Australian Government

Office of the Privacy Commissioner

Privacy Impact Assessment Guide

Revised May 2010

Table of Contents

Introduction to Privacy Impact Assessment

1 About this Guide

This Guide gives an introduction to conducting a Privacy Impact Assessment (PIA). It includes:

- **Overview of a Privacy Impact Assessment:**
  - what is a PIA?
  - PIA purpose
  - when to do a PIA
  - PIA benefits.
- **Is a PIA necessary?** Provides a *threshold assessment* that helps you decide whether *your* project needs a PIA.
- **Approaching the PIA:** Introduces key PIA stages and some tips for planning the best process for *your* project. **Note:** The Guide does not impose a particular PIA style but suggests a flexible approach depending on the nature of the project and the information collected.
- **Doing the PIA:** Gives practical details about PIAs and more information about the key stages.
- **Modules A-F:** Provides useful, practical tools to be used at specific stages.
- **Acknowledgements and Resources:** Offers some useful national and international PIA resources.

2 Meaning of terms

The terms used in this guide have these meanings:

- **Organisation:** For simplicity, this guide uses the term 'organisation' to refer to government agencies and to private and not for profit organisations, unless there is a specific need to do otherwise, eg in relation to modules E and F.

- **Personal information / information privacy:** The *Privacy Act 1988*[1] (Cth) (the Privacy Act) regulates the way certain government agencies and private sector organisations handle an individual's personal information. The Privacy Act defines 'personal information' as**:**

  "…information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."[2]

  Personal information does not always need to include specifics such as an individual's name. It can be any information that can help work out an individual's identity.

  Important: Information privacy is only one aspect of privacy. Other types of privacy include bodily privacy, territorial privacy, and communications privacy.[3] These can be considered in the PIA process, particularly where they may pose risks to the overall success of the project.

- **Privacy impact:** Means either a known impact or a risk of impact.

- **Project:** This means the activity you are assessing. The project may be any proposal, review, system, database, program, application, service or initiative that includes handling of personal information. A PIA can be used on any project that handles personal information.

- **Sensitive information** is defined in the Privacy Act[4] and applies to organisations. It is:

  (a) information or an opinion about an individual's:

  I. racial or ethnic origin; or

  II. political opinion; or

---

1 Unless otherwise stated, all references are to this Act.

2 Section 6 of the Privacy Act.

3 For a summary of different types of privacy, see 'What's privacy', R Clarke 2006, at: www.rogerclarke.com/DV/Privacy.html.

4 Defined under s 6 of the Privacy Act and the subject of NPP 10. The term is not used in the IPPs, but the Government's response to the ALRC Report 108 on privacy indicates that it will form part of a single set of principles to be applied to both government agencies and organisations. That response also indicates that biometric information and templates will be added to the definition of sensitive information. For the Government response see: www.dpmc.gov.au/privacy/alrc.cfm.

III. *membership of a political association; or*

IV. *religious beliefs or affiliations; or*

V. *philosophical beliefs; or*

VI. *membership of a professional or trade association; or*

VII. *membership of a trade union; or*

VIII. *sexual preference or practice; or*

IX. *criminal record;*

that is also personal information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information.

√ **This symbol highlights key privacy messages.**

✗ **This symbol highlights privacy risks.**

Overview

3 What is a PIA?

√ **A PIA "tells the story" of a project from a privacy perspective and helps to manage privacy impacts.**

A PIA is an assessment tool that "tells the story" of a project from a privacy perspective.[5] A PIA:

- Describes how personal information flows in a project.
- Analyses the possible privacy impacts on individuals' privacy.

[5] Professor David Flaherty, Professor Emeritus, University of Western Ontario.

- Identifies and recommends options for managing, minimising or eradicating these impacts.

  Example: Helping to identify when particular personal information collection may be unnecessary, or when the project has poor accountability or oversight processes.

- Analyses the project's effect on individual privacy.
- Helps find potential solutions and manage privacy impact through this analysis.
- Can make a significant difference to the project's privacy impact and still achieve or enhance the project's goals.
- Encourages good privacy practice and underpins good public policy in the project or, in the private sector, underpins good risk management.

4 Why do a PIA?

√ **A PIA helps to ensure the project's success.**

The Privacy Act does not refer to PIAs or require organisations to do one.

Whether a project succeeds will depend on how it meets legislative privacy requirements and broader community privacy expectations.[6] Privacy issues that are not handled properly can impact on the community's trust and undermine the project's success. It is in your organisation's interests to do a PIA for any projects that handle personal information.

Risks may include:[7]

- **Non-compliance** with the letter *or* the spirit of relevant privacy law – leading to a privacy breach and/or negative publicity.
- **Public concern and/or loss of credibility:** A perceived loss of privacy or failure to meet expectations about how personal information will be protected, which may result in damage to brand reputation.

---

[6] Making an assessment of the community's broader expectations about privacy can be difficult. More information about the Office's research into Australian privacy attitudes is available at www.privacy.gov.au/materials/types/research/view/6613.

[7] For more discussion of the risks associated with failing to consider a project's privacy implications see *Privacy Impact Assessment: A User's Guide* available at the Government of Ontario's Access and Privacy Office website at www.accessandprivacy.gov.on.ca/english/pia/index.html.

- **System redesign:** An adjustment to the project (at considerable expense and often late in the development stage).

5 Benefits

√ **A PIA helps to avoid costly or embarrassing privacy mistakes.**

Dealing with a project's privacy impacts can be challenging. Doing a PIA puts you in a more informed and stronger position to help you meet those challenges.

Identifying and analysing privacy impacts during a project's design phase allows you to:

- manage any negative privacy impacts
- avoid costly or embarrassing privacy mistakes.

More specific PIA benefits are discussed below.

Compliance with privacy law

A PIA can help identify what needs to be done to ensure that a project complies with privacy law and other legislative requirements.

The Privacy Act's principles provide minimum privacy protection in the way personal information is handled. Organisations may also have to comply with other privacy-related legislative requirements (such as secrecy provisions, industry codes or state legislation), as well as more general public or private sector obligations.

A PIA can:

- include a list of relevant privacy laws
- help identify and make any necessary adjustments during a project's development (so that it will comply with relevant privacy laws)
- discuss how the project's information-handling practices and business rules comply with specific legal obligations.

More information

- www.privacy.gov.au.

Reflecting community and organisational values

Complying with relevant privacy law is fundamental to assessing and managing privacy impacts. Compliance underpins a PIA, but it is not the whole story.

A project can have an adverse impact on an individual's privacy in many ways, and other considerations may need to be taken into account when assessing the project's impact.

As a community and as individuals we value our privacy.[8] We try hard to strike a balance between meeting our personal needs and goals, and appreciating what others need or want to know about us. Privacy underpins our human dignity and gives us a measure of control in our everyday interactions, and how our personal information is handled in the wider world.

