PRIVACY IMPACT ASSESSMENT GUIDELINES

October 2018

PRIVACY IMPACT ASSESSMENT GUIDELINES

Table of Contents

Introduction

This Privacy Impact Assessment Guideline has been prepared to assist you in conducting a Privacy Impact Assessment (PIA). It is designed to assist in evaluating compliance with the Information Privacy Principles (IPPs) contained in the *Information Act* (NT) (*Information Act*), and identify potential privacy risks[1]. However this document should not be considered a substitute for legal advice.

If you have any questions or doubts about this guideline contact your Information and Privacy Officer or contact our office at infocomm@nt.gov.au.

The PIA assesses the privacy impacts of a new project and identifies ways that personal and sensitive information can be protected. Personal information may not necessarily include details such as an individual's name but can include any information that identifies an individual or allows them to be identified. The PIA process can pinpoint risks and propose ways in which your organisation's privacy obligations can be met. The PIA is best completed in the preliminary or conceptual phase of a Project in order to identify potential privacy risks or barriers. It should also be revisited prior to the implementation of a Project to ensure that the Project complies with privacy obligations.

This guide outlines how to undertake a PIA. This process can be readily integrated into a project management methodology. For the purposes of this guide, the term 'project' is used broadly and is intended to cover the full range of activities and initiatives that may have privacy implications, such as:

- new or amended ICT systems, databases or software applications
- new or amended legislation or policies and procedures
- new programs or procedures for service delivery; or
- changes to how personal information is handled or stored.

No in-depth or specialist knowledge in privacy is required to use this resource

What is Personal Information?

Section 4A of the *Information Act* defines personal information as:

(1) Government information that discloses a person's identity or from which a person's identity is reasonably ascertainable is "**personal information**".
(2) However, government information is not **personal information** to the extent that:
(a) the person's identity is disclosed only in the context of having acted in an official capacity for a public sector organisation; and
(b) the government information discloses no other personal information about the person.
(3) In this section: "***acted in an official capacity***", in relation to a public sector organisation, means having exercised a power or performed a function as, or on behalf of, the organisation.

What is Sensitive Information?

The *Information Act* contains specific provisions relating to the collection of sensitive information (IPP 10).
While there are many types of information that attract a heightened duty of care in practice, for example credit card details, there are IPPs that specifically apply or are more onerous in relation to sensitive personal information in the *Information Act*. Sensitive information is defined in section 4 of the *Information Act*:

"**Sensitive information**" means:
(a) personal information about:

[1] This document has been adopted substantially from a publication produced by the Office of the Information Commissioner (OIC) Queensland (QLD). The Office of the Information Commissioner (NT) gratefully acknowledges resources published by the Office of the Information Commissioner Queensland and the Office of the Australian Information Commissioner (OAIC).

i. Racial or ethnic origin
ii. Political opinions
iii. Membership of a political association
iv. Religious beliefs or affiliations
v. Philosophical beliefs
vi. Membership of a professional or trade association
vii. Membership of a trade union
viii. Sexual preferences or practices
ix. Criminal record

(b) health information

Contract Service Providers

The privacy protection obligations under the *Information Act* are transferred to any Contract Service Provider where the requirement has been included in the services contract with the Contract Service Provider. Please refer to section 149 of the *Information Act* for additional information on Contract Service Providers and privacy. Please also note that Section 4 of the *Information Act* defines a contract service provider as the person or body who is collecting or handling personal information under a service contract with a Northern Territory Government (NTG) agency.

Why do a PIA?

Key benefits of undertaking a PIA include that it:

- supports good governance and informed decision-making
- ensures that the project is compliant with the *Information Act*
- encourages cost-effective solutions, since it is cheaper to make changes that will address privacy issues during the design phase than attempt to retrofit changes after a system is operational;
- reduces the risk of low adoption rates or participation in the project's deliverables by providing assurance to stakeholders that the project has been designed with privacy in mind; and
- Reduces the risk of low adoption rates or participation in project outcomes by providing assurance to stakeholders that the project is designed with privacy in mind.

A PIA is a key way of building trust as it gives confidence to those who will be affected by the project – and those responsible for the project – that the privacy impacts have been considered and appropriately addressed.

When to do a PIA?

A PIA should be undertaken as early as possible in the project lifecycle so that its findings can influence the design of the project.

At the conceptual stage of development of the project, the privacy impacts may only be able to be assessed at a very high level. However, early consideration of privacy issues will prevent unnecessary effort being expended on design options that are not compliant with the *Information Act*. As the project develops and specifications become further defined, the PIA can be revisited and updated.

Integrating PIAs into agency project management process

Project Officers are required to complete a PIA during the planning phase of any project.

How to do a PIA

While each project is different, a PIA should generally include the following steps:

- Conduct a threshold assessment
- Plan the PIA
- Describe the project
- Identify and consult with stakeholders
- Map the personal information flow
- Identify the privacy issues
- Identify options to address the privacy issues
- Prepare the PIA report; and
- Action the agency's response to the PIA report.

Each step is explained in more detail below.

Conduct a threshold assessment

A PIA is a scalable tool used to assess the privacy risks of a project.

A PIA may not be necessary if the project does not handle any personal information, or where the project does not propose any changes to existing information handling practices and the privacy impacts of these practices have been assessed previously and controls are current and working well.

If the project involves handling a minimal amount of personal information, the PIA in turn, might be quite brief. Equally, a more comprehensive PIA will be needed for a complex project.

