approach to project management – for example, by:

- including resourcing and timeframes for the PIA in the project plan
- including updates on the progress of the PIA in status reports or end stage reports
- using the project's risk matrix to analyse the likelihood, consequence and rating of privacy impacts
- recording privacy impacts in the project's risk register/log; and
- capturing the actions that need to be undertaken to implement the recommendations of the PIA in the project plan or stage plan.

Why should I do a PIA?

An agency that undertakes a PIA will:

- check whether a project is likely to comply with the *Information Privacy Act 2009* (Qld) (**IP Act**)
- support good governance and informed decision-making

[1] This guideline uses the term 'project' broadly. It is intended to cover the full range of activities and initiatives that may have privacy implications, such as new systems, processes or practices for handling personal information, new legislation or policies or an information sharing initiative.
[2] In developing this guideline, the Office of the Information Commissioner gratefully acknowledges resources published by the Office of the Australian Information Commissioner, the Privacy Commissioner's Office, New Zealand and the Office of the Commissioner for Privacy and Data Protection, Victoria.
[3] Accessible at https://www.oic.qld.gov.au/__data/assets/pdf_file/0009/26568/overview-of-the-pia-process.pdf

- identify problems early when it is easier and cheaper to address them; and
- address community concerns and build trust in the agency's information handling practices.

It is not mandatory under the IP Act to conduct a PIA. However, the Office of the Information Commissioner (**OIC**) strongly encourages PIAs as part of taking a 'privacy by design' approach and making privacy a key consideration in the early stages of a project and throughout its lifecycle.

OIC does not have a role in endorsing or approving a PIA. We can give you advice on conducting a PIA or provide feedback on a draft PIA report[4], however we recommend that you consult with your agency's privacy officer in the first instance.

When should I do the PIA?

A PIA should be undertaken early enough in the development of a project so that its findings can influence the design of the project. This will prevent unnecessary effort being expended on design options that are not compliant with the IP Act.

Tip: Build PIA checkpoints into your project plan

Projects are rarely static – specifications become further defined or changes are needed to address identified issues. Build one or more PIA checkpoints into the project plan as a trigger to check whether anything significant has changed since you did the PIA. If it has, slot that information into a new version of the PIA, and repeat the process to check whether there are new impacts that need to be addressed.

How to do a PIA

A PIA process generally involves the following steps:

1. Conduct a threshold assessment
2. Plan the PIA
3. Describe the project
4. Identify and consult with stakeholders
5. Map the personal information flow

[4] The PIA report template for health agencies includes a section on analysing the proposed information handling practices against the confidentiality obligations set out in part 7 of the *Hospital and Health Boards Act 2011* (Qld) (HHB Act) and was developed in collaboration with the Department of Health. OIC is unable to provide advice on the interpretation of the HHB Act. For projects, information and statewide initiatives relating to the Department of Health, please consult with the Privacy and RTI Unit, Department of Health via RTI-Privacy@health.qld.gov.au. For projects or information relating to the HHSs, please contact the relevant HHS' Privacy and Confidentiality Contact Officer at https://www.health.qld.gov.au/system-governance/contact-us/access-info/privacy-contacts.

6. Identify the privacy risks
7. Identify options to address the privacy risks
8. Produce a PIA report; and
9. Respond and review.

Each step is explained in more detail below.

Step 1: Conduct a threshold assessment

A PIA will be beneficial for any project that involves new or changed ways of handling personal information. However, not every project will need a PIA. For example, a PIA will not be necessary if the project will not handle any personal information or the project does not propose any changes to existing information handling practices (and where the privacy impacts of these practices have been assessed previously and found to be appropriate).

Ask yourself: 'Will any personal information be collected, stored, used or disclosed in the project?' If the answer is 'yes' then you will generally need to complete some form of PIA.

If you are unsure, our Threshold Privacy assessment tool sets out questions that you can use to determine whether your project needs a PIA.

Regardless of whether you proceed to a PIA, you should keep a record of the threshold assessment to document your decision.

Step 2: Plan the PIA

After you have completed your threshold assessment, you can start planning how you are going to undertake your PIA. When planning your PIA, you should consider:

- what aspects of the project will be assessed
- where the PIA will fit in the overall project plan and timeframes
- who will conduct the PIA and what resourcing is available
- the extent and timing of stakeholder consultations; and
- the steps that will need to be taken after the PIA, such as implementation of recommendations and arrangements for ongoing monitoring.

Tip: How detailed should the PIA process be?

How detailed a PIA needs to be will depend on the scale and complexity of the project. For simple projects, the PIA process can be quick and the PIA report may end up being only a couple of pages. Complex projects will be a more formal and intensive exercise. The level of detail will be influenced by:

- the nature of the personal information involved in the project
- whether new or innovative technology will be used to collect or store the information
- whether the provision of personal information will be mandatory
- whether the project involves data-matching
- whether information will be shared with another agency; and/or
- the likely community and/or media interest in the project.

