Privacy Impact Assessment Guideline

Version 1

STATE RECORDS
of South Australia

Government of South Australia
State Records

Table of Contents

Introduction

Purpose

This guideline has been developed to assist South Australian government agencies to successfully conduct and navigate privacy impact assessments (PIA). It provides guidance on what a PIA is, why they are needed, when they should be done and how to undertake one.

This guideline applies to all South Australian government agencies required to comply with the Department of the Premier and Cabinet Circular PC012: Information Privacy Principles Instruction (IPPI).

PIAs are considered best practice. Any agency or organisation not bound by the IPPI or another privacy regime may also use this document to undertake PIAs and to achieve best practice in South Australia.

What is a PIA?

A PIA is "a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact."[1]

A PIA can be applied to any project, initiative, program, process or system. For ease of reference, the term project will be used throughout this guideline.

A PIA will identify ways to mitigate and manage privacy risks and impacts associated with various projects and general decision making.

In addition, a PIA can be used by the agency as a useful resource for a project that outlines any future actions required.

Importantly, a PIA should be undertaken in the initial stages of development of a project to have the best opportunity to mitigate and manage privacy risks.

What is a privacy risk?

A privacy risk is the potential to cause harm to a person through collecting, holding or using their personal information.

A privacy risk can occur as a result of collecting too much information; having incorrect information; or not having the appropriate security measures in place to protect personal information from inappropriate use.

Privacy risks can have an impact on the individuals whose personal information is affected, as well as the agency. Therefore, when analysing risks, it is important to assess the risks from both perspectives.

[1] Office of the Australian Information Commissioner, 'Guide to undertaking privacy impact assessments' (11 Nov 2021)

Why complete a PIA?

A PIA will help you work out whether your project requires personal information and to assess any privacy risks.

In deciding to go ahead with a project or when planning a project, there are a range of factors to consider, e.g. benefits, public value, resources required, costs, and risks.

As well as assessing the security and value of records and systems within the project, if the project involves the handling of personal information, it is best practice to conduct a PIA.

Undertaking a PIA will improve the behaviours and practices of the agency and demonstrate respect for individual privacy. Respect is a crucial element in maintaining public trust and engagement with the public sector and its systems and processes.

A PIA will show the agency is taking a proactive approach to privacy and is taking its privacy measures seriously. It also builds compliance of the IPPI into the project as well as the processes and practices of the agency.

In addition, a PIA will analyse whether the project gives rise to unintended consequences regarding the personal information involved.

Application

The IPPI defines personal information as: "…information or an opinion, whether true or not relating to a natural person or the affairs of a natural person, whose identity is apparent, or can reasonably be ascertained, from the information or opinion."

The IPPI is binding for South Australian government agencies with some exceptions. However, any agency or organisation not bound under the IPPI or another privacy regime may use this document to assist with PIAs and mitigate breaches of personal information privacy.

Similarly, this document applies to all records managed by agencies required to comply with the *State Records Act 1997* (the Act). The definition of official record(s) as defined by section 3(1) of the Act includes information, data and records, in any format (whether digital or hardcopy), where it is created or received through the conduct of government business.

Who should undertake a PIA

With the right support, anyone can conduct a PIA. Ideally, the person or project team would be involved with conducting the PIA as they have project familiarity, knowledge of the personal information required and understand the reasons for the project.

In addition, it is beneficial for someone with privacy knowledge to be involved. If the agency has a privacy officer or privacy team, it is worthwhile consulting them for advice. They will be able to provide an understanding of the privacy requirements of the agency, as well as knowledge of existing processes the agency already has in place to manage personal information.

Who needs to be involved?

Anyone with information you need for the PIA should be involved:

People	
Project Team	They can provide guidance on processes involved in the project and what personal information is required to achieve the project outcome.
Privacy Officer/Team	They can provide guidance on the agency's personal information and privacy requirements while assisting in identifying, assessing and mitigating risks.
Other sections of the agency (not exhaustive):	o Information Technology Services - can help you understand the specifics of an IT solution, including its flaws and strengths, when considering the safety and security of personal information o Information management – can ensure all information management requirements are considered in the life cycle of the information being processed, such as retention times, disposal and access o Communications and marketing - can assist with consultation requirements of the project o Legal – to ensure compliance with legislation and identify any risks to the agency from a legal perspective
Stakeholders / contracted service providers	They can provide information and feedback relating to the project, views and expectations, what works and won't work, any foreseeable problems and potential solutions.
Customers / community	They can provide feedback on their expectations, concerns and outcomes of the project and identify any potential or real problems. This can also provide an opportunity for you to alleviate their concerns by explaining how your processes will address them.

How long will it take to conduct the PIA?

This will really depend on the size and scope of the project.

If the project is small with minimal privacy risk and not a lot of personal information is needed, the PIA will be straightforward and won't take long to complete. Conversely, if the project is large or complex, with a lot of personal information involved, then it is reasonable to assume the PIA will be more in depth and will take longer to complete.

The scope of the project will provide a level of understanding of the requirements needed for the PIA, for example resources required, consultation needed, security considerations.

In the project lifecycle, when should the PIA be conducted?

A PIA can be undertaken at the commencement of a project, as part of the planning stage, the project implementation or review stages, however, it is considered best practice to undertake a PIA as early as possible, ideally as part of the planning of the project. This ensures privacy considerations are built into the project development, with risks considered and addressed early in the process.

If the project is complex or extends over a considerable period, it may also be prudent to revisit the PIA to ensure no new privacy risks have arisen, or if they have, they can be identified and managed appropriately.