Generally, if personal information is involved in the project, some form of PIA will be necessary. The questions set out in **Appendix A** can help you to conduct a threshold assessment and work out the extent to which the project will benefit from a PIA.

It is recommended that you keep a record of the threshold assessment. If questions arise later about why a PIA was not conducted, the threshold assessment shows the basis for the decision.

Plan the PIA

Before undertaking a PIA, you will need to consider:

- how detailed the PIA needs to be
- who will conduct the PIA
- what timeframe is available
- what level of stakeholder consultation will be necessary, if any; and
- how the PIA report will be dealt with.

For complex projects or projects with significant privacy implications, it may be useful to draft Terms of Reference to formally set out how the PIA will be undertaken.

Determine how detailed the PIA needs to be

The level of detail needed in the PIA is influenced by:

- the quantity of personal information handled
- the nature of the information and whether sensitive information will be handled
- the size and complexity of the project
- whether personal information handling will be outsourced
- whether personal information will be transferred outside of the Northern Territory or outside Australia

- whether new or innovative technology will be used to collect or store personal information
- whether personal information will be linked or used for data-matching
- whether information will be shared with another agency
- the likely community and/or media interest in the project.[2]

This information can also be used to inform the level of stakeholder consultation that will be required and will assist with identifying timeframes for completion of the PIA.

Identify who will conduct the PIA

Generally, whoever is managing the project will be responsible for ensuring that a PIA is carried out.

It is recommended that advice is sought from your agency's Privacy Officer, as they can explain the agency's obligations regarding how personal information is to be collected, stored, used and disclosed by NTG agencies. For further guidance on who else might be involved in the PIA process, please see the section: *Identify and consult with stakeholders*.

Engaging an external entity with specific expertise in this area to carry out the PIA, may be preferable for projects that require a detailed PIA.

Describe the project

For consultation to be effective, stakeholders will need to be sufficiently informed about the project. A description of the project should include the following information:

- what the project will deliver and what it will achieve;
- why the project is needed;
- any links with existing projects;
- what information will be collected, used or disclosed;
- who is responsible for the project; and
- timeframes.

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

Identify and consult with stakeholders

Consultation with the people who have an interest in the project, or who will be affected by the project, is essential to the PIA process. Consultation may need to occur throughout the PIA process rather than at a single point so that the necessary people are consulted at the appropriate time.

Stakeholders you might involve in the PIA process include:

- **internal stakeholders** - such as members of the project team, information technology, privacy, legal, procurement and records management staff as well as the front-line or customer-facing staff who will have to use the new system or process that will be delivered by the project; and

- **external stakeholders** – such as suppliers, clients[3], non-government organisations, advocacy groups, and the public.

Involving internal stakeholders in the PIA process is critical as these are the people who know the project and operational environment the best. They will be able to explain and answer questions about likely information flows, governance structures, technical architecture, legislation under which the agency operates that authorises or requires certain information to be collected, used or disclosed, and

[2] For example, the project may pioneer the use of biometric technology such as fingerprinting recognition, the community's unfamiliarity with which may require educative communications in order for it to be assured as to its security and integrity.
[3] For some projects, the clients may be the agency's employees.

information retention and disposal requirements. Importantly, they may also be able to suggest potential solutions to address the identified privacy issues or provide advice on which proposal is the most appropriate.

Consultation with the stakeholders whose personal information will be affected by the project, or their representatives, is an important part of the PIA process for two reasons. Firstly, it enables the agency to understand the concerns of those individuals about the handling of their personal information. Secondly, consultation will also improve transparency and build trust by demonstrating that any privacy issues have been identified and addressed.

Consultation can take many forms, including telephone or online surveys, focus groups and workshops, seeking public submissions, and stakeholder interviews. The appropriate approach will depend on the stakeholder group, timeframes and the stage of the project. Careful consideration should be given to which consultation approach will be appropriate in the circumstances.

ⓘ Effective consultation is:

- Timely – at the right stage and allow time for responses
- Clear and proportionate – in scope and focussed
- Representative – ensure those affected have a voice
- Transparent – ask objective questions and present realistic options
- Fed back to participants – at the end of the process

Determine the degree of consultation warranted by the project

Consultation should be appropriate to the size and complexity of the project. For example, for a small project with limited privacy impacts, it may be sufficient to consult only with internal stakeholders. In contrast, a high profile project having significant privacy impacts may require broad and detailed consultation.

When deciding what degree of consultation is necessary for a project, you should consider whether there is:

- likely to be public concern about actual or perceived impact on privacy
- a large number of people or a particularly vulnerable group whose privacy is affected
- vulnerability of any personal information holdings to misuse or abuse
- any existing project consultation process into which the privacy aspects can be incorporated; and
- any 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, or advocacy groups that represent relevant sectors of the community.

Commercial-in-confidence or security considerations can sometimes affect how much information about the project can be released to third parties. In these circumstances, it may be necessary to make the release of information subject to confidentiality agreements, or to release a summary of information.

Map the personal information flow

Before you can identify how or whether a project will impact on the privacy of an individual's personal information, you need to understand whether and how personal information will be collected, stored, used and disclosed in the project from beginning to end. Commonly, this is done by mapping how personal information is likely to flow as a result of the project.