You don't need to be a privacy specialist to conduct a PIA. However, it is helpful to seek input from someone who is familiar with the IP Act, such as your agency's privacy contact officer or legal services area. Further guidance on who else might provide input to the PIA process is set out in Step 4: Identify and consult with stakeholders.

Step 3: Describe the project

Having a clear understanding of what the project intends to achieve provides context for the rest of the PIA process. There is often more than one way of designing a project to deliver the intended aim – a PIA will help identify the most privacy respectful way of achieving that aim.

This information could include:

- who is responsible for the project
- what the project will deliver
- what it will achieve
- the benefits to the agency or the community; and
- whether the project is part of a program of related projects.

This information can typically be sourced from the project's management documentation, such as the Project Brief or Business Case.

Step 4: Identify and consult with stakeholders

Consultation with stakeholders who will be affected by the project, or who have an interest in the project, is essential to the PIA process as it allows people to identify privacy impacts and solutions based on their experience or expertise. Who you should consult will depend on the nature of the project, but may include:

- internal stakeholders - such as information technology, privacy, legal, procurement and records management business areas, as well as the customer-facing staff who will use the new system or put the new policy into practice; and
- external stakeholders – such as other government agencies, suppliers, clients[5], non-government organisations, advocacy groups, and members of the public.

[5] For some projects, the clients may be the agency's employees.

Consultation is not necessarily a separate step - it can be useful to consult throughout the PIA process.

Involving internal stakeholders in the PIA process is critical as these are the people who can answer questions about likely information flows, governance structures, technical architecture, legislation under which the agency operates and recordkeeping requirements. They may also be able to suggest potential actions to address the identified privacy issues or provide advice on what option is the most appropriate.

External consultation often involves seeking the views of the people whose personal information will be affected by the project. There are two main aims: it enables the agency to understand the concerns of those individuals and improves transparency by making people aware of how their personal information will be used.

Factors that will influence how extensive the consultation needs to be are whether there is:

- likely to be concern about actual or perceived impact on privacy
- a large number of people or a particularly vulnerable group whose privacy is affected
- vulnerability of any personal information holdings to misuse or abuse; and/or
- a need to build trust in a new practice or technology.

Even if a broad public consultation is not warranted, it may be that some form of targeted consultation should be undertaken, such as with relevant government independent statutory bodies, advocacy groups or professional associations.

Tip: Effective consultation

Effective consultations should follow these principles:

- Timely – at the right stage and allow enough time for responses.
- Clear and proportionate – in scope and focused.
- Representative – ensure those likely to be affected have a voice.
- Asks objective questions and present realistic options.
- Ensure that those participating get feedback at the end of the process.[6]

[6] Information Commissioner's Office (UK), Conducting privacy impact assessment code of practice, Version 1.0, viewable at https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

Step 5: Map the personal information flow

The next step is to describe what personal information is involved in the project and how it will flow through the agency's systems and processes as a result of the output or deliverable to be produced by the project.

Clearly mapped information flows will assist you to identify privacy impacts in the next step of the PIA process.

The 'map' of personal information flows should include:

- what personal information will be collected, its source and how it will be collected
- how it will be stored, what safeguards will be in place and who will have access to it
- what the personal information will be used for and by whom
- whether the personal information will be routinely disclosed and if so, to whom will it be given and for what purpose
- how individuals will be able to access and amend their personal information; and
- how long the information will be retained.

Keep in mind that personal information includes any information or opinion about a living individual who is or can reasonably be identified[7].

There is no 'one size fits all' approach to documenting the flow of information. For example, you could use tables to set out the key information for different types of personal information to be used in the project. A diagram or business process map can be effective, especially if you wish to show the current process or system and how the project will change those systems or processes. The method you decide to use will depend on the complexity of the information flows in your project.

It can also be helpful to create two information maps – one to describe the current personal information environment and another showing the changes to be delivered by the project.

Step 6: Identify the privacy impacts

A privacy impact can be negative (a risk) or positive (an opportunity). While this section focuses on identifying and mitigating risks, you could use a similar analysis to identify and maximise opportunities.

[7] Whether information is about a 'reasonably' identifiable individual requires case-by-case consideration of factors such as the nature and amount of information, who will have access to the information and other information that is available and the practicability of using that information to cross-match or link the information held by the agency to an individual.

To identify privacy risks, you need to check the project's handling of personal information against the privacy principles:

- Information Privacy Principles – if the agency is not a health agency, or
- National Privacy Principles – if the agency is a health agency; and
- the rules about transfer of personal information outside Australia[8] – which apply to all agencies; and
- the requirement to take all reasonable steps to bind contracted service providers to the privacy principles[9] - which applies to all agencies.