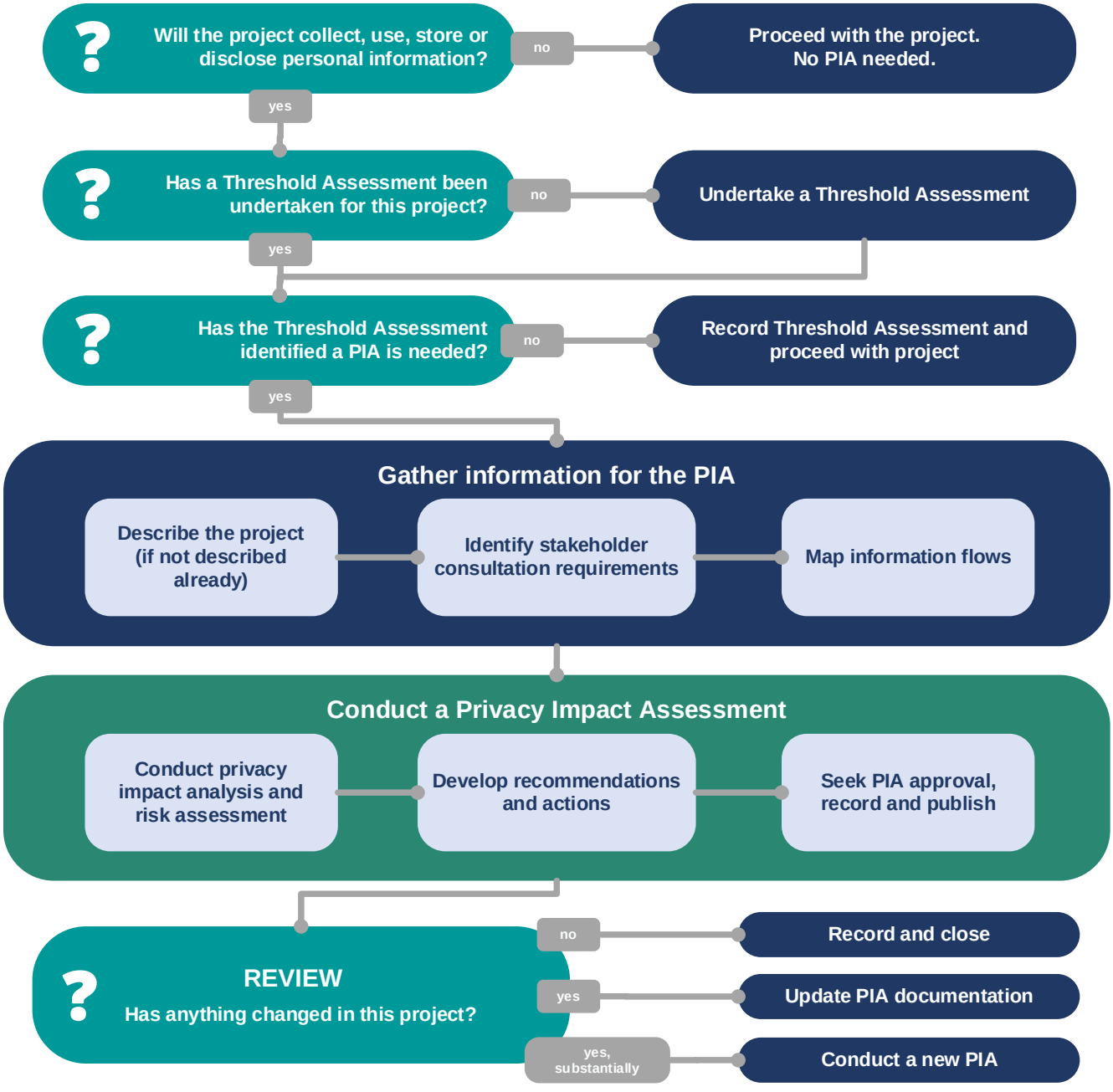
For existing projects that haven't had a PIA, it's never too late to undertake a PIA and implement any outcomes.

The PIA Process

There are several steps involved in undertaking a PIA:

1. Undertake a threshold assessment to determine if a PIA is necessary
2. Gather the information needed for the PIA
3. Analyse the privacy impacts
4. Assess privacy risks and identify potential solutions
5. Develop recommendations and actions
6. Review

The diagram below illustrates the PIA process:



1. Undertake a threshold assessment

The first step is deciding whether you need to conduct a PIA for the project, as not all projects will require a PIA. Generally, if personal information is involved, it is best practice to do a PIA.

Importantly, when considering whether to undertake a PIA, every project should be assessed individually. If you have multiple projects that each collect and use personal information differently, then a PIA should be undertaken for each project.

A threshold assessment provides an early indication if it is necessary to do a PIA. It allows you to identify how much personal information will be required to undertake the project and to discover any privacy risks. An initial assessment of the project will likely capture privacy risks and reduce the chance of missing something vital.

A threshold assessment should include the following information:

- a description of the project, including its aims and objectives
- the types of personal information to be collected, used or disclosed for the project
- the purpose for which personal information will be collected, used and disclosed
- how personal information will be collected and stored
- if the project is a new project or a modification to an existing project. For a modification, a description of the changes
- any potential privacy risks initially identified and possible mitigation measures
- any initial stakeholder views
- any additional documentation that has assisted in the decision to undertake a PIA or not (for example a project plan, risk register)
- a recommendation to proceed with a PIA, or not and the reasons why.

The threshold assessment should be approved by the relevant person (i.e. project manager) and retained as a record. The assessment document has several purposes:

- it is a signed, dated record of the initial assessment of the project
- it provides evidence and justification of the decision to conduct a PIA, or it justifies why a PIA is deemed unnecessary
- it pulls together relevant project information to be used to inform any potential PIA required
- it can be used to gain approval from management for the progression of the project.