A PIA gives organisations the opportunity to:

- consider the values the community places on privacy – trust, respect, individual autonomy and accountability
- reflect those values in the project.

A PIA also gives the organisation the opportunity to assess the project against its own values or business rules, which may add further to the legislative provisions.

To achieve the right balance, organisations should:

- consider their interests, broader community interests and the interests of the individual
- take steps to ensure that any identified privacy impacts do not outweigh the project's public benefit or, for private sector organisations, the overall organisational values and objectives.

Project risk management

PIA information feeds into broader project risk management processes.[9]

---

8 OPC Research into Community Attitudes To Privacy in Australia 2007: www.privacy.gov.au/materials/types/download/8820/6616.

9 The *Australian/New Zealand Risk Management Standard* (AS/NZS 4360:2004) and the companion handbook *Risk Management Guidelines* (HB 436:2004) are used in government to assist in the process of assessing and managing project risks.

This will put you in a better position to assess the project's privacy impact risks and help you work out the most appropriate strategy to deal with them.

Other benefits

Other PIA benefits include:

- Finding privacy solutions that progress the project's goals.
- Identifying particular privacy impacts such as:
    - function creep[10]
    - new legislation or technology.
- Improving the project's consultation process, including public consultation. Privacy issues are more comprehensively identified and stakeholders are better informed about the project's privacy and information handling aspects.
- Demonstrating that the project has critically analysed the handling of personal information with privacy in mind.
- Clearing up misconceptions about what is going to happen to the information.
- Playing a broader educational privacy role which can have far-reaching benefits – not only to the project at hand but to the organisation and the community as a whole.

6 How does a PIA work?

√ **A PIA works best when it evolves with the project.**

A PIA works most effectively when it evolves with and helps to shape the project's development. This ensures that privacy is 'built in' rather than 'bolted on'.

Making a PIA an integral part of the project from the beginning, means that you can:

- describe the personal information 'flows' fully and systematically

[10] Additional uses of a system, and/or the personal information, which 'creep' away from the original stated uses and/or from individuals' original expectations.

- analyse how the flows will impact on privacy
- identify any potential for privacy erosion early in the process (such as function creep)
- consider alternative, less privacy-intrusive practices during development (not retrospectively)
- make informed choices and recommendations about how to proceed.

Documenting a PIA is usually an evolving process. As the project develops and the issues become clearer, the PIA document can be updated and supplemented, giving you a more comprehensive and useful record.

Note: Projects which have significant scope may need more than one PIA.

7 When a PIA will be important

✓ **The project's significance and the extent to which personal information is handled.**

A project's significance and the extent to which it collects, uses or discloses personal information, generally indicates:

- the importance of a doing a PIA
- the level of detail it will need.

The greater the project's size, complexity or scope, the more likely it is that a comprehensive PIA will determine and manage its privacy impact.

Example 1: What proportion of the community is affected by the project, and the impact it may have on those individuals.

Example 2: Projects that include significant amounts of personal or sensitive information.[11]

8 Who does the PIA?

Generally, whoever is handling the project is responsible for deciding if a PIA is necessary or desirable and ensuring it is carried out.

[11] Sensitive information includes health information (See s 6 of the Privacy Act for more information).

Usually, a PIA will not be done by a staff member working in isolation. It will have different stages and personnel as the project evolves. So, a PIA generally means a team approach. It makes use of the various 'in-house experts' available (including the Privacy Contact Officer) and outside expertise as necessary. Having someone look over a project through 'fresh eyes' can help to identify privacy impacts not previously recognised.

Note: Some projects will have markedly more privacy impact than others. A robust and independent PIA conducted by external assessors may be preferable in those instances. This independent assessment may also help the organisation to develop community trust in the PIA findings and the project's intent.[12]

9 Consultation and transparency

Consultation with key stakeholders is basic to the PIA process. It helps to ensure that key privacy issues are noted, addressed and communicated.

A PIA should always consider community privacy attitudes and expectations. Affected individuals are likely to be key stakeholders, so wider public consultation is important, particularly where a lot of personal information is being handled or where sensitive information is involved. Public consultation also adds to community awareness about the project and can increase confidence in the way the project (and the organisation) is handling personal information.

The consultation's extent and timing will vary depending on the project stage – preliminary, sensitive or confidential.

Publishing the contents and findings of a PIA:

- adds value
- demonstrates to stakeholders and the community that the project has undergone critical privacy analysis
- contributes to the transparency of the project's development and intent.

[12] A number of privacy consultancies and law firms offer PIAs as a service. The Office does not endorse or recommend a particular organisation, but its privacy service providers' page at www.privacy.gov.au/aboutprivacy/helpme/psp includes some PIA providers.

Is a PIA Necessary?

10 Threshold Assessment

✓ **Will personal information be collected, used or disclosed in the project?**

Important: Not every project will need a PIA.

The first question to ask when assessing whether a PIA is needed is:

'Will any personal information be collected, used or disclosed

in the project?'

This is known as a *threshold assessment.*

If personal information is not involved in the project at any stage, the project may have a negligible impact on information privacy, and a PIA will generally not be necessary.

A threshold assessment allows projects with no or minimal information privacy implications to be identified relatively easily and quickly. To make this assessment you will need to:

- broadly describe the project and its aims
- determine whether any personal information will be handled.

If no personal information is being handled, you might still decide to conduct a PIA if you wish to show how you are avoiding the use of personal information. You might also find it useful to show how the project will deal with other kinds of personal privacy, such as bodily, territorial and communications privacy.

Module A will help organisations to make this threshold assessment.

Key stages and planning

11 Key stages

Once you decide that a particular project needs a PIA, the next question will probably be:

'What PIA approach will be most appropriate?'

Remember: There is no one-size-fits-all PIA model.

The various PIA models at Appendix A: *Acknowledgements and Resources* may help your organisation to work out the best approach for your project/s.

Some models focus on compliance with a particular jurisdiction's privacy legislation, but they all have some means of measuring a project's privacy impact. Generally, there are five key stages to the PIA process.

5 key PIA stages

1. **Project description:** Broadly describe the project, including the aims and whether any personal information will be handled.
2. **Mapping the information flows and privacy framework:** Describe and map the project's personal information flows and document all relevant legislative and organisational rules.
3. **Privacy impact analysis:** Identify and analyse the project's privacy impact.
4. **Privacy management:** Consider how to manage any privacy impact, particularly options that will improve privacy outcomes and still achieve the project's goals.
5. **Recommendations:** Produce a final PIA report covering the above stages and including recommendations.

A PIA should address all of the key stages. The project will determine how much detail is necessary at each stage.