Using diagrams can be helpful to illustrate the flow of personal information. You might consider one version showing how things work now, and a second version showing how things are intended to work if the project is implemented according to its current design. At a minimum, the map should describe:

- what personal information will be collected, who it will be collected from and how it will be collected;
- any legislation which authorises or requires your agency to collect the personal information;
- how the personal information will be stored;
- who has access to the personal information;
- what the personal information will be used for;
- whether the personal information will be disclosed and if so, to whom it will be given and for what purpose;
- whether the personal information will be shared with any other entities; and
- whether personal information will be transferred outside the Northern Territory or outside of Australia.

Appendix B provides further guidance on the level of detail required to sufficiently describe the personal information flow.

Identify the privacy issues

Once you have mapped the personal information flow, you can begin identifying privacy issues by comparing the project's personal information handling practices against the privacy obligations set out in the *Information Act*.

These obligations apply to all agencies, and include:

- Information Privacy Principles (IPPs)
- the rules about transfer of personal information outside of the Northern Territory[4] and the requirement to bind contract service providers to the privacy principles[5]

In addition to compliance with the *Information Act*, you may also need to consider:

- whether there is other legislation that applies to your agency that requires confidentiality or secrecy in the handling of information handling;[6] and
- community expectations of privacy.[7]

Measuring community expectations

The best way to assess community expectations is to conduct public consultation on the project's proposed handling of personal information. If widespread consultation is not an option, consider more targeted consultation, for example, with advocacy groups or professional associations. You could also look at community responses to similar projects or published research into community attitudes about privacy.[8]

The questions in Appendix C will help you to identify where there are privacy issues. Not all questions will be relevant to every project. Equally, you may need to consider other questions, taking into account the nature of your project and your agency.

[4] See IPP 9 in Schedule 2 of the *Information Act*

[5] See Section 149 of the *Information Act*

[6] For example, the *Care and Protection of Children Act* (NT); the Commonwealth *Privacy Act 1988*.

[7] While information privacy obligations are set out in the *Information Act*, being aware of the community's perceived privacy concerns about a project and addressing those concerns can be critical to the uptake of a project.

[8] For example, the OAIC Community Attitudes to Privacy, viewable at https://www.oaic.gov.au/engage-with-us/community-attitudes/

Tip – Recording privacy issues

It is recommended that the management of privacy issues is integrated into the overall project management process by recording privacy issues in the project register or issues log. This will ensure that privacy issues are regularly monitored and reported on by the project manager.

Identify options to address the privacy issues

Once you have an understanding of the privacy issues, the next step is to consider what action can be taken to address them and ensure compliance with the *Information Act*. Where there are multiple options for addressing a privacy issue, you may need to evaluate the costs, risks and benefits of each option to identify which option is the most appropriate.

Options for addressing privacy issues may include:

- operational controls (for example, legislative requirements and regulations, contractual obligations, agency policies or procedures, staff training and accountability measures)
- technical controls (for example, access control mechanisms, encryption and design changes); and
- physical controls (for example, lockable filing cabinets and limiting access to certain floors or areas).

Examples of common privacy issues and potential ways of addressing them are outlined in **Appendix D.** This is not a comprehensive list of all possible privacy issues; rather, it provides a starting point for your own analysis and assessment.

Waiving or modifying an agency's compliance with the privacy principles

The *Information Act* requires all NTG agencies to comply with each of the IPPs. However, in accordance with Part 5 Division 4 of the *Information Act*, the Northern Territory Information Commissioner can authorise NTG agencies to collect, use or disclose personal information in a way that would otherwise contravene or be inconsistent with the IPPs if certain circumstances arise.

Only a public sector organisation can apply for a grant of authorisation to depart from the IPPs. If the NTG agency will not be compliant with one or more of the IPPs for the project, as identified by the PIA, a grant of authorisation may be appropriate. Please refer to the NT Office of the Information Commissioner Guideline *Authorising departure from the IPPs*[9] and discuss your concerns with your in house Information and Privacy Officer. Alternatively, you should consider whether your agency requires its legislation to be amended to allow the project to be implemented, or whether the project should not proceed in its present form.

Prepare the PIA report

A report that sets out all the information gathered throughout the PIA, and its findings, is an important outcome of the PIA process.

Key elements of a PIA report include:

- a project description
- the PIA methodology
- a description of the personal information flow
- the stakeholder consultation undertaken
- a description of the privacy issues; and
- recommended actions to ensure compliance with the *Information Act*.

[9] This guideline can be found at https://infocomm.nt.gov.au/resources/guidelines

The PIA report should be provided to the relevant governance body for approval.

A suggested outline for a PIA report and drafting tips are provided in **Appendix E**.

Action the Agency's response to the PIA Report

The PIA process does not end with preparation of the PIA report.

The agency's response and recommended actions should be fed back into the wider project management process[10] and incorporated into project or stage plans to ensure that the activities necessary to implement the recommendations are assessed, identified, monitored and reported.

ⓘ **Tip**

Publishing the findings of a PIA, together with the agency's response to those recommendations, is encouraged as it contributes to the transparency of the project's development and intent, and provides reassurance to individuals that their personal information will be handled in compliance with the *Information Act*.

If detailed information about the project cannot be published due to security or commercial-in-confidence sensitivities, consider alternatives such as releasing a summary version of the PIA report.