A threshold assessment template has been developed to assist in this step of the process. See Appendix A

2. Gather information

Once you have assessed that a PIA is necessary, the next step is to gather the information needed for the PIA. A good starting point is to use the information from the threshold assessment.

A PIA is a tool used to assess the risks associated with the personal information needed for a project and at the same time ensure the agency achieves its objectives. The size and complexity of the PIA will be dependent on the scope and scale of the project.

If large amounts of personal information are required with high privacy risks involved, it may be beneficial to seek expertise outside of the agency to assist with the PIA.

Describe the project

It is useful to describe the project, what it does and doesn't cover, what it aims to achieve, its purpose and the benefits of the project. This provides an understanding of why personal information is being collected and used, how it will be collected, how it will be used and details what types of personal information the project requires to be successful. A project plan or project brief might already contain this information.

The PIA should indicate if the project is a new initiative, or a modification to an existing one and if it is a once off modification or an ongoing change. It should also advise whether there are any links to other projects or programs the agency already has implemented.

Importantly, the PIA should outline the different components of the project and how it will work. This may include many different areas of the agency. It might also include a discussion of the relevant parties (for example, agency personnel, contracted service providers) and their roles in the project.

Legal authority that the agency must collect and use personal information should also be identified as part of the PIA, whether it is the IPPI or some other legislative requirement.

The PIA should also advise who will conduct the PIA, the budget required, key decision-making points and indicate timeframes and milestones.

Stakeholder consultation

It is essential to engage with the people who have an interest in the project (stakeholders) and those who will be affected by the project (those whose personal information is required).

Consultation may include internal and external stakeholders such as:

- other areas of the agency
- regulatory authorities
- customers
- academics
- service providers
- the public
- industry experts

Undertaking consultation as part of a PIA can:

- demonstrate the agency is taking the protection of individual privacy seriously

- offer stakeholders the opportunity to be involved in the risk analysis or share concerns about the project
- potentially uncover risks that have not been identified
- find out stakeholder expectations

The PIA should outline any stakeholder consultation that has already occurred, the outcomes of that consultation and any future consultation planned.

Importantly, consultation can occur throughout the lifecycle of the project and it is possible that different stakeholders may be added to the consultation process during the PIA.

Map information flows

It is important to think of the whole lifecycle of personal information within the project (collection, use, disclosure, storage and destruction) and one of the easiest ways to capture this is by mapping the information flows.

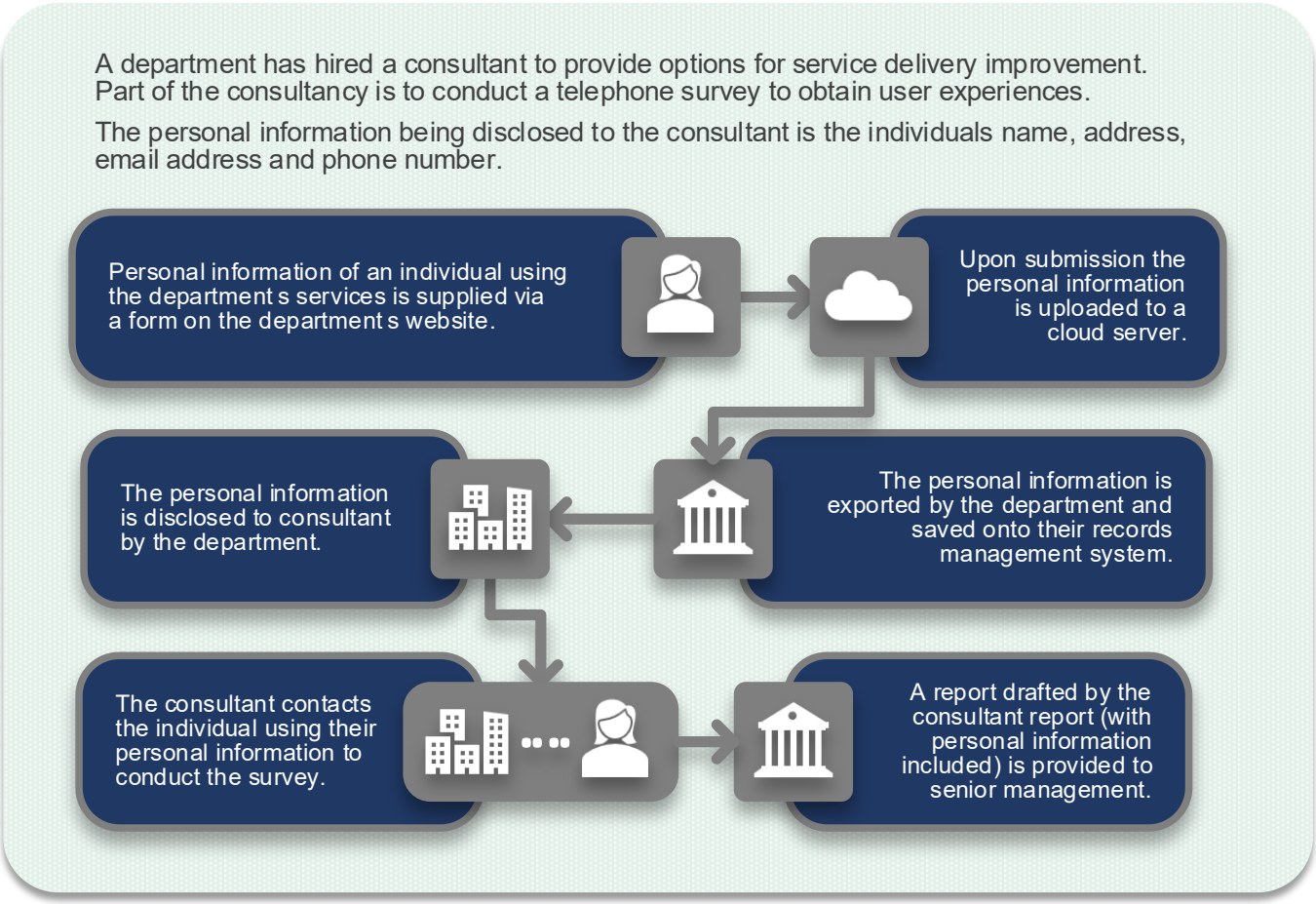
Mapping should explain:

- who will collect the personal information and from whom
- what personal information will be collected
- how the personal information will be collected
- how the personal information will be used
- how the personal information will be stored and kept safe and secure
- why the personal information is necessary for the project
- processes for information quality
- security safeguards and access controls
- whether the personal information will be disclosed to anyone else/other agencies
- how people can access and correct their personal information
- how long the personal information will be retained for and how it will be disposed of.

Understanding how the personal information of the project is being processed will help to comply with the IPPI and ensure the project's objectives are achieved. It will also help with information management and identify and reduce privacy risks.

Mapping can be achieved through an information flow diagram. This diagram can show the flow of information involved in the project, indicating the systems used, the different parties involved (if applicable) and the methods of transfer.

The diagram below is an example of an information flow:



The Office of the Australian Information Commissioner provides detailed guidance on mapping information flows in its Guide to undertaking privacy impact assessments.

3. Analyse the privacy impacts

All projects involving personal information will require a certain level of analysis.

Prior to commencing the privacy impact analysis, it is important to have a thorough understanding of the project. A review of project plans, the threshold assessment document and information flow maps or diagrams will increase accuracy and efficiency of the analysis of the privacy risks.

If the project has the potential for a high-risk impact, more detailed analysis may be needed. A high risk will not necessarily stop the project but may highlight some important actions to mitigate risks.

At a minimum, the analysis should involve:

- the risks of privacy impacts on individuals through the collection of their personal information
- whether the personal information is needed for the project, for example do individuals need to be identified or can they remain anonymous?
- whether sensitive information is involved. (Sensitive information includes, but is not limited to, information about an individual's racial or ethnic origin, political opinions, religious beliefs or affiliations, criminal records, sexual preferences or practices, biometric information, health information and genetic information. The privacy risk associated with your project can increase if sensitive information is involved given the potential for adverse consequences for an individual, or those associated with the individual, if it is mishandled (for example, discrimination, mistreatment, humiliation or embarrassment).
- whether a collection notice has been developed for the collection of personal information relating to the project
- whether risks can be avoided
- whether there is an adequate complaints mechanism in place
- how complaints/breaches will be handled
- any disclosure of personal information required for the project and the associated risks
- the context/environment within which the project will operate, for example have there been concerns in the past about handling this type of information or activity; are there issues of current public concern that should be addressed; what is the nature of the agency's relationship with the individuals that are impacted?

These questions are not exhaustive. You should consider all relevant risk factors for your project.

A PIA template has been developed to assist in this step of the process. See Appendix B

It is worth noting, a PIA is not designed to capture every risk of the project but it should identify realistic risks and assess their seriousness.

Importantly, the analysis should provide an indication of whether the project has acceptable risk and can proceed, or if modifications should be made.

If the project is particularly complex and public facing it may be worthwhile engaging external specialists to undertake the PIA.

Compliance check

It is good practice to assess whether the project's processes are compliant with the IPPI, as well as any other legislation that may be relevant.

Any instances of non-compliance should be described and explained. For example, explain why you haven't complied with one or more principles, or describe why compliance isn't required.

4. Assess the privacy risks and identify potential solutions

A privacy risk assessment is a good way to record privacy risks identified during the previous steps and what you are going to do about them, if anything.

You need to consider what options may allow you to remove, manage or mitigate any risks identified.

You should also consider your agency's attitude to risk. A low tolerance to risk might equate to even minor risks being an issue for the project to progress.

Your assessment should investigate:

- the risk of privacy impacts
- the likelihood and severity of risks
- whether privacy impacts can be avoided
- what actions can be taken to resolve risks
- whether the agency will choose not to mitigate some privacy risks
- how the privacy impacts affect the projects objectives
- compliance with the IPPI
- how privacy breaches will be handled.

If your agency has a risk assessment framework, it is recommended you use that. If not, the PIA template (Appendix B) provides an example table that can be used for the risk assessment.

Following the risk assessment, you should summarise your findings. The summary should include any substantial risks identified as part of the assessment, any risks that have been able to be mitigated, those risks that cannot be mitigated and why, as well as any changes to the project because of the privacy risks identified.

5. Recommendations and actions

Recommendations

From the steps above, a number of recommendations and actions may have emerged. These recommendations and actions should identify how privacy measures can be improved and how negative impacts can be eliminated or mitigated.

The recommendations should cover:

- an action list
- privacy management strategies
- if further stakeholder consultation is required
- any changes regarding the protection of personal information whilst still achieving the project's aims and objectives
- whether any information gaps of the agency have been identified.

Ultimately, the recommendations should consider whether the project has acceptable privacy outcomes or whether the privacy impacts are too great for the project to proceed.