12 Planning

√ **The significance of the project and the extent to which personal information is handled.**

The project's nature and stage of development will determine the most appropriate PIA process. A project may:

- Be at a conceptual or at a more advanced stage of development.
- Have a limited or broad scope.
- Be an 'incremental' program (altering a well-established existing program) or a significant new one. **Note:** An incremental project can also have broad scope and privacy implications.
- Involve a limited or significant amount of personal information.
- Include information which is sensitive in nature[13].

Module B gives some guidance and examples about how the PIA process can differ depending on the type of project or the stage it is at.

Doing the PIA

13 Project description

√ **Describe the big picture.**

A PIA needs a broad, 'big picture' description of the project, including:

- The project's overall aims.
- How these aims fit with the organisation's broader objectives.
- The project's scope and extent.

[13] For government agencies: Although the IPPs do not mention sensitive information for the conduct of a PIA, it is useful to consider information that is sensitive in nature. A guide to agencies as to what information is sensitive can be gathered from the definition in section 6 of the Privacy Act.

- Any links with existing programs or other projects.
- Some of the key privacy elements. **Example:** The extent and type of information that will be collected, how security and data quality are to be addressed, and how the information will be used and disclosed.

This information is important as it gives you context for the rest of the PIA. Any *Threshold Assessment* information (see **10** above) can also be usefully included at this stage.

14 Mapping information flows and privacy framework

Understand how the information flows in the project and what are the privacy-related legislative and organisational rules.

Now that you have a broad outline of the project's nature and scope, you need to describe and map the project's personal information flows.

To do this effectively you will need to communicate with other staff (and stakeholders). If you try to do this in isolation, you run the risk of overlooking valuable information about how the project will work, and how personal information will be handled. This could cause your organisation problems later on that may be difficult or expensive to remedy.

Detailed information mapping should include:

- what personal information will be handled
- how the personal information will be collected
- how it will be used
- internal flows
- disclosures
- security measures
- data quality measures
- any privacy, secrecy or other relevant legislation applying to the information flow

- any organisational or other business privacy rules applying to the information flow.

Mapping should also describe the current personal information environment and how the project will affect it.

Example: If a project involves new uses for personal information you already hold, identify and describe the information and the original collection context (including the purpose of the collection).

Once the mapping is done, you can begin preliminary assessment of privacy impact or compliance issues and start thinking about how you might handle them, including:

- the way personal information is collected, used and disclosed
- the way individuals can *access* information about them, and *correct* it if necessary
- *security* safeguards
- *data quality processes*
- whether an *identity management* system is involved.

Module C will help you get a clear picture of the project's information flows so that you can begin to identify and assess possible privacy issues.

15 Privacy impact analysis

√ **Privacy impacts affect individual choice.**

Now that you have mapped the information flows, you need to identify and critically analyse how the project impacts upon privacy – positively *and* negatively.

Analysis should include:

- serious privacy impacts and impacts that are less so
- whether the impacts are necessary or avoidable
- how the impacts may affect the project's broad goals
- the project's affect on an individual's choices about who has access to particular information about them

- whether the project has acceptable privacy outcomes, or unacceptable privacy impacts (include any stakeholder or public consultation results that will help you to work out how to improve the privacy outcome).

Factors influencing analysis include:

- The content and context in which the information is collected.

  A negative privacy impact may not be significant at first glance. But, the simplest personal information, handled inappropriately, may impact on someone's privacy in ways the organisation did not intend.

  Example: You want to put individuals' personal information on a public register. The privacy impact could mean that one or more persons could be under threat of harassment or violence and their personal safety put at risk.

- Some types of personal information are more sensitive than others, such as genetic, general health or criminal conviction information.

- Other legislation may apply to the way certain information is handled.

Module D is a starting point for analysis and should help you draw out the project's privacy impacts.

Modules E and F ask about compliance issues in relation to the Privacy Act principles. Module E is for government agencies and Module F is for private sector or not-for profit organisations. These modules cover some of the same issues that you looked at when you mapped the information flows but they focus more closely on compliance with the Privacy Act. Note that there may be other privacy-related legislation and organisational rules that apply to your organisation, for example, state-based legislation that you need to consider apart from the Privacy Act principles.

16 Privacy management

√ **Privacy protection and project goals can both be achieved.**

At this stage you have to work out and consider what options may help you get rid of or lessen any negative privacy impacts identified in your project.

This does not necessarily mean compromising your organisation's goals. You may find options that will make a significant difference to the privacy impact and still allow you to achieve the project's goals.

Example: Using privacy enhancing technologies (PETs)[14] to minimise collection of personal information while still allowing your organisation to achieve the project's functions.

Module F – responses or actions and negative privacy impacts.

This stage can also feed into broader project risk management processes (see **5** above).

17 Recommendations

Setting out all PIA information (analysis, assessment and any other relevant material) in a report is very useful.

The report should include any recommendations for the project's future. A PIA that *critically* focuses on all project elements can produce a variety of recommendations.

Note: These recommendations may not meet all your expectations.

Example: The PIA may recommend further fine-tuning in a particular area of the project, such as your organisation's collection practice.

Aim of the report

The PIA report should identify avoidable impacts or risks and recommend ways to remove them or reduce them to an acceptable level, including:

- changes that will achieve a more appropriate balance between the project's goals, the interests of affected individuals and the organisation's interests
- the need for further consultation
- whether the privacy impacts are so significant that the project should not proceed.

  Some examples of PIA reports can be found at **Appendix A: *Acknowledgements and Resources***.

[14] For an introductory discussion of Privacy Enhancing Technologies (PETs) and Privacy Intrusive Technologies (PITs), see *Under the Gaze, Privacy Identity & New Technology*.

18 After the assessment … what then?

Documenting a PIA – its analysis, assessment, findings and recommendations – gives you an ongoing, useful decision-making tool. The document becomes a valuable resource for the project team, senior management and other stakeholders and can also inform and educate others involved in, or affected by, the project.

Examples

- The PIA should feed into planning the project's next steps. This could include resource allocation (including training), stakeholder management, senior management briefing, designing, trialling, testing, consultation, public education and evaluation.
- As the project progresses, the PIA may need to be revisited and an updated or revised version produced to take account of developments in the design or implementation of the project.
- PIA recommendations successfully implemented can form part of a post-implementation review.

The Privacy Commissioner encourages organisations, where appropriate, to:

- include the PIA findings in any further public consultation on the project
- make the PIA findings available to the public as part of the project's implementation.

The Privacy Commissioner acknowledges that there may be circumstances where the full or part release of a PIA may not be appropriate. For example, the project may still be in its very early stages. There may also be security, commercial-in-confidence or, for private sector organisations, other competitive reasons for not making a PIA public in full or in part.

However, transparency and accountability are key issues for good privacy practice and outcomes, so where there are difficulties making the full PIA available, the Commissioner encourages considering the release of a summary version.

19 Role of the Office

The Office has no formal role in the development, endorsement or approval of PIAs. However, subject to available resources, the Office may be able to help organisations with advice during the PIA process.

