The independent regulator fostering trust and accountability in WA through privacy and freedom of information.

Guidance for IPP Entities

How to do a Privacy Impact Assessment

Office of the Information Commissioner
Western Australia

Publication date: 29/10/26

Version Control: 1.0

Table of contents

	Page
Overview	2
Elements of a PIA	2
Project description	3
Consultation	4
Map information flows	6
Privacy risk analysis	8
Recommendations	13
Report	13
Review	14
References	15

How to do a Privacy Impact Assessment

Overview

The *Privacy and Responsible Information Sharing Act 2024 (WA)* (PRIS Act) requires Western Australian public sector entities and their contracted service providers (called IPP entities) to undertake a Privacy Impact Assessment (PIA) in certain circumstances.

The purpose of this resource is to explain how to conduct a PIA.

This is the final resource in a suite of three resources designed to guide IPP entities through why, whether and how to conduct a PIA:

1. **WHY:** Introduction to PIAs
2. **WHETHER:** Do I need to do a PIA?
3. **HOW:** How to do a PIA

These resources should be read together. They are available on the Office of the Information Commissioner Western Australia's (OIC WA) website.

Elements of a PIA

A PIA is a flexible process that should be proportionate to the nature, scope and complexity of the project being assessed. Whilst the form and level of detail of each PIA can vary, the following steps should form part of every PIA:

1. **Describe the project** – describe the project's purpose, scope and context
2. **Consult with stakeholders** – identify and consult with relevant stakeholders and incorporate any feedback
3. **Map information flows** – map how personal information flows through the project
4. **Analyse the privacy risks** – identify any privacy risks and how the project meets or does not meet the requirements of the PRIS Act
5. **Make recommendations** – make recommendations about how to eliminate, reduce or manage the identified privacy risks
6. **Draft the PIA report** – draft the PIA report
7. **Review the PIA** – review the PIA at key points in the project lifecycle or where there is a change resulting in increased privacy risks



A PIA is not a strictly linear process. Steps may overlap, occur concurrently or need to be revisited as a project develops or new information becomes available. Accordingly, an IPP entity should consider whether the order of the steps is appropriate for the project and how they fit within the IPP entity's existing project management lifecycle.

Project description

The project description should provide a broad overview of the project, including a clear description of its purpose, scope and context.

Someone without specialised knowledge in the area (including people external to the entity) should be able to pick up the PIA and understand the project from the description. Be mindful to keep the language accessible and explain any technical terms.

Remember, the purpose of a PIA is to assess the risks involved in handling personal information. Therefore, the description should highlight where personal information is involved.



Don't include any analysis of the privacy impacts in the project description, this will be performed later in the PIA process.

Purpose

The description must clearly set out the purpose of the project. In other words, what are the goals of the project and how the IPP entity will measure success. It should be clear how the handling of personal information contributes to those goals.

If the expected benefits of the project aren't clear, it will be difficult to assess whether any privacy impacts are proportionate to the benefits of the project and, therefore, whether the privacy risks have been appropriately managed.

Scope

A PIA must have a clear scope. This ensures it is clear what the PIA covers and what it does not cover.

The scope will depend on:

- the stage of development of the project (for example, is it a pilot or a full-scale implementation)
- the nature and extent of the personal information handling involved, and
- any connection with other systems or projects.

Where a project is completed in stages, it will be important to identify clearly what stages the PIA covers and when it will be reviewed. For example, if the PIA only covers the pilot stage of the project, it should be reviewed before a decision is made about whether to approve an expanded or full-scale implementation.

The scope of the PIA will impact how effectively privacy risks can be identified. If the scope is defined too narrowly, significant privacy impacts may be overlooked.

Example 1 – Scope of the PIA defined too narrowly

A Department plans to implement a new cloud-based enterprise platform. The platform is a low-code software-as-a-service solution designed to automate a range of internal workflows (Workflow Engine). The business case states:

> *"Workflow Engine can be used to support a broad range of business purposes, including managing IT service desk requests, project management workflows and executive dashboarding and approvals. Given the platform's highly configurable design, new applications can be built at speed to meet changing business needs."*

The Department conducts a PIA on Workflow Engine, but the PIA does not consider the separate business applications. A separate PIA is not completed each time a new business application is built on the platform, and the original PIA is not updated to cover the expanded use case. As a result, the

PIA does not consider the full range of personal information processed by Workflow Engine, or the full range of purposes for which that information is used.