Actions

An action list is useful to manage and monitor identified actions. These can be presented in a table, for example:

Reference number	Action	Owner	Timeframes	Status
R01	*It was identified the agency has no personal information breach response plan. Develop a plan and disseminate.*	*Privacy Team*	*Urgent, within the next three months.*	*In progress*
R02	*Review PIA for any additional privacy risks.*	*Project Manager*	*Every year whilst project is in operation.*	*Not started*

The PIA recommendations and actions should be provided to the appropriate parties so they can be managed. If the agency has a privacy officer or privacy team, they should also be notified of the outcomes of the PIA.

Report

It is best practice to publish a PIA report. This indicates the project has considered and analysed privacy risks. It is an important agency reference and it provides transparency to the public.

Key elements of the report include:

- the project description
- a comparison of new and old information flows depicting the procedural changes
- outcomes from the privacy analysis, risk assessment and compliance check
- any stakeholder consultation undertaken and the outcomes of that consultation
- any actions identified to be managed
- detail about any privacy risks that can't be mitigated
- whether the project will proceed or not and why.

Endorsement

A PIA does not necessarily require formal sign-off or authorisation. It is up to you to decide on appropriate authorisations for projects.

It can depend on the size of the project, the volume of personal information to be collected and used, and the impact of the project on individuals (the subject holders of the personal information). For major projects the chief executive may be the appropriate approval, whereas the privacy officer or project owner may be suitable for more minor initiatives.

For projects carrying significant risk, or for activities for which there is a requirement for a particular level of legislative authority, it is recommended approval or endorsement should be sought from the principal officer or delegate or other authority (for example, a Minister).

Example:
An agency has decided to outsource storage of personal information in the cloud. The project is small in nature, with minimal personal information involved. The project owner is the appropriate approval.

Example:
An agency has decided to do a major upgrade and develop an online platform for customers to access information and services online. The principal officer should endorse the PIA.

6. Review

Depending on the timeframes involved, PIAs should be reviewed and updated.

Projects can evolve and change over time so it can be beneficial to schedule reviews into the PIA process. It is important to review the PIA to consider any new privacy risks as a result of the project changing or growing.

If the project has changed substantially, a new PIA may be required.

Depending on the size of the project and the complexity of the PIA it may be beneficial to seek an external independent review of the PIA. The benefits of an external review include assurance the PIA has been carried out properly and the possible identification of risks and opportunities that may have been missed.

Best practices

Agencies should consider the following best practices regarding PIAs:

- PIAs should be made public on an agency's website. Making PIAs publicly available provides transparency and demonstrates the agency has considered privacy risks. Employees should have access to the agency's PIAs to understand how the agency manages the personal information it collects and holds. In addition, employees can use existing PIAs as an example for any future PIAs required.
- Ideally, the agency establishes and maintains a PIA register, which is publicly available. If a PIA is not able to be disclosed due to the nature of the personal information, a summary can still be provided.

Acknowledgements

Many organisations in the privacy field have produced comprehensive documentation available to assist with PIAs and privacy matters.

State Records would like to acknowledge and recognise the development of this guideline was informed by the work of the:

- Office of the Australian Information Commissioner
- Information and Privacy Commission, New South Wales
- Office of the Victorian Information Commissioner
- Office of the Privacy Commissioner, New Zealand

Appendices

Appendix A – Threshold Assessment template

Appendix B – PIA template

Date approved	Approved by	Version
November 2024	Director, State Records	1

Need further assistance?

State Records

Tel (+61 8) 7322 7077

Email staterecords@sa.gov.au

Web www.archives.sa.gov.au

Appendix A: Threshold Assessment Template

- *Make this document your own. Add or insert agency branding.*
- *The text in the boxes (like this one) is provided to guide you and should be deleted.*
- *List any relevant agency documentation and attach it to the threshold assessment for reference, for example risk registers, project plans.*
- *Ensure the threshold assessment is dated and signed.*
- *Keep as a record.*

Threshold Assessment - [Insert project name]

1. Description of the project

Type here

In this section provide the following details:

- *A brief description of the project*
- *It's objectives and the reasons why the project is necessary*
- *Describe if the project is a new system or existing system and the main changes that are proposed*
- *Describe the expected benefits of the project*
- *Outline any parties involved*
- *Describe the context, for example if the project aims fit within the agency's broader objectives i.e. Strategic Plan.*

2. Personal information needed for the project

Type here

In this section provide the following details:

- *Description of the personal information that will be collected and used for the project i.e. name, date of birth, address*
- *The purpose for the personal information being collected and used*
- *How the personal information will be collected and how it will be kept safe and secure*
- *Any authority under which the personal information is collected i.e. relevant legislation*
- *The table below can be used to assist. Amend the table as necessary.*

Type of personal Information	Source of Information	Purpose of information for the project

3. Privacy and risk assessment

In this section, consider what the project is trying to achieve, the personal information required and the impacts of the project on individuals. The table below provides some initial questions to consider. Amend the table as necessary.

If you tick yes, explain your response, describe any risks you can identify and ways to address them.

A risk matrix has been provided to assist with assessing your risks. The ratings relate to:

- *Impact: the effect on your agency and individuals if the event occurred.*
- *Likelihood: the probability of the privacy risk occurring. When assigning a likelihood rating, consider the cause of the risk and any existing security measures in place within your agency.*
- *Risk: once you have identified the impact and likelihood of the privacy risk, in the table assign an overall risk rating.*

Different projects will have different risk levels. For example, a like for like system upgrade in your agency may have a likelihood rating of 'unlikely' but may involve a significant amount of personal information so should an event occur as a result of the project, there may be 'high' consequences.