In addition to compliance with the IP Act, you should also consider:

- whether the project is subject to other legislation[10] that contains confidentiality or secrecy provisions; and
- the community's expectations of privacy.

Tip: Community expectations of privacy

Even where an act or practice does not contravene the privacy principles, individuals may be uncomfortable with the collection or use of their information for particular purposes. For example, an individual may expect that information about them is collected directly from them rather than a third party, or an individual may not agree that the act or practice is 'reasonable'.11 Consultation with the community is a key way to find out whether the project is seen as privacy-intrusive.

The PIA report template includes questions to help you identify potential privacy impacts. Not all questions will be relevant to every project. Equally, you may need to consider additional questions to reflect the nature of your project and your agency.

Tip: Recording privacy risks

Recording privacy risks in the project risk register/log helps ensure accurate reporting to the Project Executive/Steering Committee/senior management. It will also help ensure that actions needed to address the risk can be tracked and prioritised appropriately.

[8] Section 33 of the IP Act.
[9] Chapter 2, part 4 of the IP Act.
[10] For example, the *Invasion of Privacy Act 1971* (Qld) or an agency's enabling legislation such as the *Hospital and Health Boards Act 2011* or *Child Protection Act 1999* (Qld).
[11] A number of privacy principles contain the word 'reasonable' or 'reasonably' to qualify a test or obligation.

Step 7: Identify options to address the privacy risks

You now need to consider what action can be taken to address the identified privacy risks. Where there are multiple options for addressing a privacy issue, you may need to evaluate the costs, risks and benefits of each option to identify which option is the most appropriate.

Options for addressing privacy issues include:

- operational controls – such as policies and procedures, staff training or communication strategies (e.g. a collection notice)
- technical controls – such as access controls, encryption and design changes; and
- physical controls – such as doors or locks.

Tip: Dealing with risk

Using a risk matrix[12] helps prioritise risks according to how likely it is that the risk will materialise and the severity of its potential consequence. It is important to note that while identifying and mitigating privacy risks is a critical component of good privacy practice, risk mitigation does not provide an alternative to compliance with the privacy principles. Privacy needs to be incorporated with other project goals such as functionality; not balanced against them.

If it is not possible to mitigate a privacy risk, you could seek a waiver or modification of the agency's obligation to comply with the privacy principles[13]. Approval is only granted where the public interest in non-compliance is stronger than the public interest in compliance.

Step 8: Produce a PIA report

The next step is to prepare a report for approval by the Project Executive/Steering Committee/senior management. The report should at a minimum:

- describe the information flows involved in the project
- provide a summary of the analysis against the privacy principles to show what the privacy impacts are (both positive and negative)
- recommendations to remove or mitigate privacy risks
- set out what consultation processes were undertaken; and

[12] For more information on the risk management process, please see Queensland Treasury's – A Guide to Risk Management, accessible at https://www.treasury.qld.gov.au/resource/guide-risk-management/.

[13] See OIC Guideline: Public interest approvals: Power of the Information Commissioner to waive or modify the privacy principles, accessible at https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/power-of-the-information-commissioner-to-waive-or-modify-the-privacy-principles.

- identify whether the PIA should be reviewed during the project.

A PIA report template is available – one for agencies other than health agency and another specific to health agencies – for you to use as a starting point and edit as necessary.

Step 9: Respond and review

It is important that actions are taken to implement the recommendations made in the report, and to continue to review and update the PIA, even after the project's completion.

The first step is to document what the Project Executive/Steering Committee/senior management agreed to, that is:

- what recommendations will be implemented (or are already implemented); and
- any recommendations that will not be implemented, and the rationale for this decision.

It can often be helpful to prepare a plan for implementing the recommendations to record what actions need to be taken, timeframes and responsibilities. Alternatively, you could integrate the agreed recommendations into a revised project plan as this will help ensure that the activities necessary to implement the recommendations are managed and reported.

Hint

Publishing a PIA report and the agency's response to the recommendations demonstrates a commitment to openness and transparency and that the project has been designed with privacy in mind. If detailed information about the project cannot be published due to security or commercial concerns, consider publishing a summary or redacted version of the PIA report.

A PIA report is a living document. It should be revisited and updated if changes to the design of the project create new privacy impacts that were not previously considered.

Similarly, a PIA does not end on delivery of the project. Reassessing the privacy impacts of the system or process after it is in operation, for example when updates are deployed or new features are released, will help ensure that the agency continues to approach privacy as a 'design feature' of its processes and activities.

For additional information and assistance please refer to and the OIC's guidelines, or contact the Enquiries Service on 07 3234 7373 or email enquiries@oic.qld.gov.au.

This guide is introductory only, and deals with issues in a general way. It is not legal advice. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

If you have any comments or suggestions on the content of this document, please submit them to feedback@oic.qld.gov.au.

Published 16 September 2014 and Last Updated 25 July 2018

Changes to legislation after the update date are not included in this document