MODULE A – Threshold Assessment

1 If an organisation or government agency bound by the Privacy Act is developing a project that involves personal information, it must comply with that Act. Your organisation is responsible and accountable for the personal information it collects, even when the information is held by external service providers or contractors operating in Australia or overseas.

How Threshold Assessment works

2 A *Threshold Assessment* helps you work out, early in the project**,** whether a PIA is necessary. There is no hard-and-fast rule about when to do a PIA, and each project must be considered individually.

3 The *Threshold Assessment* establishes whether the project collects, uses or discloses personal information. Generally, if personal information is not involved in the project, the project is unlikely to impact on information privacy and a PIA will not be necessary. [15]

Note: Just because there is no personal information collection in a project does not guarantee that there will be no information privacy impact.

Example: A project will use de-identified information. The PIA could explain how and why this information will be used and how the agency will prevent the future re-identification of the data.

What is personal information?

4 Under the Privacy Act, personal information does not always have to include details such as an individual's name. It may include other information that can identify an individual or allow their identity to be worked out[16] (see *Meaning of terms* for a full definition of personal and sensitive information).

5 What appears to be de-identified or unidentifiable information to the record-keeper, may allow others in the community to identify an individual.

---

[15] This Guide deals with information privacy, but other types of privacy (such as bodily, territorial or communications privacy) can also be considered using the methodology of a PIA, especially where they may pose risks to the overall success of the project. For a summary of different types of privacy see, 'What's privacy', R Clarke 2006, at: www.rogerclarke.com/DV/Privacy.html.

[16] *Meaning of terms* has a full definition of personal and sensitive information.

Example: Generic information about ethnic origin may not, by itself, identify an individual. But, if ethnicity and other information is disclosed about an individual in a small town (that has only a limited number of people from that ethnic background) the person could be identified and the information could become personal information under the Privacy Act.

7 Personal information may be collected directly from an individual or indirectly from another source, so collection should be considered broadly.

Threshold Assessment Template

1. Organisation.

2. Contact details of the person responsible for completing this Threshold Assessment.

3. Brief description of the project.

The Guide (**11: *Project description***) makes suggestions about what could be usefully included in a broad project description (including when modifying an existing program).

4 Does the project involve the collection, use or disclosure of personal information?

- See *What is personal information?* (*Meaning of terms*).
- Briefly describe the personal information (if any) that will be collected, used or disclosed (such as name, address, date of birth, health information and so on).
- Explain some of the key privacy elements.

  Example:

  - the general purposes for which information will be collected, used and disclosed
  - any authority under which it is collected
  - the nature and sensitivity of the personal information and so on.

If the project is going to modify an existing program, describe the changes (if any) to the way personal information will be handled.

Yes ❑ No ❑

If you have answered YES to question 4 then some form of PIA will probably be necessary. See **Section 9: *Key stages of a PIA*** of the Guide to continue.

Note: *if you decide that a* ***PIA is necessary****, please keep the description of the project from* ***question 3*** *above and include it in the PIA.*

Sign off below and keep this Threshold Assessment for your records.

Name _____ Name_____

Signature_____ Signature_____

(Proponent) (Proponent's manager)

Date: _____ Date: _____

MODULE B – Nature of the Project

Broadly assessing a project will help an organisation decide on the most appropriate PIA process. Assessment will generally include:

- **The project's scope:** Is it limited or broad?
- **The type:** Is it a new program, or altering an established existing program?
- **The stage of development:** Is it at a conceptual or a more advanced stage of thinking?

Project scope

To assess the project's scope look at key attributes, including the:

- **Quantity** of the personal information handled.
- **Sensitivity** of the personal information involved, such as biometric or genetic components.
- **Significance** of the project – its size or complexity.
- **Interaction** – the degree of cross organisation or cross-sector involvement needed. **Example:** Sharing or data-matching across organisations or jurisdictions.
- **Public impact** of the project and its significance. **Example:** Handling significant amounts of personal information about each individual, or about a significant number of individuals.

A project's privacy scope can increase depending on the risk of adverse privacy impacts.

Example

- personal information handling will be or has been **outsourced**
- **new legislation or new technology** will be needed for handling this personal information
- personal information will be aggregated in **databases**
- entirely **new collections** of personal information are planned (e.g. because there are new functions)

- a **new method** of using or disclosing personal information is being introduced.

Generally, the greater the scope of the project, the more likely it will be that:

- a PIA will help determine and manage the project's privacy impacts
- the PIA will be more detailed.

Type of project and stage of development

Consider:

- the **type** of project. Is it new or adding to an existing project (incremental)?
- the **stage of development.** Is it conceptual or more advanced?

This Guide does not recommend a particular PIA process for the various types of projects organisations will develop. Some PIA examples (Appendix A) demonstrate how the process can vary for different project types or for projects at different stages. These examples are not exhaustive.

Incremental projects

If a project is incremental, the Guide should be applied to the new personal information flows, unless the existing program or system will benefit from a PIA.

Incremental projects can be as significant in their scope and privacy implications as any other project. The more significant the scope the more comprehensive the PIA should be.

Example A: Incremental projects of limited scope

If a project is incremental and relatively limited in scope, only a short PIA may be needed.

Example: A project making a relatively minor adjustment to an established, existing program, or securely collecting and using a very limited amount of personal information (not sensitive information).

Note: Even a shorter PIA should address all the key stages. But, you may find that:

- the degree of mapping of information flows needed is quite small
- there are fewer questions that require answers
- the privacy impact analysis shows the privacy impacts are minimal
- there are fewer recommendations
- the final report is brief.

Example B: Projects at conceptual stage of development

Initially, projects at the conceptual stages of development may only be able to address the PIA key stages in a less-detailed way.

Example: Information flows can only be mapped from the information available at the time, limiting the preliminary analysis of privacy impacts and possible management strategies.

As the project develops and the issues become clearer, the PIA can be updated and supplemented, becoming more comprehensive.

In significant projects, preliminary reports and interim recommendations will be important to ensure that privacy is built in.

Example C: Significant projects at advanced stages of development

Projects that have broad scope and are at a relatively advanced stage of development will need a comprehensive PIA (or sometimes more than one). A comprehensive PIA will work through the key stages in much more detail. However note that it is best practice to undertake a preliminary PIA early in the concept/design stage to head off any potential privacy impacts before they become entrenched in the planning process.

MODULE C – Mapping Information Flows

Describe and map the project's personal information flows. This will form the basis of the analysis of the project's privacy impacts, including:

- the ***collection*** of personal information
- its ***use*** and ***disclosure***
- the ability individuals have to ***access*** information about them
- the ability individuals have to ***correct*** information about them if need be
- the applicable ***security*** safeguards
- the processes for ensuring ***data quality***
- whether an ***identity management*** system is involved.