LIKELIHOOD				
Almost certain	Medium	High	**Significant**	**Significant**
Likely	Medium	High	High	**Significant**
Possible	Low	Medium	High	High
Unlikely	Low	Medium	Medium	High
Remote	Low	Low	Medium	Medium
	Low	Medium	High	Significant
				IMPACT

Does the project involve any of the following?	Yes/No (tick)	If yes, explain your response	Describe any risks and how to mitigate them	Rate the risk: Low, Medium, High, Significant
Personal Information				
Handling large amounts of personal information Consider the amount of personal information and the number of individuals that will be impacted by your project. Even if each individual only has a small chance of suffering a negative impact, handling personal information on a large scale can increase the privacy risk of your project.				
Handling sensitive information The privacy risk associated with the project can increase if sensitive information is involved. Consider the potential for adverse consequences for an individual, or those associated with the individual, if the information is mishandled (for example, discrimination, humiliation or embarrassment).				
Collection				
A new collection of personal information				
A new way of collecting personal information Example: moving from paper to online collection				
Storage, security and retention				
A change in the way personal information is stored or secured				
Transferring personal information offshore or using a third-party contractor				

Does the project involve any of the following?	Yes/No (tick)	If yes, explain your response	Describe any risks and how to mitigate them	Rate the risk: Low, Medium, High, Significant
Use or disclosure				
A new use or disclosure of personal information that is already held Example: a new project using information already held with the agency				
Disclosure of personal information outside of the agency Example: the use of contractors/consultants				
Access to information				
A change in policy that results in people having less access to information held about them				
Identifying individuals				
Establishing a new way of identifying individuals Example: using biometric data, e.g. voice recognition				
Information management generally				
A substantial change to an existing policy, process or system that involves personal information				
Other				
Anything else that may impact on privacy				

4. Summary of privacy impact

Type here

In this section summarise the assessment above.

Explain the risks, at a minimum those that are rated medium/high. Advise what the agency will do to mitigate the risk, whether the risk can't be mitigated or whether the agency chooses a different approach to mitigate the risk to ensure the project can still proceed.

Use the table below to provide a rating. Explain the rating given.

The privacy impact for this project has been assessed as:	Tick
Inadequate information – More information and analysis is required to assess the privacy impacts.	
Low – The project involves minimal personal information, with uncontroversial use and low risk of harm. Risks can be fully mitigated.	
Medium – Some personal information is involved, but any risks can be mitigated satisfactorily.	
High – The project involves significant personal information, with risks identified.	

5. Recommendation

Type here

In this section, using the information above, either recommend that a PIA is required or that one is not necessary. Give reasons to support your recommendation.

Highlight any potential issues or risks identified through the threshold assessment process that will need to be considered and/or actioned.

6. Sign Off

_____ _____

Name *Position*

_____ _____/_____/_____

Signature *Date*

Appendix B: Privacy Impact Assessment Template

- *Make this document your own. Add or insert agency branding.*
- *The text in the boxes (like this one) is provided to guide you and should be deleted.*
- *List any relevant agency documentation and attach it to the PIA for reference, for example risk registers, project plans.*
- *Ensure the PIA is dated and signed.*
- *Keep as a record.*

Privacy Impact Assessment - [Insert project name]

1. Project Overview

Type here

In this section provide the following details:

- *Name of the project*
- *Name of the agency*
- *Any agency approvals required*
- *Relevant contact details*
- *Details of any privacy officers of the agency*
- *Relevant dates*
- *A brief description of the project*
- *It's objectives and the reasons why the project is necessary*
- *Describe if the project is a new system or existing system and the main changes that are proposed*
- *Describe the expected benefits of the project*
- *Outline any parties involved*
- *Describe the organisational context, for example if the project aims fit within the agency's broader objectives i.e. Strategic Plan.*

2. Privacy Impact Assessment Scope

Type here

In this section provide the following details:

- *Describe what the PIA does and doesn't cover*
- *Any limitations*
- *Outline whether this is a new or reviewed PIA and why.*

3. Personal Information

Type here

In this section provide the following details:

- *Description of the personal information that will be collected and used for the project i.e. name, date of birth, address*
- *The purpose for the personal information being collected and used*
- *How the personal information will be collected and how it will be kept safe and secure*
- *Any authority under which the personal information is collected*
- *The retention and disposal arrangements for the personal information*
- *Any information mapping, flow diagrams that might be beneficial in explaining the project and its information flows.*

4. Threshold Assessment

Type here

In this section advise whether a threshold assessment has been undertaken for the project. Summarise the details of the threshold assessment and any recommendations.

5. Stakeholder Consultation

Type here

In this section outline any consultation that has already occurred and summarise the outcomes. Outline any consultation that will be undertaken for the project, both internal and external.

6. Privacy Analysis

In this section, populate the table that identifies the privacy elements and risks of the project. The table follows the information lifecycle (and the IPPI order) allowing consideration of the project's information flows from collection through to disposal. Some parts of the table may not be relevant or applicable and can be marked N/A. Amend the table as necessary.

Check whether the project's processes are compliant with the IPPI, as well as any other legislation that may be relevant. Any instances of non-compliance should be described and explained. For example, explain why you haven't complied with one or more privacy principles, or describe why compliance isn't required.

For potentially high-risk elements requiring a more thorough analysis, further documentation outside of this table may be required.

Example text has been included (to be deleted), using a simple hypothetical project: the roll-out of a new time recording system for offsite staff.