Five years later, the third-party provider of Workflow Engine is the victim of a cyber-attack resulting in the unauthorised disclosure of personal information stored within the platform. An investigation into the incident reveals that Workflow Engine was being used to manage employee travel arrangements, which involved the collection and storage of employee health and identity information. Further, the investigation revealed that this information should not have been collected and stored in Workflow Engine (as it was already held in the Department's HR system) and the security controls were not commensurate with the level or risk.

Sometimes only a small portion of the project will involve personal information. In these cases, it may be appropriate to define the PIA's scope with reference to only those parts of the project involving the handling of personal information and not to the project as a whole. Where the scope is narrower than the project scope, it will be important to document why the scope is being confined in this way.

Example 2 – Scope of the PIA appropriately defined

A Local Government wants to undertake a road improvement project involving the redesign of several traffic intersections and pedestrian crossings. As part of the project, the Local Government proposes to install CCTV cameras and record footage of the intersections to monitor pedestrian volumes and traffic patterns.

In this situation, the Local Government has done a privacy threshold assessment and identified the use of CCTV is the only part of the project involving the handling of personal information. Therefore, the Local Government decides to limit the scope of the PIA to that activity, and not to the road improvement project as a whole. The reasons for the decision are documented in the privacy threshold assessment and included as an attachment to the PIA.

Context

The description of the project should include information about the context of the project. This should include a description of both internal and external factors that may be relevant when assessing the privacy impacts of the project.

Relevant factors may include:

- how the project fits within the IPP entity's broader strategy and objectives
- whether the project links to any other projects, and any key dependencies
- whether the IPP entity or the relevant business area has any relevant previous experience, including experience handling similar types of personal information for similar purposes
- the nature of the IPP entity's relationship with the individuals' whose personal information will be handled
- the nature of the IPP entity's relationship with any contracted service providers or third-party vendors who are involved in the project, and
- whether the project is of public interest.

Consultation

Consultation is an important step in the PIA process. Stakeholders may be better placed to identify privacy impacts, suggest appropriate mitigation strategies or otherwise inform the recommendations. Consultation can also help build community trust and confidence the privacy risks are being responsibly managed.

The appropriate level of consultation will not be the same for every project. Generally, the greater the assessed privacy impact of the project, the more consultation required.

The method for undertaking consultation should be tailored to the circumstances. Productive consultation involves stakeholders being able to actively contribute their perspectives, including their views on any potential privacy impacts and appropriate mitigation actions.

Timing is an important consideration when undertaking consultation. Consultation must be undertaken early enough in the project lifecycle to ensure the results can influence the design of the project. If a stakeholder needs to be consulted later in the PIA process, the IPP entity may need to revise its expected timeline to ensure it can sufficiently incorporate any feedback.

When considering who to consult with, start by identifying the people or groups who may be affected by, or otherwise have an interest in, the project. This might include:

- Internal staff or business areas – this is most important when the project is internal only.
- The individuals' whose personal information will be handled as part of the project – this can provide insights into individuals' expectations, and any privacy impacts not yet considered.
- The public generally – this is especially relevant where the project may have a community impact or where public sentiment in relation to the project is not well understood.
- Advocacy organisations and community leaders – this can provide insight into relevant social issues and help the IPP entity understand the privacy impacts in relation to vulnerable groups of people. This is especially important when the project involves the personal information of individuals from culturally and linguistically diverse backgrounds.
- Industry experts or academics – this is especially important when the IPP entity does not have the necessary in-house expertise to effectively assess the project and any associated privacy risks.
- Other IPP entities and interstate counterparts – this is particularly important when personal information will be disclosed across entities.

Input from contracted service providers and third-party vendors

Where a project involves a contracted service provider or a third-party vendor it will be important to seek their input when completing the PIA.

For example:

- Where a project involves the implementation of a third-party product, it may be necessary to seek a detailed explanation of how the product works and the extent to which the product might be configured to support privacy.
- Where a project involves a third-party having access to or receiving personal information, it will be necessary to understand what controls the third-party has implemented to prevent misuse and unauthorised access or disclosure of the personal information.