The questions below will help you describe how your project deals with each of these areas and draw your attention to any privacy issues.

Your responses should be documented and used for privacy impact analysis. They will also be useful for any PIA reports.

1 Collection

√ **Good collection practices underpin good privacy**

✗ **Collecting unnecessary or irrelevant personal information, or intrusive collection.**

Describe:

- how the collection relates to the organisations functions or activities
- what public interest justifies the collection
- why the personal information, including the particular items and kinds of information, are necessary for the project
- whether the information can be collected in a de-identified or anonymous way

- whether individuals can choose not to provide some or all of the personal information
- how the information will be collected
- if the method will be unreasonably intrusive for some individuals.

  Examples:

  - Making individuals talk about intimate or sensitive information in a public area where others can overhear.
  - Collecting images of individuals' private activities without their knowledge.

1.1 Scope of collection

√ **Detail the collection process.**

✗ **Bulk collection of personal information, some of which is unnecessary or irrelevant.**

Describe:

- The personal information to be collected.

  Example: Name, address, occupation, identification numbers.

- Where the information is to be collected from.

  Example: Directly from the individual or from other individuals, organisations or publicly available sources.

- Why each element of the information is being collected.
- Whether the information will be paid for or exchanged for something of value.
- How an individual's circumstances will be taken into account when the personal information is being collected.

Example: Cultural diversity, hearing impairment, languages other than English.

Example: Identify the purposes for each collection, the sensitive nature of the collection, including: financial, political or religious beliefs, health, sexual practices, biometric or genetic information.

- Any statute, authority or requirement you are relying on to collect the information.
- Collection alternatives that have been considered and rejected. **Example:** Using de-identified data.

If you are getting the individual's consent to the collection, outline what other matters may depend on that consent. **Example:** Is a particular service or benefit only available if the individual consents to some, or all, of the collection?

1.2 Notice

√ **What do individuals know about the collection?**

✗ **Individuals are unaware of the collection or its purpose.**

Always handle personal information in a transparent way so that there are no surprises for the individual. Identify and describe information about the collection given to the individual and how it is given, including:

(a) **Purpose and authority**

- Why the personal information is being collected.
- Is the collection authorised or required by law, and, if so, which law?

(b) **Use and disclosure**

- Uses or disclosures that you consider consistent with the purpose for collection.
- The people or organisations to which you usually or sometimes disclose personal information (and any further uses and disclosures by those people or organisations).

- Proposed uses or disclosures for purposes other than the purpose of collection.

(c) **Choice**

- If choices exist about the way personal information is handled, do individuals know about these choices? Have you told them?

1.3 Method of collection

✗ **Covert collection is generally highly privacy invasive, and should only take place in prescribed circumstances.**

Identify and describe:

- How often the personal information is to be collected (only once or ongoing).
- Any potentially sensitive or intrusive methods of collection, including photographs, fingerprinting, iris scanning, drug testing and the collection of genetic information.
- any covert methods of collection (such as surveillance) and why they are necessary and appropriate. **Example:** Website cookies, and surveillance devices, including listening devices and cameras.
- Whether the technology is privacy enhancing or privacy invasive, and why.

2 Use

√ **No surprises! Use personal information in ways that the individual expects.**

Generally, 'use' means what happens to personal information in the hands of the organisation that collects it.

2.1 Use

Identify and describe:

- all the uses of the personal information, including those which may be expected but are uncommon
- how all these uses relate to the purpose of collection
- any changes to the purpose for use after the information is collected
- measures in place to prevent secondary purpose uses.

2.2 Secondary purposes

✗ Using personal information for unplanned secondary purposes.

If information may be used for a secondary purpose, identify and describe:

- whether consent is required for the secondary use
- if the use is directly related to the purpose of collection
- whether an individual can say no and still be involved in the project
- any consequences for the individual who says no
- how individuals will be involved in decisions if new, unplanned purposes for handling personal information occur in the life of the project.

2.3 Data linkage / matching

✗ Unnecessary or unplanned data linkage.

Aggregating or bringing together, personal information that has been collected for different purposes has privacy risks. **Example:** It may reveal personal information not previously available or not necessary for the purpose.

Identify and describe:

- Any intention or potential for personal information to be data-matched, linked or cross-referenced to other information held in different databases (by you or other agencies or organisations).[17]
- How data matching linkage or cross-referencing might be done.
- Any decisions affecting the individual that are to be made on the basis of data-matching, linking or cross-referencing.
- Safeguards that will be in place to limit inappropriate access, use and disclosure of this information.
- Audit trails and other oversighting mechanisms that will be in place.
- Protections in place to ensure data linkage accuracy and that individuals will not be adversely affected by incorrect data matching. **Example:** Have individuals been told about the data linkage?

3 Disclosure

√ **No surprises! Tell the individual about disclosures.**

✗ **Unexpected disclosures can lead to privacy complaints.**

Generally, 'disclosure' means releasing the personal information you have collected to another agency, body or organisation (this does not include the individual the information is about).

Identify and describe:

- To whom, how and why the personal information will be disclosed.
- Whether the disclosed information will be protected from privacy risks in the same way as information you hold. **Example:** Covered by the Privacy Act, or by a similar privacy law.
- If the information is to be published, or disclosed to a register, such as a public register.

[17] Also see the OPC's *Guidelines for the Use of Data-Matching in Commonwealth Administration* at www.privacy.gov.au/materials/types/download/8688/6527.

- Whether the individual has been told about the disclosure and what choices they have (including publishing or suppressing their information).
- Whether the disclosure is authorised or required by law and specify the relevant provisions.

4 Access and correction

√ **Getting access to personal information should be clear and straightforward.**

X **Inaccurate information can cause problems for everyone!**

Identify and describe:

- how an individual can access their personal information, including any costs to the individual
- how the individual can have the information about them corrected, or annotations made, if necessary.

5 Security

√ **Keep information secure.**

X **Unauthorised internal and external access and use.**

Assess the project against your agency's/organisation's IT, telecommunication and physical security measures. **Example:** Laptops, encryption, access to sites and systems (physical and online).

Describe:

- security measures that will protect the personal information from loss, unauthorised access, use, modification, disclosure or other misuse
- how data is transferred between sites
- how personal information will be protected if it will be managed by someone else

- who will have access
- who authorises access
- the systems that will prevent and detect misuse or inappropriate access
- what action will be taken if there is a security breach (such as informing individuals).

5.1 Retention and destruction

X Retaining personal information unnecessarily.

Identify and describe:

- when personal information will be de-identified or destroyed
- how this will be done securely
- whether an information retention policy and destruction schedule is in place
- how compliance with this policy and any relevant legislation about record destruction will be assessed.

6 Data quality

X Making decisions based on poor quality data.