Question		IPPI	Assessment (or N/A)	Privacy considerations
Personal Information				
1	**Does the project involve personal information?** List the personal information the project requires.		*Yes – name, title, ID number, work location, time spent on site.*	
2	**Does the project involve sensitive information?** List the sensitive personal information the project requires. Sensitive information includes, but is not limited to, information about an individual's racial or ethnic origin, political opinions, religious beliefs or affiliations, criminal records, sexual preferences or practices, biometric information, health information and genetic information. The privacy risk associated with your project can increase if sensitive information is involved given the potential for adverse consequences for an individual, or those associated with the individual, if it is mishandled (for example, discrimination, mistreatment, humiliation or embarrassment.		*No*	

Question		IPPI	Assessment (or N/A)	Privacy considerations
Collection of information				
3	**Does the project involve a new way of collecting personal information?**	2	*Yes – information that has not been collected from volunteers and service providers is now required.* *Information is being collected through a new platform.*	*Collection notices should be distributed, outlining what information will be collected and why. People should also be advised the reasons for the changes ie moving to a new system.* *Individuals may not be aware of the information being collected and the usual practices regarding its use.*
4	**Is any personal information being collected unnecessarily for the project?**	1	*No – a whole of government direction requires evidence that an individual has attended an offsite location and the time spent there.*	*Collecting too much information can lead to uncontrolled use and disclosure.* *Consider reducing what is collected.* *Reference the authority in the collection notice.*
5	**Do you need to collect information that identifies an individual for the purposes of the project, or can individuals remain anonymous?** **Does evidence of identity need to be collected, or simply sighted?**	1	*Yes - collection is required – participants cannot remain anonymous* *No - identity evidence can be sighted and recorded, not collected.*	*If services can be undertaken anonymously, then personal information is not needed. However, in this instance whole of government direction requires individuals onsite to be recorded.* *If identity can be sighted, then personnel with authority to sight information should be clearly defined. There should be a robust process in place to record sighting.* *If services require identity, then information must be managed in accordance with the IPPI.*
6	**If individuals can remain anonymous, will you be collecting indirect identifiers, such as demographic information?**	1	*N/A*	*Indirect identifiers still need to be managed securely to prevent re-identification.*
Method and notice of collection information				
7	**How will the personal information be collected?**	1, 2, 3	*For staff, offsite status will be recorded in HR system.*	

Question		IPPI	Assessment (or N/A)	Privacy considerations
	Is a third party involved? List or describe how the information will be collected, i.e. an online application, over the phone, documentation.		*For volunteers and contractors, reported information will be entered into the system by line managers.*	
8	**Will the individual be notified about the collection of their personal information?** Describe the steps taken to provide notice to the individual OR explain why notice will not be provided to the individual. Include a link or attach collection notices where appropriate.	2	*For staff, collection is notified at sign-up.* *For volunteers and contractors, line managers will provide the advice with printed options available.*	*Collection notices should describe all requirements for collection, including the authority under which it is being collected, how it will be used, how it can be corrected, to whom disclosed and the usual practice for retention or disposal.*
9	**Will any personal information about the individual be collected indirectly from another source?** Describe how and from which other sources the personal information will be collected.		*No*	
10	**Will the individual be notified that their personal information has been collected from another source?**		*N/A*	
Primary and additional uses and disclosures of personal information				
11	**Is the personal information (including any sensitive information) involved in this project used or disclosed for the primary purpose it was collected for?** Describe what personal information will be used or disclosed, and for what purposes.		*Yes - Advice about individual's offsite status will be recorded against their name in the across-government HR system.*	*Need to ensure the system is safe and secure.*
12	**Does the project use or disclose personal information (including sensitive information) for**		*No*	

Question		IPPI	Assessment (or N/A)	Privacy considerations
	a new or additional purpose other than the original purpose of collection? Describe the new/additional purpose for the use or disclosure of the information.			
13	**Will the individual be notified of the additional use(s) of their personal information?** Explain how the individual will be given notice of the secondary use(s) of their information, or why notice of the secondary use will not be provided.		*If it occurs yes. Options could include via intranet information or email.*	
14	**Will any personal information be shared outside of your agency?** If yes, please describe what information and for what purpose. Identify any information sharing agreements are or will be in place, and how disclosures will be recorded.		*No – statistical reporting will be provided but not for any agencies with an off-site cohort smaller than 10.*	
Management of personal information				
15	**Is there a document(s) available to the public that sets out your agency's policies regarding the management of personal information, such as a privacy policy?** Identify the document(s) and provide a link where available or include as an attachment to this PIA.		*Yes - privacy policy on website*	*Update privacy policy.* *Ensure collection notice exists for this collection.*
16	**Will the document be updated to reflect the new collection or use of personal information for the purposes of this project?**		*See above*	*Update privacy policy and ensure collection notice exists for this collection*
Access and correction of personal information				

Question		IPPI	Assessment (or N/A)	Privacy considerations
17	**Is there a procedure in place that can allow individuals to request access to, or correction of, their personal information?** Describe how individuals can seek access and correction and how they will be made aware of this.		*Freedom of Information applies for volunteers and contractors.* *For staff an administrative scheme is in place with HR for access and correction.*	*Consider developing and communicating approach outside of FOI for the update of information.* *Include this advice in the collection notice.*
Storage and security of personal information				
18	**Where and how will personal information be stored?** Describe how (i.e. hard copy, digital) and where the personal information will be stored (i.e. external provider, cloud)		*The HR platform will store all staff-entered information.* *Other registers may be stored in an excel/word file on a network drive.*	*Storage is secure and access is managed based on authority and need.*
19	**Are there security measures in place (existing or intended) to protect the personal information collected and used for this project?** List any policies, procedures, or controls that the agency implements to protect personal information.		*Yes*	*Process for the collection and management to be clearly documented. Including who has the right to collect the information and who has the right to access the information.*
20	**Who will have access to the personal information?**		*Line managers*	*Only authorised persons should be able to access the information and a log of access should be in place.*
21	**Are there access, security and monitoring controls in place to protect against internal and external risks and ensure that personal information is only accessed by authorised persons?**		*See standard arrangements for HR systems and network directories.*	*Held within secure storage areas of agency*
Third party providers				
22	**If applicable, what will happen to personal information held by third party providers (such**		*N/A* *Procedures to be clarified.*	*Ensure all contracts include clear guidance about record retention and disposal and use. Model terms and conditions are available on SRSA website.*