A PIA should not be a siloed activity. It may overlap with other important steps in the project lifecycle, such as vendor risk assessments and cyber-security assessments.

The PIA does not need to duplicate the work of other assessments, but it should be clear how the outcomes of those other assessments have been incorporated into the PIA analysis and informed the final recommendations. For more information see the section of this guidance titled "Integrating a PIA with other assessments".

Map information flows

Mapping the information flows helps an IPP entity understand the project through a privacy lens.

The map of information flows is a factual description of the way personal information will be handled throughout the project. The map of information flows should be set out in a structured format and address how personal information is handled at each stage of the information lifecycle, from collection through to destruction or de-identification.

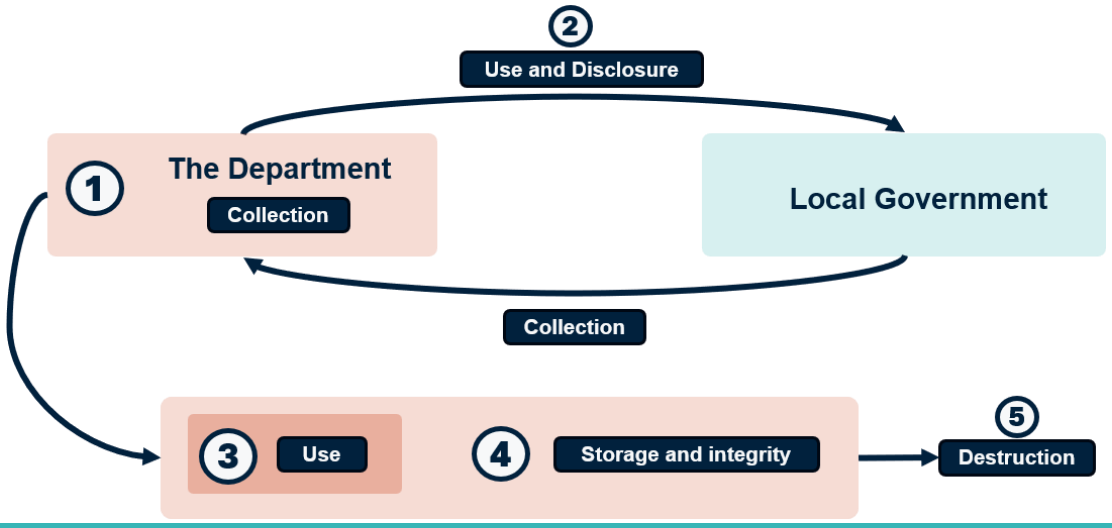
Stage of the information lifecycle	Describe
Collection	• what personal information will be collected, including what sensitive personal information will be collected (if any) • the types of individuals or groups of individuals whose personal information will be collected • where the personal information will be collected from (for example, collected directly from the individuals or a third party), and • how the personal information will be collected (for example, manually, using an online form or using other technology tools).
Use	• how the personal information will be used • whether the personal information will be used for different purposes by different business areas • whether the personal information will be modified, transformed or combined with other information, and • whether the personal information will be used as part of an automated decision-making process.
Disclosure	• to whom the personal information will be disclosed (for example, third-parties or contracted service providers) • how the personal information is disclosed (for example, what systems are used to transfer the information), and • whether the personal information will be disclosed outside Australia.
Storage and integrity	• where the personal information will be stored, including what systems it will be stored in • the technical, physical or organisational controls applied to protect the personal information, and • who will have access to personal information.
Destruction or de-identification	• how long the personal information will be kept • the procedure for destruction of personal information when it is no longer required, and/or • whether the personal information will be de-identified when it is no longer required.

Information flow diagram

A useful way of mapping the information flow is by using a diagram or table.

Example – Information flow diagram

The Department is doing a PIA for a project piloting the use of a new online permit application system. The new system includes an online portal and AI functionality that can be used to summarise applications. The approving officer at the Department will use the AI generated summaries to assist them in making a decision about which individuals will be granted a permit. The Department maps the information flows:



1 Collection

The applicant uses an online form available on the Department's website to submit their application.