Identify and describe:

- The consequences for individuals if the personal information is not accurate or up-to-date, including:
  - the kinds of decisions made using the information
  - the risks of inaccurate information
  - how information will be kept up-to-date.

- The processes that ensure only relevant, up-to-date and complete information is used or disclosed.
- How personal information updates will be given to others who have previously been given personal information about an individual.

7 Identity management

√ Don't verify identity unless necessary.

Organisations will need robust identity management processes in place to identify the individuals (whose personal information they are dealing with).[18]

Identify and describe:

- The extent to which the project can proceed using anonymous or de-identified information.
- Whether it is necessary to verify identity, and the degree of confidence needed. **Example:** Taking the value of the transaction into account.
- How identity will be verified.
- Whether a new identification number needs to be issued to individuals, and its purpose, including:
    - whether the number could be used for other purposes or adopted by other agencies or organisations
    - what protections could be put in place to prevent other use or adoption.
- Any expected uses and disclosures of this or other identification numbers (by any agency or organisation).
- Other information that may need to be verified, such as an individual's qualifications.

[18] See also "*Proof of ID Required? Getting Identity Management Right*" – www.privacy.gov.au/materials/types/download/8386/6339.

MODULE D – Privacy Impact Analysis

Privacy impact analysis investigates:

- how information flows affect individuals' choices in the way personal information about them is handled
- the degree of intrusiveness into individuals' lives
- compliance with privacy law
- how the project fits into community expectations.

Key questions

- Does the project comply with relevant privacy legislation (see ***Modules E & F***) and any other specific legislative obligations applying to personal information?
- Do individuals have to give up control of their information and how much?
- Will the project change the way individuals interact with the agency or organisation, such as:
    - more frequent identity checks or checks in different circumstances
    - costs
    - the impact on individuals or groups who do not have identity documents.
- Will decisions that have consequences for individuals be made on the way personal information is handled in the project (such as decisions about services or benefits):
    - Does the project deliver accurate and relevant information adequately informing these decisions?
- Is there a complaint-handling mechanism?
- How will you handle a privacy breach?
- Are there audit and oversight mechanisms (including emergency procedures) if the system fails?

- Does the project recognise function creep? **Example:** Is there an interest in using the personal information collected for the project for other purposes or might that occur in the future?

- How valuable is the information to unauthorised users? **Example:** Is it information that others would pay money for or try hard to gain access to?

- Is any intrusion (physical or property) or surveillance (covert or overt) fully justified and in proportion to the outcome?

    - Is it the only way of achieving the aims of the project?

    - Is it done in the least intrusive manner?

    - Is it subject to legislative or judicial authority?

    - What auditing and oversighting measures are in place?

- How consistent is the project with community values about privacy? **Example:** Does it involve new ways of identifying individuals, create significant databases or use genetic or biometric material or information?

- Is privacy factored into the analysis of cost-benefit and investment return?

MODULE E – Compliance Checklist for Agencies

This Checklist will help you work out if the way personal information is to be handled in your project complies with your obligations under the Privacy Act.

You can modify this module to suit your specific needs, linking the PIA and any agency-specific processes electronically or attaching a summary or copy.

Important information

Many terms used in the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) have specific meanings. Always refer to the Privacy Act's definition.

The IPPs regulate how Australian and ACT government agencies manage personal information, including its collection, record keeping, use and disclosure and storage and security. The IPPs also allow individuals to access personal information about them and have it corrected if it is wrong.

This section includes a plain English summary of the eleven IPPs and NPPs 7, 8, 9 and 10.

Always read the full text of the IPPs before answering the questions in this section. The Guidelines for IPPs 1-3, 4-7, 8-11 and NPPs 7-10 will also be helpful.

If you answer 'NO' to any of the questions below, your agency may not have authority to collect personal information under the Privacy Act. You may need to get more advice about compliance with that IPP from your Privacy Contact Officer, legal unit or appropriate external source.

The Checklist

This section is for Australian and ACT government agencies. The IPPs have been summarised. For the full text see s 14 of the Privacy Act.

IPP 1 – Manner and purpose of collection

IPP 1

The information must be necessary for the agency's work, and collected fairly and lawfully.

1 Is the information collected for a lawful purpose directly related to a function or activity of the collector?

Yes ❑ No ❑

If yes, specify the **purpose** of collection and the **function** or **activity** to which it is directly related. If the collection is **authorised** or **required** by, or under, a specific Act, regulation or determination, specify the authority's details.

Note: this information will also be relevant to **Question 3** under **IPP 2** below.

If no, what are the alternatives?

2 Will the information collected be **necessary for** or **directly related to** that purpose?

Yes ❑ No ❑

If yes, how?

If no, what are the alternatives?

3 Will the information be collected by **lawful** and **fair** means?

Yes ❑ No ❑

If yes, specify the means.

If no, what are the alternatives?

IPP 2 – Solicitation of personal information from individual concerned

IPP 2

An agency must take steps (usually through an IPP 2 notice) to tell individuals:

- why they are collecting personal information
- what laws give them authority to collect it
- who they usually disclose it to.

1 Is the collector soliciting the personal information from the individual concerned?

Yes ❑ No ❑

If yes, how is the information solicited?

If no, why it will not be collected from the individual concerned, including the authority for not doing so (if relevant).

- If information is **not solicited** from the individual concerned, you may not need to answer **questions 2–4**.

  But, you may find these questions useful as there may be privacy risks (such as inaccuracy) when personal information is not collected directly from the individual (see ***Module C, 1-Collection***).

2 Will **reasonable steps** be taken to tell the individual about the purpose of the collection?

Yes ❑ No ❑

If yes, what are they?

If no, why not?

3 If the collection is **authorised** or **required** by law, will the individual be advised?

Yes ❑ No ❑

If yes, which law and how.

If no, why not?

4 Will the individual be advised about the **usual disclosures**?

Yes ❑ No ❑

If yes, what are these disclosures and how will you advise the individual.

If no, why not?

IPP 3 – Solicitation of personal information generally

IPP 3

An agency must take reasonable steps to ensure the personal information it collects is:

- relevant
- up-to-date and complete
- not collected in an unreasonably intrusive way.

1 Will **reasonable steps** be taken to ensure that any solicited personal information collected is **relevant, up to date** and **complete**?

Yes ❑ No ❑

If yes, what steps?

If no, why not?

2 Will **reasonable steps** be taken to ensure that the information will be collected in a way that does not **unreasonably intrude** on the individual?

Yes ❑ No ❑

If yes, what steps?

If no, why not?

IPP 4 – Storage and security of personal information

IPP 4

Personal information must be stored securely to prevent its loss or misuse.

If you want to modify information technology (IT), you may also have to manage other agency-specific processes. Include a summary or copy of the process in the PIA record.

Note: The unit responsible for IT maintenance and security should complete any assessments about new or existing systems. The unit manager should sign off on the assessment.

a) Security safeguards[19]

1 Will there be **reasonable technical security** in place to protect against loss, unauthorised access, use, modification or disclosure, and against other misuse?

