Office of the Information Commissioner
Queensland

IPOLA

IPOLA GUIDELINE

Applying the legislation – Information Privacy Act 2009

Undertaking a Privacy Impact Assessment

This guide does not reflect the current law.

It highlights important changes to the *Information Privacy Act 2009*.

This guide does not constitute legal advice and is general in nature only. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

1.0 Overview

Queensland government agencies[1] are required to handle personal information in accordance with the Queensland Privacy Principles (**QPPs**) and overseas disclosure rules (**section 33**) in the *Information Privacy Act 2009* (Qld) (**IP Act**). A key part of meeting these obligations is assessing the privacy impacts of policies, projects, and other agency undertakings.

2.0 What is personal information

Personal information is any information about an identified individual or an individual who can be identified. The QPPs and section 33 of the IP Act apply to personal information generally, but there is also a subset of personal information called sensitive information which has its own special rules.

Refer to ***Key privacy concepts – personal and sensitive information*** for more information.

3.0 Privacy impact assessments

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

- whether a project will involve personal information or sensitive information
- the project's potential impact on individual privacy

[1] Agency include a Minister and bound contracted service provider, or other entity required to comply with the IP Act.

- whether the project's proposed collection, use, and disclosure of personal information will comply with the QPPs and section 33; and
- risks of, and mitigation strategies for, any potential negative impacts.

Project is used broadly in this guideline[2] to refer to the full range of agency activities and initiatives which could have privacy implications, e.g. new systems, processes or practices, new legislation or policies, or information sharing initiatives.

In addition to this guideline, which sets out important steps in the PIA process, agencies may find ***existing PIA resources*** useful. PIA resources will be updated to align with IPOLA changes (under development).

3.1 Integrating the PIA with project management

Integrating the PIA process into the agency's project management systems and processes can create efficiencies and help ensure privacy impacts are considered early on a throughout the life of a project.

This can be done, 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.

3.2 Why a PIA is important

The IP Act does not require a PIA, however the Office of the Information Commissioner (**OIC**) strongly encourages PIAs as part of a privacy by design approach. Including privacy as a key consideration in the early stages of a project and throughout its lifecycle significantly reduces the risk of noncompliance.

A PIA:

- assesses whether a project complies with the QPPs and section 33
- supports good governance and informed decision making
- allows potential problems and risks to be identified early, when addressing the is easier and cheaper; and
- recognises and addresses community privacy concerns, which can build trust in the agency's information handling practices.

[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.

3.3 When should the PIA be conducted

A PIA should be undertaken early enough in the development of a project that its findings can influence the design of the project. This will prevent unnecessary effort being expended on noncompliant design options.

3.4 PIA checkpoints

Projects are rarely static; specifications are redefined or changed as it progresses. Building one or more PIA checkpoints into the project plan, as a trigger to check whether anything significant has changed since the PIA was first conducted, will help ensure the privacy impacts of project changes are addressed.

4.0 How to conduct a PIA

A PIA generally involves the following steps:

1. Threshold assessment.
2. Plan the PIA.
3. Describe the project.
4. Identify and consult with stakeholders.
5. Map the personal information flow.
6. Identify the privacy risks.
7. Identify options to address the privacy risks.
8. Produce a PIA report; and
9. Respond and review.

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 involve personal information or does not propose any changes to existing information handling practices (where the privacy impacts of these practices have previously been assessed previously and deemed appropriate).

If the answer to: 'Will any personal information be collected, stored, used or disclosed in the project?' is yes, some form of PIA will generally be required. ***Threshold privacy assessment form*** *(under development)* may be helpful in making this determination.

Keeping a record of the threshold assessment is an important part of documenting the PIA decision.

Step 2: Plan the PIA

If the threshold assessment indicates a PIA is required, the next step is to plan the PIA. 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.

The PIA does not need to be conducted by a privacy specialist, but it is important to seek input from your agency's privacy officer or other officer familiar with the IP Act.

In addition to this guideline, which sets out important steps in the PIA process, agencies may find ***existing PIA resources*** useful. PIA resources will be updated to align with IPOLA changes (under development).

4.1.1 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 be quite short. Complex projects will involve 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.