The Department collects the following personal information directly from individuals using the online form:

- contact details, including name, address, phone number and email address
- permit application details (the information flow should list the different types of personal information included in the application)

2 Use and Disclosure

The Department discloses the names and contact details of applicants to the relevant Local Government (identified using the individual's address) for the purpose of determining whether or not the individual has any existing permits or any other information relevant to the application.

The Local Government conducts a search and provides the Department with relevant results (this is a collection by the Department).

All correspondence between the Department and the Local Government is conducted via email.

3 Use

The Department combines the permit application details and the Local Government search results with information they already hold about the applicant.

The approving officer uses AI to summarise the available information according to the criteria relevant for assessing the permit application. The approving officer then uses these summaries to assist in making a decision about the application.

4 Storage and integrity

The online application forms and related information are saved to a folder in the Department's electronic document and records management system ("eData").

The AI system operates within the Department's enterprise environment. No information inputted into the AI system leaves the Department's environment.

The folders in eData that relate to permit applications have access controls limiting access to the relevant administrative and approving officers.

5 Destruction or De-identification

The Department has a retention and disposal authority which requires records relating to decisions about permit applications to be retained for five (5) years after the date of the decision.

Metadata specifying the retention period is automatically applied to each record in eData. The system automatically schedules the destruction of records at the end of this retention period.

Privacy risk analysis

The analysis is the most important part of the PIA. A thorough analysis involves identifying the potential privacy impacts of the project and the likelihood of those impacts occurring (i.e. identifying any privacy risks).

An important step in the analysis is considering how the project meets the requirements of the PRIS Act. However, this should be done with the objective of reducing the risks identified and not as a standalone "checkbox" activity.

The steps in undertaking an analysis are:

1. Identify **privacy risks, and**
2. Assess how the project does or does not meet the requirements of the IPPs (**IPP analysis)**

Privacy risks

A PIA seeks to identify privacy risks and form a view about the severity of the impact and the likelihood it will be realised. In some cases, a PIA might also be used to highlight the positive privacy aspects of a project.

If a Privacy Threshold Assessment has been completed for the project, the privacy impacts identified as part of that process should be the starting point of the analysis.

Risk identification should not be limited to an assessment of whether a project is compliant with the PRIS Act. This is because the goal of privacy risk management is the prevention of harm, not only compliance with the law. An effective PIA should consider how compliance with the IPPs can help privacy risks (and the associated harm) from being realised.

Privacy risks can arise both when the project goes according to plan and when it doesn't. For example, over collection of personal information can arise when a project goes to plan but hasn't been designed with privacy in mind. In contrast, an information breach usually arises when something goes wrong.

Example 3 - Privacy risks when a project goes to plan

A Department wants to assess whether staff are maintaining productivity whilst working remotely. They decide to pilot a new software to monitor staff activity when working at home by continuously tracking staff computer screens and keystrokes.

Using the new software, the Department is able to successfully measure changes in staff productivity. However, the pilot results in the collection of large amounts of personal information and generates a culture of mistrust that impacts employee morale. In this case, the Department decides that the impact on privacy is disproportionate to the benefits of the software, especially when compared with alternative productivity measures, such as outcome-based metrics.

Privacy risks can also include risks to the IPP entity. For example, an IPP entity might suffer reputational damage or loss of trust if a project doesn't meet community expectations about the handling of personal information. These types of unmanaged privacy risks might mean the project doesn't achieve the anticipated uptake and, therefore, doesn't realise the expected efficiency or financial benefits.

An IPP entity may choose to integrate the assessment of privacy risks into its existing risk management framework. This approach can help ensure that privacy risks are assessed consistently and are subject to the appropriate level of oversight.

IPP analysis

The IPP analysis sets out how the project meets the requirements of the IPPs. The IPPs outline the minimum requirements for handling personal information across each phase of the information lifecycle (see figure 2). Meeting these requirements is an important step in identifying and managing a project's privacy risks.

The IPP analysis should culminate in a prioritised action plan. The action plan is a series of steps the IPP entity will undertake to ensure the project meets the requirements of the PRIS Act and that any privacy risks have been appropriately mitigated. This action plan will be considered at the mitigation and recommendations stage of the PIA, and is usually prioritised to address the highest risks first.