Update the PIA if required

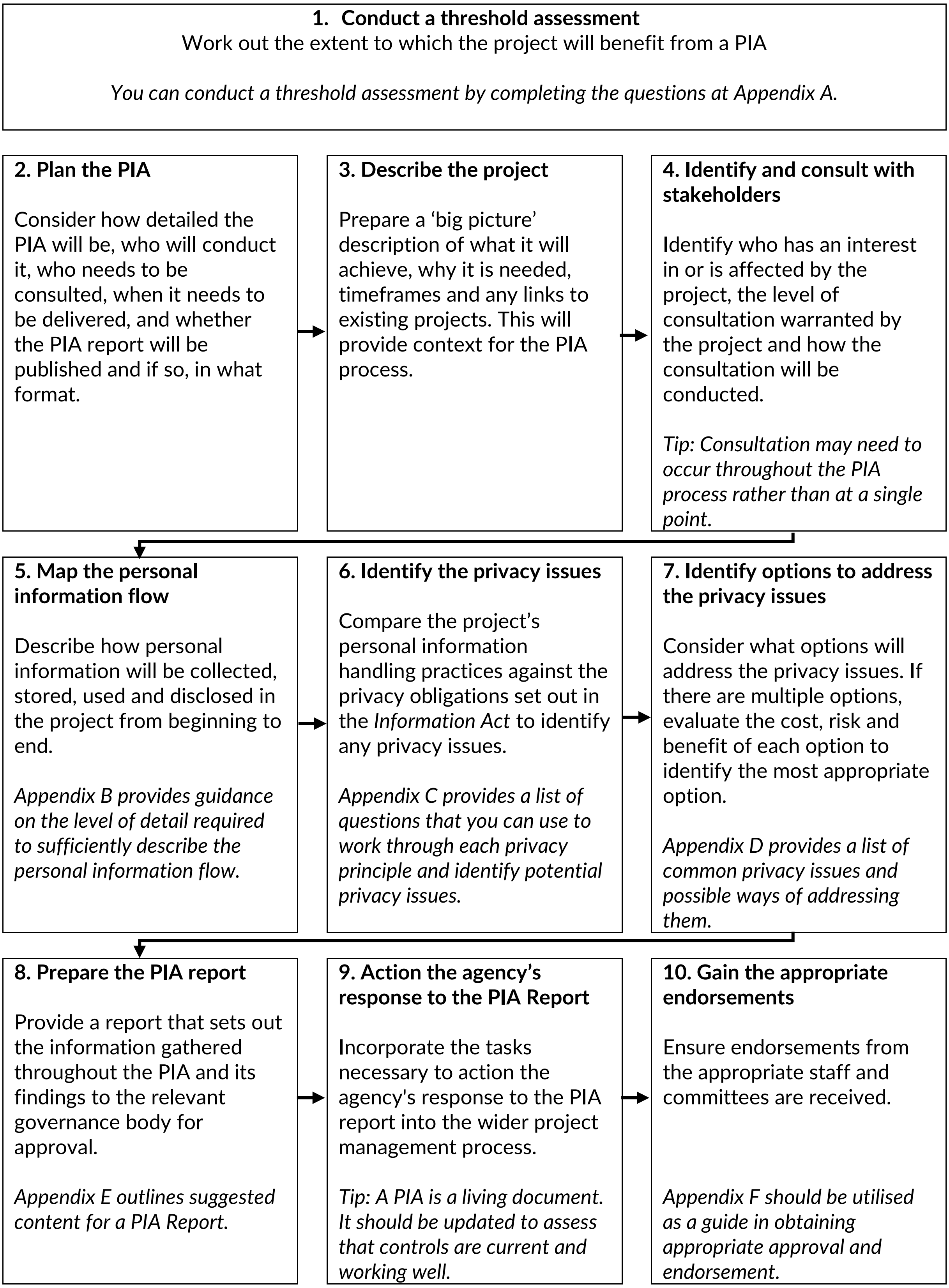
Many projects undergo changes before they are finally implemented. The PIA should be revisited and updated if changes create new privacy impacts that were not previously considered.

Workflow and approval process

The following workflow diagram provides a brief overview of the requirements to complete a Privacy Impact Assessment and details for the individual parts to be completed:

[10] For example, by updating the Project Register or Issues Log to record a description of the issue, the agreed actions to resolve it, a target date by which the issue needs to be resolved and other related information.

Conduct a threshold assessment



1. Conduct a threshold assessment

Work out the extent to which the project will benefit from a PIA

You can conduct a threshold assessment by completing the questions at Appendix A.

2. Plan the PIA

Consider how detailed the PIA will be, who will conduct it, who needs to be consulted, when it needs to be delivered, and whether the PIA report will be published and if so, in what format.

3. Describe the project

Prepare a 'big picture' description of what it will achieve, why it is needed, timeframes and any links to existing projects. This will provide context for the PIA process.

4. Identify and consult with stakeholders

Identify who has an interest in or is affected by the project, the level of consultation warranted by the project and how the consultation will be conducted.

Tip: Consultation may need to occur throughout the PIA process rather than at a single point.

5. Map the personal information flow

Describe how personal information will be collected, stored, used and disclosed in the project from beginning to end.

Appendix B provides guidance on the level of detail required to sufficiently describe the personal information flow.

6. Identify the privacy issues

Compare the project's personal information handling practices against the privacy obligations set out in the *Information Act* to identify any privacy issues.

Appendix C provides a list of questions that you can use to work through each privacy principle and identify potential privacy issues.