Question		IPPI	Assessment (or N/A)	Privacy considerations
	as contracted service providers, third party platforms)?			
Complaints and breaches				
23	**Who can individuals complain to if they have concerns about the handling of their personal information?** Identify the avenues for complaint procedures.		*For employees of the Crown: Complaints can be made to the agency collecting, the Office of the Commissioner for Public Employment (OCPSE), or the Ombudsman* *For volunteers and contractors, the agency collecting, the Privacy Committee of South Australia, or the Ombudsman*	*Clearly articulate complaint avenues in the collection notice.* *Note: Employees of the Crown can make complaints to OCPSE.*
24	**Does your agency have a data breach response plan?**		*No*	*Refer to the Personal Information Breach Guideline. Each agency should have a response plan.*
Retention and disposal				
25	**How long will the personal information be kept for?** Describe any retention and disposal schedules.		*Retention and disposal to be managed under General Disposal Schedule (GDS) for personnel / contractor information.*	*Retention and disposal arrangements are documented.* *General or specific records disposal schedules (GDS or RDS) specify how long various information is to be retained and are available on SRSA website.*
26	**How will personal information be destroyed once it is no longer required?** Explain how the destruction of the personal information will occur.		*Destruction to occur in accordance with an approved Disposal Schedule.*	*Electronic files must be purged and any hardcopy documents destroyed through non reversible means.*
27	**As an alternative to destroying personal information, will any personal information be de-identified once it is no longer required?**		*No*	*Sometimes information is considered for use in a de-identified manner. This should be considered at the outset.*

Question		IPPI	Assessment (or N/A)	Privacy considerations
	Describe any de-identification measures that will be used.			
Other considerations				
28	**Will any training be provided to staff to ensure the appropriate collection and handling of the personal information collected for this project?**		*Yes*	*Staff clearly understand their role and the importance of the information they are collecting*
29	**Does the project comply with your agency's other information handling or information management policies?**		*Yes*	
30	**Will this PIA be published?**	NA	*Yes – on agency intranet*	*Transparency in the collection, use and management of personal information is important to ensure public trust.*

7. Risk Assessment

In this section, use the table to record any privacy risks that have been identified during the privacy analysis and how the agency proposes to mitigate and manage those risks. It can be useful to link this back to the privacy principles to show why these risks and the proposed actions are relevant.

If the agency has a risk assessment framework, use it. If not a risk matrix has been provided to assist with assessing your risks. The ratings relate to:

- *Impact: the effect to your agency and individuals if the event occurred.*
- *Likelihood: the probability of the privacy risk occurring. When assigning a likelihood rating, consider the cause of the risk and any existing security measures in place within your agency.*
- *Risk: once you have identified the impact and likelihood of the privacy risk, in the table assign an overall risk rating.*

Summarise the recommendations of your risk assessment.

LIKELIHOOD

Almost certain	Medium	High	**Significant**	**Significant**
Likely	Medium	High	High	**Significant**
Possible	Low	Medium	High	High
Unlikely	Low	Medium	Medium	High
Remote	Low	Low	Medium	Medium
	Low	Medium	High	Significant

IMPACT

Risk ref	Responsibility	Description of the risk	Risk rating	Accept risk	Risk management strategy	Residual risk rating	Risk owner
	Identify who may be responsible or who may be consulted with (ie ICT, Project team, HR)	*The risk of [event] caused by [how] resulting in [impact(s)]*	*Identify the impact risk, likelihood risk and subsequent overall risk*	*Identify whether the agency will accept the risk (yes or no)*	*Detail the measures taken (or to be taken) to mitigate and manage the risk. Where relevant, include the timeframe for implementing the strategy and identify who is responsible for it.*	*Identify the impact risk, likelihood risk and subsequent overall risk after security measures have been applied.*	*Assign a risk owner who will be responsible for monitoring and reviewing the risk.*
R001	*ICT, privacy*	*New system for recording times of offsite staff – staff may not be aware of the information being collected.*	*Medium*	*Y*	*Collection notices will advise staff on the new system and the collection of their personal information*	*Low*	*Manager*
R002	*HR/Privacy*	*Access to the system – who can view staff times offsite*	*Medium*	*N*	*Implement access controls so only those who need access, have access. This will reduce access to personal information of staff to only those that require it.*	*Low*	*HR/Management*

8. Action Plan

Type here

In this section describe what actions are being taken (short or long term) and how they'll be monitored. It can be presented in a table and should include:

- *Reference*
- *Action*
- *Owner*
- *Timeframe*
- *Date completed*

If a PIA needs to be revisited this section should describe any actions taken to ensure it continues to be fit for purpose for the project.

9. Documentation

Type here

List and record any relevant agency documentation that has been used as part of the PIA process, for example risk registers, project plans, strategic plans.

10. Endorsement

Type here

Ensure the relevant people endorse the PIA.

_____ _____

Name *Position*

_____ _____/_____/_____

Signature *Date*

_____ _____

Name *Position*

_____ _____/_____/_____

Signature *Date*