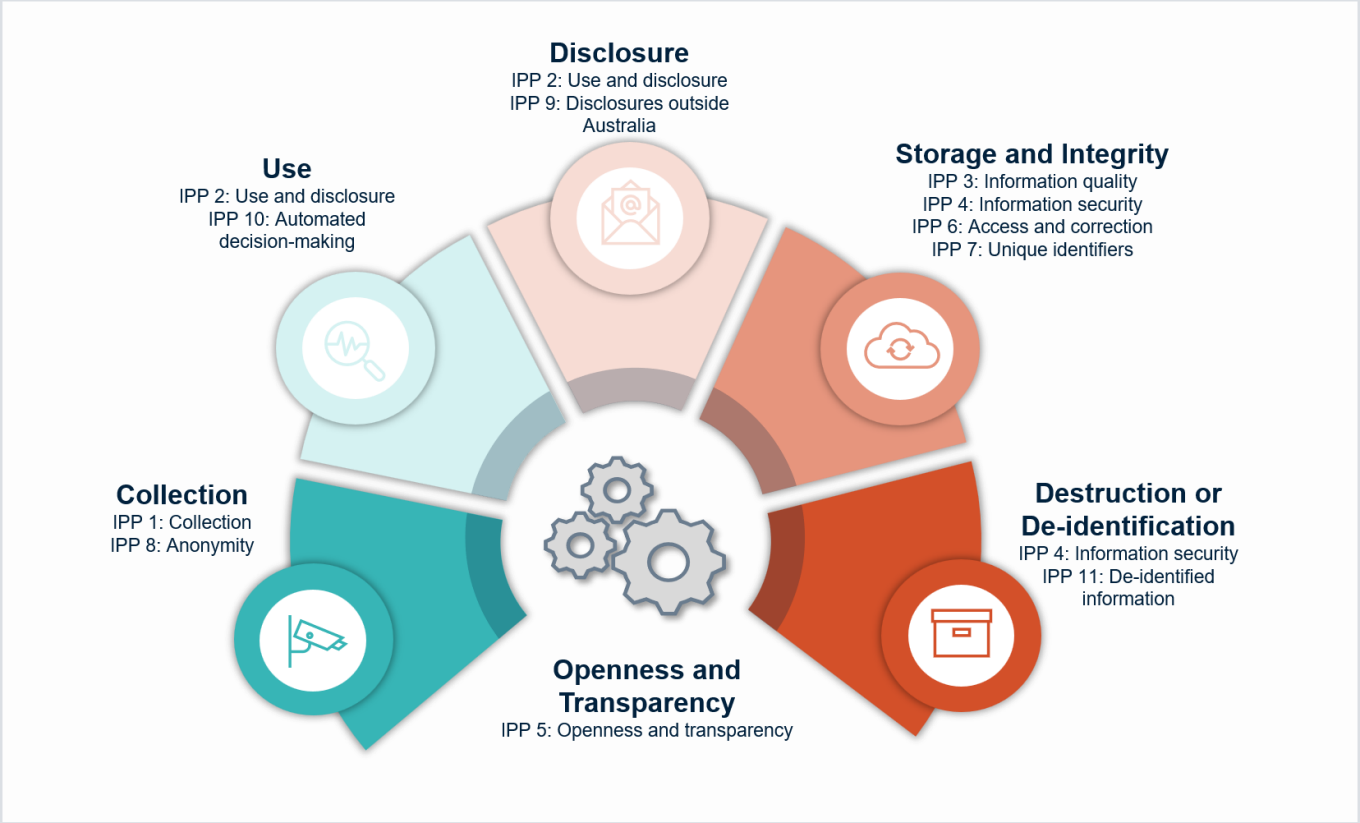


Figure 1 The information lifecycle with IPPs

IPP 1: Collection

An IPP entity must not collect personal information unless it is necessary for their functions or activities.

Wherever possible the project should look for ways to limit the collection of personal information. This is because the best way to manage privacy risks is to not collect the personal information in the first place. Personal information should not be collected on the off chance it might be useful in the future, even if it is easy to collect.

Even when it is necessary to collect personal information, an IPP entity will often still have choices about how to collect it.