7. Identify options to address the privacy issues

Consider what options will address the privacy issues. If there are multiple options, evaluate the cost, risk and benefit of each option to identify the most appropriate option.

Appendix D provides a list of common privacy issues and possible ways of addressing them.

8. Prepare the PIA report

Provide a report that sets out the information gathered throughout the PIA and its findings to the relevant governance body for approval.

Appendix E outlines suggested content for a PIA Report.

9. Action the agency's response to the PIA Report

Incorporate the tasks necessary to action the agency's response to the PIA report into the wider project management process.

Tip: A PIA is a living document. It should be updated to assess that controls are current and working well.

10. Gain the appropriate endorsements

Ensure endorsements from the appropriate staff and committees are received.

Appendix F should be utilised as a guide in obtaining appropriate approval and endorsement.

APPENDIX A – THRESHOLD PRIVACY ASSESSMENT

1. Project Name

2. Brief description of the project

Outline what the project will deliver, what it will achieve, and who is responsible for delivering the project.

3. Personal information flow

Provide a brief description of the personal information that will be collected, stored, used or disclosed (for example - name, address, date of birth, photograph or video recordings, and so forth).

Note: *A PIA will not be necessary if the project will not deal with any form of personally identifiable information.*

4. Stakeholders

List the internal and external stakeholders who have an interest in the project, or who will be affected by the project.

Internal

External Stakeholders

5. Threshold privacy assessment

A PIA is recommended if you answer **"Yes"** to any of the following questions.

	Will the project involve:	**Yes**	**No**
1	Collecting personal information, compulsorily or otherwise?		
2	Using personal information to make decisions or take action against individuals in ways which can have a significant impact on them (for example, whether to receive a service or benefit)?		
3	Collecting personal information in a way that might be perceived as being privacy intrusive, such as surveillance or use of biometrics (for example, finger scans or facial recognition)?		
4	Using personal information that is already held by the agency for a purpose it is not currently used for?		
5	Disclosure of personal information, whether to another agency, the private sector or to the public?		
6	Will there be any exchange of personal information between agencies or entities?		
7	Linking, matching or cross-referencing of personal information across or within agencies?		
8	Using personal information for research or statistics?		
9	A new or changed way of transferring personal information between agencies or between an agency and another entity?		
10	New or changed legislative provisions relating to how personal information is collected, used or disclosed?		
11	A new or amended way of storing, securing or retaining personal information?		
12	New or changed methods of verifying an individual's identity?		
13	Transferring personal information outside of the Northern Territory (for examples, by publishing information to a website or use of cloud services)?		
14	Any other measures that may affect personal information or which could raise other privacy concerns?		

6. Project Officer’s recommendation

□ I, the project officer, have read the Information Privacy Principles found in Schedule 2 of the *Information Act*.

A Privacy Impact Assessment [is / is not] needed for this project

Name:	
Position title:	
Signature:	
Date:	

7. Privacy Officer’s endorsement

A Privacy Impact Assessment [is / is not] needed for this project

Name:	
Signature:	
Date:	
Comments:	

If the Privacy Officer states that a Privacy Impact Assessment is required then it must be conducted.

APPENDIX B – MAPPING PERSONAL INFORMATION FLOW

The following areas of consideration are provided to help you describe in sufficient detail how personal information will 'flow' as a result of the project.

Collection of personal information

For each agency or business unit[11] involved in the project, describe:

- what personal information will need to be collected
- what sensitive information will need to be collected
- the purpose for which the personal information is being collected
- any legislation which authorises or requires the agency to collect the personal information
- how the personal information will be collected (for example, on paper, by e-mail, online transactions, camera surveillance, and so forth); and
- who the personal information will be collected from (for example, from the person whom the information is about, somebody else, from an existing information source within the agency, or from another agency?).

Use of personal information

For each agency, business unit, contract service provider, vendor or school involved in the project, describe all the planned uses of the personal information, whether currently held by the agency or being collected by the project.

Disclosure of personal information

For each agency, business unit, contract service provider, vendor or school involved in the project, outline whether any personal information will be disclosed to a third party (including where the personal information will be shared with another agency or service provider) by describing:

- whom the personal information will be disclosed to and for what purpose; and
- how this disclosure falls within one or more of the exceptions in IPP 2 and IPP 9.

Accuracy and quality of personal information

For each agency or unit involved in the project, outline what steps will be taken to check the accuracy, completeness and currency of personal information prior to its use.

Storage and security

For each agency or unit involved in the project, including contract service providers, outline:

- what personal information will be stored
- where personal information will be stored especially if interstate or in the cloud or off-shore;
- how the personal information will be stored; and
- who will have access to the personal information.

[11] Including any Contract Service Providers

Access and Correction

Describe how individuals will be made aware of what personal information is held about them and how they request access to or amendment of their personal information (for example, through administrative release or a legislative scheme).

ⓘ **Tip**

Diagrams may help to illustrate personal information flow. Where necessary, provide an accompanying table to explain the diagram. You might consider one version showing how things work now, and a second version showing how things will work as a result of the project.

For comment during consultation process – Would it be beneficial to include a flowchart example in the final document.

APPENDIX C – IDENTIFYING PRIVACY ISSUES

The following questions can be used to help identify where there is an issue that your project will not comply with the Information Privacy Principles (IPPs) set out in the *Information Act*.