Step 3: Describe the project

Having a clear understanding of the project's purpose and outcomes will provide context for the PIA process. There is often more than one way of designing a project to deliver its intended outcome; a PIA will help identify the most privacy compliant way of reaching that outcome.

Relevant 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. 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 the information technology, privacy, legal, procurement and records management business areas, customer facing staff who will put the project into practice, and employees whose privacy may be impacted by the project; and
- external stakeholders – such as other government agencies, suppliers, clients, non-government organisations, advocacy groups, and members of the public.

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 involved in the project and its outcomes.

Factors that will influence the required extensiveness of consultation include 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
- a 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.

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.

Step 5: Map the personal information flow

The next step is to describe the personal information is involved in the project and how it will flow through the agency's systems and processes as a result of the project's outcome.

Clearly mapped information flows will assist in identifying 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 and from whom it will be collected
- whether any of the personal information is sensitive information
- how it will be stored, its security safeguards, 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
- whether the personal information will be disclosed out of Australia
- how individuals will be able to access and amend their personal information; and
- how long the information will be retained., and protocols for deidentifying or disposing of personal information consistent with relevant QPPs/statutory retention/public records obligations.

There is no *'one size fits all'* approach to documenting the flow of information. For example, you could use tables to describe the different kinds of personal information involved in the project and how it will flow. A diagram, business process map, or comparative information map may be effective, especially to show how current processes or systems will be change by the project,

The best method will depend on the complexity of the information flows in your 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, a similar analysis can be used to identify and maximise opportunities.

Privacy risks are identified by checking the project's handling of personal information against the QPPs and section 33. If the project or its outcomes will involve contractors, it must also be checked against the requirement in chapter 2, part 3 to take bind contracted service providers to the IP Act.

Agencies should also ensure that the project allows noncompliance to be identified, in order to meet its mandatory data breach obligations in chapter 3A of the IP Act.

Refer to ***existing PIA resources*** and PIA resources updated for IPOLA (under development) for further information.

The ***PIA report template*** (under development) includes questions to help identify potential privacy impacts. Not all questions will be relevant to every project and additional considerations may be required, depending on the nature of your project and your agency.

Confidentiality and human rights obligations

A PIA can also be used to measure the project's compliance with:

- legislative confidentiality or secrecy obligations
- non-legislative confidentiality obligations; and
- the *Human Rights Act 2019* (Qld), particularly the right to privacy.

4.1.2 Community expectations of privacy

Even where an act or practice complies with the IP Act, individuals may be uncomfortable with their information being involved in the act or practice. Consultation with the community is a key way to assess whether a project is seen as privacy-intrusive.

4.1.3 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.

Step 7: Identify options to address the privacy risks

If privacy risks have been identified, they must be addressed. If there are multiple options for addressing the risk, it may be necessary to evaluate the costs, risks and benefits of each option to identify which is the most appropriate.

Options for addressing privacy issues include:

- operational controls – such as policies and procedures, staff training or communication strategies
- technical controls – such as access controls, encryption and design changes; and
- physical controls – such as doors or locks.

Refer to ***Minimising privacy risks*** (under development) for more information.

Dealing with risk

Using a risk matrix[3] helps prioritise risks according to their likelihood and potential severity.

While identifying and mitigating privacy risks is a critical component of good privacy practice, risk mitigation does not provide an alternative to IP Act compliance. Privacy must be incorporated into project goals, not balanced against them.

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

Refer to *QPP codes and* privacy *waivers* for more information.

Step 8: Produce a PIA report

The next step is to prepare a report for the approval of 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
- identify whether the PIA should be reviewed during the project.

Refer to ***existing PIA resources*** and PIA resources updated for IPOLA (under development) for further information.

[3] 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/.

Step 9: Respond and review

It is important that recommendations made in the report are implemented and that the PIA is updated and reviewed, even after the project's completion.

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

- 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, they could be integrated into a revised project plan, which will help ensure the activities necessary to implement the recommendations are managed and reported.

Publishing the PIA report

Publishing a PIA report and the agency's response 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 IPOLA assistance, please contact the IPOLA team by email IPOLA.Project@oic.qld.gov.au

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

Published October 2024 and Last Updated 8 October 2024