Considerations for IPP 1 include:

- whether the amount of personal information collected can be reduced (consider both the volume and the types of personal information)
- whether less specific information can be collected instead (for example, a suburb or postcode instead of a residential address)
- whether the collection is fair and reasonable
- whether the collection can be performed by less intrusive means (for example, is the information being collected covertly, in a way that is disruptive or otherwise out of step with community expectations), and
- whether the individual knows or will be notified their personal information is being collected.

IPP 2: Use and disclosure

An IPP entity can only use and disclose personal information for the purpose it was collected for (the primary purpose), unless an exception applies. The risk of unauthorised use or disclosure of personal information increases where there was no clearly defined or understood purpose when the personal information was first collected.

Considerations for assessing whether the proposed use or disclosure is consistent with the primary purpose, include:

- what individuals were told when the personal information was first collected and whether this is related to the proposed use or disclosure of the personal information
- whether consent is being sought for use or disclosure, and if it is, how the IPP entity will ensure it is voluntary, informed, current, specific and unambiguous
- whether the use or disclosure is fair and reasonable
- whether any laws require or authorise the use or disclosure of the personal information, and
- whether the information is subject to an information sharing agreement under the PRIS Act.

IPP 3: Information quality

An IPP entity must take reasonable steps to make sure the personal information it collects, uses or discloses is correct, complete, and up to date.

Considerations for IPP 3 include:

- what assurance mechanisms will be used in the project to ensure information quality, and
- what mechanisms are available to individuals to update or correct their personal information.

IPP 4: Information security

An IPP entity must take reasonable steps to protect personal information it holds from misuse, loss, unauthorised access, modification, or disclosure.

Considerations with respect to protecting personal information include:

- what technical, physical and organisational security controls protect the personal information from misuse, loss, unauthorised access modification or disclosure having regard to the nature and sensitivity of the information
- whether there are appropriate monitoring processes in place to identify unauthorised system access, data exfiltration or information loss, and
- whether there is a clear procedure in the event of an information breach.

An IPP entity must also take reasonable steps to destroy, or permanently de-identify personal information when it is no longer needed, unless a law requires the IPP entity to keep it. Considerations with respect to destruction or de-identification of personal information include:

- how to identify when personal information is no longer required to be kept, and
- how personal information will be destroyed or de-identified when it is no longer required.

IPP 5: Openness and transparency

An IPP entity must have a publicly available privacy policy that sets out what personal information it collects and holds, and how and why it handles personal information.

Considerations for IPP 5 include:

- whether the proposed handling of personal information is consistent with the IPP entity's existing privacy policy, and
- whether the privacy policy is available to people who want to access it.

IPP 6: Access and correction

Both the PRIS Act and the *Freedom of Information Act 1992* (WA) (FOI Act) provide mechanisms for individuals to seek access to, and correction of, their personal information. Where an agency holds the personal information, an individual may apply for access under the FOI Act. Where a contracted service provider to government (rather than the agency itself) holds the requested information, an individual may request access under IPP 6 of the PRIS Act.

Both the PRIS and FOI Acts require the entity holding the requested information to take reasonable steps to assist an individual to make a valid access application. Importantly, if an access application is made under the wrong legislation, the entity must deal with it under the correct legislation without requiring the individual to re-apply.

Considerations for access and correction include:

- what processes are in place to identify records containing an individual's personal information and provide access, and
- what processes are in place to ensure contracted service providers will notify the outsourcing entity of requests they receive for access or correction of personal information.

IPP 7: Unique identifiers

IPP 7 restricts an IPP entity from assigning, adopting, using, disclosing or requesting a unique identifier, except in certain circumstances.

Limiting the use of unique identifiers is important because excessive use increases the risk of an identifier becoming a universal identifier. Universal identifiers enable personal information to be matched and combined across different entities in ways individuals may not expect, sometimes resulting in large scale tracking bordering on surveillance.

Considerations for IPP 7 include:

- if the project involves the assignment of unique identifiers, whether it is necessary to perform the IPP entity's functions or activities efficiently
- if the project involves adopting, using or disclosing a unique identifier assigned by another IPP entity, whether a relevant exception applies, and
- if the project requires an individual to provide a unique identifier to access a service, whether this is required or authorised by law or otherwise sufficiently connected to the purpose for which the unique identifier was assigned.