Limit collection (IPP 1)[12]

- Collect only that personal information necessary for or required to fulfil a purpose that is directly related to a function or activity of your agency.
- Obtain it lawfully and fairly and in a way that is not unreasonably intrusive into an individual's personal affairs.
- Inform the individual of:
  - what you are going to do with their information;
  - any applicable law;
  - any third parties the information will be given to;
  - any consequences for the individual if all or part of the information is not provided;
  - their right to access the information upon request; and
  - how they can contact the organisation.
- Take reasonable steps to ensure the information is complete and up to date (IPP 3).

Questions to ask

- Is all personal information to be collected necessary to achieve the identified purpose?
- Is collection of the personal information necessary or directly related to the purpose?
- Is personal information to be collected for more than one purpose? and
- If so, will an individual be reasonably aware of what information will be used for which purpose? and
- Will individuals be aware of which information is mandatory and which information is optional?
- How will individuals be made aware of what their personal information will be used for, any law that authorises or requires the collection, and the entities to whom their personal information will be routinely disclosed?[13]
- Will the personal information being collected be checked to ensure that it is complete and up to date?
- Will the way in which the information is collected be an unreasonable intrusion into the personal affairs of the individual?

Limit use and disclosure (IPPs 2 and 3)[14]

- Use information only for the purpose for which it was collected or for a directly related purpose.
- Take reasonable steps to make sure the information is accurate, complete and up to date before you use it.
- Only use or disclose the portion of information that is necessary.
- Do not disclose personal information to anyone other than the individual who is the subject of it, unless one of the exemptions in the *Information Act* permits it.

Questions to ask

- Will there be any procedures or processes to guide when use or disclosure of personal information can occur under any of the permitted exemptions in the *Information Act*? For example:

[12] Refer to NT OIC guideline Privacy – Collection of information for more information.

[13] Also referred to as a 'Collection Notice' or 'Privacy Notice'

[14] Refer to NT OIC guideline Privacy – Use and Disclosure for more information.

  - Where satisfied on reasonable grounds that it is necessary to prevent or lessen a serious threat to the life, health, safety or welfare of an individual means, or to public health, safety or welfare?
  - Where satisfied on reasonable grounds that is necessary for law enforcement purposes?
  - For limited research or statistical purposes?
  - Where the individual has agreed to the use or disclosure?
- If you will be relying on the agreement of each individual concerned to use or disclose personal information, what process will you use to obtain the individual's valid agreement, ie that the agreement is informed and voluntary?[15] Will you keep a record of the agreement? Will individuals be permitted to opt out and if so, how is that to be done?
- Who will you routinely disclose personal information to? What exemption will be relied upon to disclose this personal information?
- What is the harm to individuals if inaccurate, incomplete or out of date personal information held by your agency is acted upon?

Keep it safe (IPP 4)[16]

- Make sure personal information is protected by appropriate security safeguards to prevent it being lost, accessed improperly, misused, modified or disclosed.
- If giving the information to a third party, take reasonable steps to prevent its unauthorised use or disclosure.

Questions to ask

- Will the security safeguards used to protect personal information from loss, unauthorised access, use, modification, disclosure or other misuse provide an adequate level of protection that can reasonably be expected to be provided?[17]
- What training and awareness will be provided to ensure that staff are aware of security policies and practices?
- If personal information will be given to another entity in connection with a service to your agency, what processes or procedures will be used to prevent any unauthorised use or disclosure of information by that entity?
- Is there a process or procedure for determining when personal information is no longer required to be retained?[18]

Be transparent and accountable (IPPs 5 and 6)[19]

Inform the public about what sort of personal information you hold and how it is used and how to request access to or amendment of documents containing their personal information.

Limits on interstate or overseas transfer (IPP 9)

Do not transfer personal information outside the Northern Territory unless:

- the individual agrees to the transfer; or
- the transfer is required or authorised under a law of the Territory or the Commonwealth; or

[15] Please see NT OIC guideline Privacy – Use and Disclosure .

[16] Refer to NT OIC guideline Privacy – Management of information for more information.

[17] NTG ICT documentation can be found at: http://ntgcentral.nt.gov.au/ntg-tools-services/ict-and-records-management/policy-and-governance/ict-documentation

[18] Records Management Standards for public sector organisations in the NT can be found at http://www.nt.gov.au/dcis/info_tech/records_policy_standards/records_management_standards/index.shtml

[19] Refer to NT OIC guideline Privacy – Openness for more information.

- the organisation reasonably believes that the person receiving the information is subject to a law, or a contract or other legally binding arrangement, that requires the person to comply with principles for handling the information that are substantially similar to these IPPs; or
- the individual consents to the transfer; or
- the transfer is necessary for the performance of a contract between the organisation and the individual or for the implementation of pre-contractual measures taken in response to the individual's request; or
- the transfer is necessary for the performance or completion of a contract between the organisation and a third party, the performance or completion of which benefits the individual; or
- all of the following apply:
  - the transfer is for the benefit of the individual;
  - it is impracticable to obtain the consent of the individual to the transfer;
  - it is likely that the individual would consent to the transfer; or
- the organisation has taken reasonable steps to ensure that the information will not be held, used or disclosed by the person to whom it is transferred in a manner that is inconsistent with these IPPs.

Questions to ask

- Will information be transferred outside the Northern Territory, for example, stored with a cloud-based service that uses servers physically located in another state or country (other than Australia)?
- Will agreement from the individual need to be sought? If so, what process will you use to obtain the individual's valid agreement, ie that the agreement is voluntary, informed, specific and current?
- What process or procedure will there be for an individual to pursue a privacy complaint for breach of privacy?