Yes ❑ No ❑

If yes, what security and how will it be information be protected.

If no, why not.

[19] The Office acknowledges the British Columbia Office of the Information and Privacy Commissioner's *Privacy Impact Assessment Template*.

2 Will there be **reasonable physical security** in place to protect against loss, unauthorised access, use, modification or disclosure and other misuse?

Yes ❑ No ❑

If yes, what security and how will it be done.

If no, why not.

3 Will there be security policies and procedures in place during the handling (routine or otherwise) of the information?

Yes ❑ No ❑

If yes, what are they and how will they protect information.

If no, why not.

4 Will controls and procedures be created for the authority to add, change or delete personal information?

Yes ❑ No ❑

If yes, what are they?

If no, why not.

5 Will system security include an **ongoing audit process** to track system use, including back-up materials?

Example: When and who accessed, and if personal information is collected will privacy protections be built in?

Yes ❑ No ❑

If yes, what is the process and how will it protect privacy**.**

If no, why not.

6 Will audit mechanisms identify inappropriate system access?

Yes ❑ No ❑

If yes, how and the consequences.

If no, why not.

b) Safeguarding information provided to external parties

An agency must take **reasonable steps** to prevent the unauthorised use or disclosure of information it gives external parties providing a service to the agency (such as private sector contractors, overseas agencies or organisations).

1 Will the contractual obligation the agency imposes on the external party comply with s 95B of the Privacy Act?[20]

Yes ❑ No ❑

If yes, what are the relevant provisions.

If no, why not.

2 Will the contract include requirements inconsistent with NPPs 7-10?

Yes ❑ No ❑

If yes, specify the proposed inconsistencies and the reasons.

[20] For more information go to Information Sheet 14 – "Privacy Obligations for Commonwealth Contracts", the Australian Government Solicitor's Legal Briefing No 63 – "Outsourcing: Agency Obligations under the Privacy Act" and IPP 11.3.

3 Will the agreement with a State/Territory government or agency/body or the arrangement with a foreign government, agency, body or organisation include:

- Explicit undertakings that the recipient will afford the same privacy restrictions and protections as the information receives in the hands of the Commonwealth agency. (This includes against different third party uses and disclosures.)

Note: Also consider IPP 11.3 obligations (see below) at this point.

Yes ❑ No ❑

If yes, specify the proposed undertakings, any Privacy Act protections excluded and how adherence will be monitored.

If no, why not.

IPP 5 – Information related to records kept by a record-keeper

A record-keeper must take reasonable steps to allow a person to find out:

- if the record-keeper has possession or control of personal information
- the nature of that information
- the purposes that information is used for
- the steps to take to get access to their record.

The record-keeper must maintain a record of the:

- nature of records kept
- purpose of each type of record
- classes of individual about whom records are kept
- period each type of record is kept
- persons that may have access to the records and when
- how an individual can access their records.

The record-keeper must make sure that:

- this information is made available for public inspection
- a copy of this record is given to the Privacy Commissioner in June each year.

1 Will the **record-keeper** be **authorised by law** to refuse to inform any person of the records in the record-keeper's possession or control?

Yes ❑ No ❑

If yes, which law and how will this be done.

2 Will processes be put in place to satisfy obligations at question 1 above?

Yes ❑ No ❑

If yes, specify how each criteria will be satisfied.

If no, why not.

IPP 6 – Access

IPP 6

Individuals can have **access to records**, unless the record-keeper is **required** or **authorised** to refuse access under any Commonwealth law.

(This IPP effectively grants access to information on the basis of the rights available under the *Freedom of Information Act 1982.)*

1 Will processes be put in place to provide access to records under the relevant Commonwealth law such as the *Freedom of Information Act 1982* or the *Archives Act 1901*?

Yes ❑ No ❑

If yes, what processes.

If no, why not.

IPP 7 – Alteration of records

IPP 7

A **record-keeper** must take **reasonable steps** to ensure that the record is accurate, relevant, up to date, complete and not misleading.

The **record-keeper** can, on request, attach a statement from the individual correcting, deleting or adding to the record.

1 Will **reasonable steps** be taken to make sure that records are accurate, relevant, current, complete and not misleading?

Yes ❑ No ❑

If yes, describe the steps.

If no, why not.

2 Will provision be made for attaching corrections?

Yes ❑ No ❑

If yes, how.

If no, why not.

IPP 8 – Record-keeper's obligation to check accuracy etc of personal information before use

IPP 8

Record-keepers must take **reasonable steps** to ensure information is accurate, current and complete before using it.

1 Will processes be put in place to ensure accuracy, currency and completeness before information is used?

Yes ❑ No ❑

If yes, what processes.

If no, why not.

IPP 9 – Personal information to be used only for relevant purposes

IPP 9

A **record-keeper** must only use information for a relevant purpose.

1 Will relevance be tested before use?

Yes ❑ No ❑

If yes, how will it be tested.

If no, why not.

IPP 10 – Limits on use of personal information

Generally:

- **Use** is what happens to the personal information inside the agency (it includes putting the information in a publication).
- **Disclosure** is releasing personal information from the record-keeper's control.
- **Consent** means express consent or implied consent[21].

IPP 10

A **record-keeper** can generally only use the information for another purpose in special circumstances, including with consent and for health and safety or law enforcement reasons.

1 Will the individual be asked to consent to the proposed use of personal information about them for other purpose(s)?

Yes ❑ No ❑

If yes, specify how will you get this consent and describe the other purpose(s).

If no, why not and describe the other purposes.

2 Will a record be kept of whether the consent was **express** or **implied**?

Yes ❑ No ❑

[21] IPP Guidelines 8-11 have more information about implied and express consent.

Note: This is not strictly an IPP requirement, but it is **good privacy practice.**

If no record will be kept, why not?

If you are going to rely on **implied consent**, specify why.

3 Will there be guidance/process in place to help the record-keeper determine what **necessary to prevent or lessen a serious and imminent threat to the life or health** means, before using this exemption?

Yes ❑ No ❑

If yes, what guidance/process.

If no, why not.

4 Will there be guidance/process to help the record-keeper determine whether a proposed other purpose is **required** or **authorised** by or under law, before invoking this exemption?

Yes ❑ No ❑

If yes, what guidance/process.

If no, why not.

5 Will there be guidance/processes in place to help the record-keeper determine what is **reasonably necessary** for enforcement of a **criminal law**, **pecuniary penalty** or **protection of the public revenue**, before invoking this exemption?

Yes ❑ No ❑

If yes, what guidance/process.

If no, how will the **reasonably necessary** test be satisfied and the relevant law(s) determined.

6 Will there be guidance/process in place to assist the record-keeper determine what **directly related purposes** are?

Yes ❑ No ❑

If yes, what guidance/process.