IPP 8: Anonymity

An IPP entity must give an individual the opportunity to not identify themselves unless the law or circumstances make it necessary.

Considerations for IPP 8 include:

- whether individuals will have the option of not identifying themselves
- whether a law requires or authorises individuals to be identified, and
- whether it is possible to deal with an individual who wants to remain anonymous (regardless of whether it is more convenient if they identify themselves).

IPP 9: Disclosures outside Australia

An IPP entity must not send personal information overseas unless certain requirements are met.

Considerations for IPP 9 include:

- if the personal information will be disclosed out of Australia, and
- what steps the IPP entity will take to ensure the information will be handled consistently with the IPPs.

IPP 10: Automated decision-making

If an IPP entity employs an automated decision-making (ADM) process that uses personal information to make significant decisions about individuals, it must conduct an impact assessment of the ADM process that considers:

- how to eliminate or minimise the risk of harm, bias, and discrimination,
- the process for human intervention, and
- whether the handling of personal information complies with the PRIS Act.

An IPP entity must also tell individuals it is using an ADM process and provide a process for people to request human intervention in the decision.

There is overlap between the requirement to undertake a PIA and the requirement in IPP 10 to undertake an assessment that considers (among other things) whether the handling of personal information as part of an ADM process complies with the requirements of the PRIS Act. An IPP 10 assessment can be undertaken separately or integrated into a PIA, depending on what is most appropriate for the project. Where a separate IPP 10 assessment has been performed, this should be referenced in the PIA.

Considerations for IPP 10 include:

- whether the project involves making decisions about individuals
- whether any part of the decision-making process is automated
- the extent of any human intervention in the decision-making process, taking into account the circumstances in which the decision is made, including the authority and skills of the decision maker, resourcing (including time available to make the decision), explainability of outputs and the decision-maker's ability to challenge the output of the automated system
- whether individuals are informed ADM is being used and how they can request human involvement in the decision, and
- how the remaining requirements of IPP 10 have been met.

IPP 11: De-identified information

An IPP entity must take reasonable steps to protect the de-identified information it holds from misuse, loss, unauthorised re-identification, access, modification or disclosure.

An IPP entity must not re-identify de-identified information except in certain circumstances.

Considerations for IPP 11 include:

- whether the use or disclosure of de-identified information creates a risk of it being re-identified. For example, where the recipient of de-identified information holds other information which, when combined with the de-identified information, could enable individuals' identities to be worked out
- what safeguards are in place to protect the de-identified information
- whether there is authorisation to re-identify de-identified information, and
- how the IPP entity will test the effectiveness of any de-identification processes used.

Recommendations

The next step in the PIA process is to use the findings of the analysis to make recommendations about how to eliminate, reduce or manage the privacy risks of the project.

Risk mitigation strategies can include:

- technical controls
- organisational controls

- communication strategies

When considering the appropriate risk mitigation strategies, the IPP entity should consider:

1. the outcome of the IPP Analysis and the steps required to ensure the project meets the requirements of the IPPs, and
2. what other steps (if any) are necessary to address the identified privacy risks.

It is essential the IPP entity considers the effectiveness of any proposed mitigation strategies and any residual risks remaining once the action plan has been implemented.

Making recommendations

The foremost recommendation should be whether the project should proceed or not. A project should only proceed if it has acceptable privacy outcomes. This may be because the privacy risks are insignificant, can be eliminated, or can be reduced to an acceptable level through the application of identified mitigation strategies.

Where a project proceeds, appropriate recommendations need to be made about how to eliminate, reduce or otherwise manage the identified privacy risks. This may involve making changes to the design of the project.

When developing recommendations, consider whether consultation is needed (if it has not already occurred) or whether the PIA would benefit from further input. For more information see the section of this guidance titled “Consultation”.

Sometimes the PIA might uncover privacy risks or opportunities that fall outside the scope of the project being assessed, but which provide an opportunity to strengthen the entity’s broader privacy management practices. For example, the PIA may identify opportunities to uplift information security or quality management processes. Where possible, these findings should be captured and escalated in accordance with the IPP entity’s existing risk management processes.