Outsourcing

Take all reasonable steps to bind a contract service provider to compliance with the privacy principles.

Questions to ask

- Will the project involve your agency engaging an external service provider to perform a function or activity for the benefit of the agency, or to a third party of behalf of the agency? Is the contractor an interstate or overseas-based entity? (see points above) Will a flow of personal information be necessary for the service provider to fulfil the function being outsourced? **If yes:**
  - What steps will your agency take to ensure that the service provider is bound to comply with the privacy principles outlined in the *Information Act* (NT)?[20]
  - Is the contractor bound by any other Australian legislation that contain privacy principles? For example, the Australian Privacy Principles outlined in the *Privacy Act 1988*.
  - Who will be responsible for dealing with access and amendment applications in relation to personal information held by the contract service provider?
  - How will the information be destroyed after the contract with the service provider is completed?

[20] For further guidance on contract negotiations for external cloud services refer to the NTG Cloud Computing guideline - contract negotiations for external cloud services.

APPENDIX D – COMMON PRIVACY ISSUES AND POTENTIAL WAYS TO ADDRESS THEM

The following common privacy issues and potential actions to address them are only intended to prompt your own analysis and assessment.

Not every listed privacy issue will be relevant to your project, nor will every privacy issue associated with your project necessarily be included here. You should also bear in mind there are many different actions that can be taken to ensure compliance with the *Information Act* and the suggested actions below may not be the most appropriate approach for your agency.

Privacy issue	**Potential action to ensure compliance with the *Information Act***
Collection	
Collecting more personal information than is needed to fulfil the stated purpose.	Check that every piece or field of data you intend to collect can be justified. For example, do you need to collect a street address if all you need is a postal address? Consider whether the precision of information can be reduced. For example, if you need to know a person's age in order to provide age-appropriate services, ask for the person's age range or year of birth, not their exact date of birth. Design questions to elicit only relevant information. For example, if you are checking whether language assistance is needed, asking 'Do you need an interpreter? If yes, for what language?' rather than 'Spoken languages' will avoid collecting information for which you have no purpose.
An individual was not aware that it is the agency's usual practice to disclose their personal information to a third party.	Ensure that a consistent collection notice is provided across all methods of collection, including paper forms, downloadable forms, web forms, over the telephone or face to face. Identify additional opportunities to provide a collection notice, for example, not only before or at the time of collection, but when providing acknowledgement or receipt of the personal information. Consider whether a layered collection notice is useful. Providing a brief collection notice on the form may be more readily accessible and this could then be supplemented by a longer notice on the agency's website or vice versa.
The collection of personal information could be considered 'unfair' if an individual was under the impression that their personal information was required by law.	If you are required or authorised by law to collect personal information, ensure that there is clear distinction between this information and any other personal information you are collecting which is not required by law(for example, demographic information).
Individuals may be unaware of a usual practice by your agency to disclose their personal information.	Ensure you have included all foreseen routine disclosures in an appropriate collection notice, including any disclosure that will be authorised or required by law.
Collecting demographic information about a person could be seen as intrusive and may affect the way that individuals engage with your agency, for example, the person may be more likely to give false answers to protect their privacy.	Have a specific purpose in mind for the personal information before collecting it and collect only that information which is necessary to fulfil that purpose. Ensure that the collection notice explains what this information will be used for. Make it clear which personal information is being collected for demographic purposes and indicate that this information is optional.

Storage and Security	
Use of portable storage devices (for example, USB drives) increases the risk of unauthorised disclosure or accidental loss of personal information.	Control the use of portable storage devices through technical controls (for example, hardware-encrypted storage drives) and implement policy and procedures so that employees understand their obligations when using portable storage devices.[21]
Storing identifiable personal information in cloud facilities can pose security risks	Ensure compliance with the NTG *Cloud Computing Guidelines*, *Cloud Computing Standard*, *Cloud Computing Policy* and follow all recommendations for security and privacy compliance. Consider whether contract provisions are required to shift liability for privacy breaches from the agency to the contract service provider or vendor.
Keeping data for longer than it is required increases the risk of a data security breach, or unauthorised use or disclosure.	Ensure that retention periods have been prescribed for the personal information and that there is a mechanism for identifying when the personal information is no longer needed.
Failing to implement appropriate security safeguards can increase the risk of unauthorised access, use, modification or disclosure.	Check that the measures used to secure personal information against loss and unauthorised access, modification, use and disclosure are proportionate and appropriate to the possible risk of a security breach and the level of harm that could result from a breach? Consider whether a threat and vulnerability assessment is necessary to identify appropriate security measures (for example, where a web application, online portal or remote access technology is used to provide access to the information). Document security handling practices and provide ongoing awareness activities and training. Consider developing targeted training for specific job roles.
Using regular post to send personal information can increase the risk of unauthorised disclosure.	Use registered post to send sensitive information or any other personal information that could cause embarrassment, loss or hurt to the person if it were received by someone else. Use window envelopes to avoid mixing up labelled envelopes and their intended contents for bulk mail-outs.
Testing and training environments may expose personal information to unauthorised disclosure.	Ensure your project will use only dummy data in testing and training environments.
Access and amendment	
An individual cannot find out what type of personal information is held by your agency, the purpose for which the information is used and what they need to do to obtain access to documents that contain their personal information.	Ensure an up-to-date list of your agency's list of personal information holdings is readily available to anyone who asks for it. Ensure call centre staff are aware of who in the agency can answer privacy enquiries.
Poorly managed amendment requests can frustrate people and can lead to poor data quality.	Consider whether a policy is needed that sets out who in your agency can action routine or simple amendment requests, and which types of amendments will require a formal application under the *Information Act*.
Use and disclosure	

[21] For further guidance, please refer to NT OIC Cloud Computing and Privacy Principles Guidelines.