Actioning the recommendations

All recommendations should clearly identify what actions need to be taken to achieve them. This includes outlining who has responsibility for each action and the timeframe for implementation. For more information see the section of this guidance titled “Integrating the PIA with other assessments”.

Report

Section 79 of the PRIS Act requires an IPP entity to prepare a written report on the PIA setting out an assessment of:

- the likelihood the performance of the function or activity will result in an interference with privacy
- the privacy impacts of the performance of the function or activity and the recommended mitigation strategies, and
- any other information the IPP entity considers relevant.

The audience for the PIA report will include both people familiar with the project and those who aren’t. This means the report needs to provide enough background information so someone who hasn’t been involved in the PIA can understand the analysis and recommendations.

At a minimum, the PIA report should include information addressing each of the essential elements of a PIA, as outlined in this guidance.

There is no specified form for the PIA report. A PIA report can be in the format most appropriate for the intended audience.

Publishing the PIA

Under the PRIS Act, parties to an information sharing agreement must make the relevant PIA report publicly available. Although this requirement does not apply to PIAs conducted for other functions or activities, there are significant benefits to publishing a PIA.

Publishing a PIA is an opportunity to build public trust and confidence in the way an IPP entity handles personal information. It demonstrates privacy impacts are being considered, and steps are being taken to manage them. Publishing a PIA is also an opportunity to demonstrate transparency and support Open Government Principles. This can, in turn, improve public uptake and help ensure the benefits of the project are realised.

Nonetheless, there will be circumstances where publishing a PIA in full is not appropriate. For example, where the PIA contains information not appropriate for public release (such as commercially sensitive information) or where it would compromise information security. In these cases, it may be appropriate to publish an edited version the PIA report, which removes the sensitive elements but still provides enough information for the public to understand what risks were identified and how they are being managed.

At a minimum, IPP entities should make a register of the PIAs they have conducted publicly available.

Review

A PIA is an ongoing process that doesn't end after the report has been completed. A PIA should be reviewed at multiple stages, including during the development stage of the project, prior to implementation and any time there is a change that could result in new or increased privacy impacts.

When conducting a review:

- consider what has changed
- identify any new or changed privacy impacts
- update the PIA analysis, and
- update the recommendations.

Incorporating the outcomes of the review into the PIA report can be a helpful way of keeping track of changes and communicating with relevant stakeholders. The level of analysis required at each review stage is dependent on the scale of the change and resulting impact on privacy.

Integrating a PIA with other assessments

A PIA should not be a siloed exercise. A PIA often works best when it is considered alongside other assessments being performed as part of the project. Examples of other assessments that may be relevant to the PIA include:

- vendor risk assessments
- cyber-security assessments
- information technology or architecture reviews
- AI self-assessment
- ADM Assessment

Integrating the PIA with other assessments can reduce duplication, make use of information and expertise already gathered and ensure recommendations are fully informed.

References

Information Commissioner's Office United Kingdom, *Data Protection Impact Assessments (DPIAs)* <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/>.

Office of the Australian Information Commissioner, *Guide to undertaking privacy impact assessments* (2021) <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/guide-to-undertaking-privacy-impact-assessments>.

Office of the Information Commissioner Queensland, *Privacy impact assessments* (2025) <https://www.oic.qld.gov.au/government/privacy/privacy-impact-assessments>.

Office of the Privacy Commissioner Te Mana Matapono Matatapu, 'How to do a Privacy Impact Assessment' <https://www.privacy.org.nz/responsibilities/privacy-impact-assessments/>.

Office of the Victorian Information Commissioner, *Privacy Impact Assessment Guide* (2021) <https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-impact-assessment/>.

Privcore, 'What makes a great Privacy Impact Assessment' (2021) <https://www.privcore.com/_files/ugd/440bc4_772f0f06b9cf4f37be5da234458062f2.pdf>.

Office of the Information Commissioner Western Australia

Office of the
Information Commissioner
Western Australia

Address: Albert Facey House, 469 Wellington St, Perth WA 6000, Australia
Website: www.oic.wa.gov.au • **Telephone:** +61 8 6551 7888
Freecall (WA country): 1800 621 244 • **Email:** info@oic.wa.gov.au

The independent regulator fostering trust and accountability in WA through privacy and freedom of information.