Inaccurate, out of date or incomplete information is used, which may lead to inappropriate decisions that have a negative impact on the individuals concerned.	Consider implementing procedures for how often personal information will be reviewed and updated. Identify any circumstances in which particular personal information must be checked before it can be used for a particular purpose. Ensure the date and source of the last update is recorded when data is updated or amended.
An individual's refusal of consent, or conditional consent, is not respected.	When relying on consent to authorise a secondary use or disclosure, ensure there is a workable mechanism by which the wishes of a person who refuses consent, or provides conditional consent, are recorded and acted upon promptly. If providing a mechanism for individuals to agree to their information being used or disclosed, preference is given to an 'opt in' before the 'opt out' mechanism.
Personal information will be shared with another agency.	Establish the purpose for the sharing of the personal information before any sharing occurs. Identify which of the exemptions in the *Information Act* will be relied on to permit this use or disclosure.
An individual is able to be identified from de-identified data.	Assess the likelihood of re-identification before disclosing de-identified data by considering factors such as: • the amount of alternative information about the individuals contained in the dataset that is publicly available • the ease of access to the alternative information • the level of detail provided • the number of steps and the associated amount of time, resources and effort required to identify an individual • how up to date the information is; and • the extent to which only people with personal knowledge of individuals such as family or close friends would be able to identify an individual.
Offices open to the public pose a risk of unauthorised access to or disclosure of personal information.	Implement physical security measures such as preventing public access to areas where personal information is stored or used. Ensure access to separate meeting rooms in which no information is stored so that meeting can take place without the risk of people accessing personal information.
Contract Service Providers	
A contract service provider will in any way deal with personal information to provide services under an arrangement to perform one or more of the contracting agency's functions.	Take reasonable steps to ensure that the contract service provider is bound by contract to comply with section 149 of the *Information Act*.
Transfer of information outside Australia	
Personal information will be stored in an overseas cloud-based solution.	Check where the cloud provider operates from, even when dealing with an Australian company. If the servers used by that provider are not located in Australia, you will need to consider how the obligations in IPP 9 are satisfied.[22]

[22] For resources regarding Cloud Computing go to: NT OIC Guideline Cloud Computing and Privacy Principles and the NTG Cloud Computing Policy and Standards for more information.

APPENDIX E – PIA REPORT FORMAT

Suggested content to be included in a PIA report is set out below. The format of the report should be tailored to suit the size and complexity of the project.

Section	Content
Executive summary	Depending on the length of the PIA report, it may be necessary to provide an Executive Summary. This could include: • the purpose of the PIA • brief project description and key information flows • summary of findings; and • recommended actions to ensure compliance with the *Information Act*.
PIA methodology	Outline the purpose of a PIA, who conducted the PIA, timings, and the key steps that were taken to complete the PIA.
Project description	Provide a description of what the project will deliver and what it will achieve, why the project is needed, any links with existing projects, who is responsible for the projects and timeframes in which the project will be delivered.
Personal information flow	Describe how personal information will be handled in the project, from beginning to end. This should be sufficiently detailed to explain what information will be collected, how it will be collected, how it will be stored, and who will have access to it what it will be used for, and any third parties to whom it will be routinely disclosed. Where appropriate, consider using diagrams to help illustrate information flow.
Stakeholder consultation	Detail what stakeholder consultation was undertaken, timing, who was consulted, method of consultation, the focus of the consultation, whether any further consultation will be necessary and what feedback was provided.
Privacy issues	Outline what privacy issues were identified by comparing the project's personal information handling practices against the privacy obligations set out in the *Information Act*.
Recommendations	Outline the recommended actions that are necessary to ensure compliance with the *Information Act*. Where appropriate, prioritise the list of recommended actions or set target dates by which the issue needs to be resolved.
Conclusion	Summarise significant findings and critical recommendations.
Appendices	Appendices can be used to communicate more detailed information, for example: • questions asked of stakeholders and the responses that were provided; and/or • what options were considered to address the identified privacy issues and the cost, risk and benefit analysis of each option.

APPENDIX F - CHECKLIST

Use this checklist as a guide to ensure that you have completed everything and received the correct approvals/endorsements

Task	**Date completed**
Conduct a threshold assessment – See Appendix A	
*Prepare the PIA report – See Appendix E *This task incudes:* ○ *Describe the project* ○ *Identify and consult with stakeholders* ○ *Map the personal information flow* ○ *Identify the privacy issues and options to address the privacy issues* ○ *Include privacy protection clauses in service provider contract/agreements* ○ *Action the agency's response to the PIA report*	
*Endorsement of PIA by relevant line manager	
*PIA noted by relevant leadership group representative	
*PIA noted by departmental Privacy representative	
*PIA noted by Audit and Risk representative	

* Only applicable if PIA is required after threshold assessment recommendations