If no, how will the **directly related purpose** test be satisfied.

7 Will there be processes in place to allow the record-keeper to record that a use under IPP 10(d) has occurred?

Yes ❑ No ❑

If yes, what are the processes.

If no, why not.

IPP 11 – Disclosure

IPP 11

A record-keeper can generally only disclose information in special circumstances, such as with the individual's consent or for health and safety or law enforcement reasons.

1 Will processes be put in place to:

- make individuals aware of the usual disclosures
- help the record-keeper determine if the individual was **reasonably likely to have been aware** of the disclosures?

Note: Responses to the **IPP 2 questions** above will be relevant here.

Yes ❑ No ❑

If yes, what processes.

If no, why not.

2 Will the individual have consented to the disclosure(s)?

Yes ❑ No ❑

If yes, how is consent sought and describe the proposed disclosure(s).

If no, why will consent not be relied on and describe the proposed disclosure(s).

3 Will a record be kept of whether the consent was **express** or **implied**?

Yes ❑ No ❑

Note: This is not strictly an IPP requirement, **but** it is important.

If no record will be kept, why not?

If you are going to rely on **implied consent**, specify why.

4 Will there be guidance/process in place to help the record-keeper determine what **necessary to prevent or lessen a serious and imminent threat to the life or health** of a person means, before invoking this exemption?

Yes ❑ No ❑

If yes, what guidance/process.

If no, why not.

5 Will there be guidance/process in place to help the record-keeper determine whether a proposed disclosure is **required** or **authorised** by or under law?

Yes ❑ No ❑

If yes, what guidance/process.

If no, why not.

6 Will there be guidance/process in place to help the record-keeper determine what is **reasonably necessary** for enforcement of a **criminal law**, **pecuniary penalty** or **protection of the public revenue**?

Yes ❑ No ❑

If yes, what guidance/process will satisfy the "**reasonably necessary**" test, and determine the relevant law(s).

If no, how will the record-keeper will satisfy the test and determine the law(s).

7 Will there be processes in place to allow the disclosure under IPP 11(e) to be recorded?

Yes ❑ No ❑

If yes, what processes.

If no, why not.

8 Will there be processes in place to ensure that the person, body or agency the information has been disclosed to **will only use or disclose** the information for the **purposes it was disclosed**?

Note: Responses to some of the **IPP 4 questions** will be relevant here.

Yes ❑ No ❑

If yes, what processes and how will compliance be monitored.

If no, why not and how will this requirement be satisfied.

B) Commonwealth Contracts

Under the Privacy Act, agencies must ensure that a **contracted service provider** in a Commonwealth contract does not breach the IPPs (s 95B).

Contracted service providers must also comply with the **NPPs**, unless the contract states otherwise.

Four NPPs have no IPP **equivalents** (below). Agencies should:

- include these four NPP provisions when contracting services.
- ensure that any personal information collected under a Commonwealth contract is not used or disclosed for direct marketing unless the contract requires it (s 16F of the Privacy Act).

- **contracted service provider**, means:

  "...an organisation that is or was a party to the government contract and that is or was responsible for the provision of services to an agency or a State or Territory authority under the government contract; or a subcontractor for the government contract".

NPP 7 – Identifiers

NPP 7

An **organisation**, must not:

- adopt as its own **identifier** of an individual, an identifier assigned by an agency
- use or disclose an agency identifier unless necessary to fulfil an agency obligation, or for **law enforcement and similar purposes**.

- **identifier** means:

  "...a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the A New Tax System (Australian Business Number) Act 1999) is not an identifier."

- **organisation** means:

  (a) an individual; or

  (b) a body corporate; or

  (c) a partnership; or

  (d) any other unincorporated association; or

  (e) a trust;

  that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory."

1 Is the organisation a **prescribed organisation** for the purposes of NPP 7?

Yes ❑ No ❑

If yes, specify the prescribing instrument and its relevance to any disclosures**.**

If no, answer **questions 2 to 4** below.

2 Will the agency disclose any **assigned identifiers** to an organisation for any purpose?

Yes ❑ No ❑

If yes, specify the organisations and purposes.

If no, go to **NPP 8** below.

3 Will steps be taken to ensure that the organisation **does not adopt** a Commonwealth identifier as its own?

Yes ❑ No ❑

If yes, what steps will be taken and how will compliance be monitored.

If no, why will it be appropriate for the organisation to adopt the identifier and how will it comply with the Privacy Act.

4 Will steps be taken to ensure that the organisation does not use or disclose Commonwealth identifiers, beyond its obligations to the agency?

Yes ❑ No ❑

If yes, what steps will be taken and how will compliance be monitored.

If no, why not, why will it be necessary for the organisation to use or disclose Commonwealth identifiers and how will it will comply with the Privacy Act.

NPP 8 – Anonymity

NPP8

Where possible, organisations must allow individuals to do business without having to identify themselves.

1 Will individuals have the option of not identifying themselves for any specified transactions?

Yes ❑ No ❑

If yes, how.

If no, why will an anonymous option not be provided, and describe the transactions.

NPP 9 – Transborder data flows

NPP 9

An **organisation** in Australia or an external Territory may only transfer personal information to a foreign country if:

- the recipient is subject to a law, binding scheme or contract similar to the NPPs
- the individual **consents** to the transfer
- the transfer is **necessary for the performance of a contract** between the individual and the organisation, or for **necessary pre-contractual measures** taken in response to the individual's request
- the transfer is necessary for the conclusion or performance of a contract, in the interest of the individual, between the organisation and a third party
- **all** of the following apply:
  - the transfer benefits the individual
  - it is **impractical to obtain consent**
  - if it were practical, the individual would be likely to consent
- the organisation has taken **reasonable steps** to ensure that the information will not be held, used or disclosed by the recipient inconsistently with the NPPs.

1 Will personal information, managed under a contract with an organisation, be transferred to a foreign country?

Yes ❑ No ❑

If yes, specify:

- the **NPP 9** provisions that will be relied on for the transfer
- the contractual provisions
- the countries or third parties will be involved
- how compliance will be monitored.

You may need to get advice about compliance with this NPP if you have answered "**Yes**" to **question 1** but have not specified how NPP 9 requirements will be satisfied or which countries or third parties will be involved.

NPP 10 – Sensitive information

NPP 10

An **organisation** must not collect **sensitive information** about an individual unless:

- the individual has **consented**
- the collection is **required by law**
- the collection is **necessary to prevent or lessen a serious and imminent threat to the life or health of an individual**, where the individual is **physically or legally incapable of giving consent** or **cannot communicate consent**
- if the information is collected in the **course of the activities** of non-profit organisations[22], provided the conditions in NPP 10.1(d)(i) and (ii) are met
- the collection is **necessary for the establishment, exercise or defence of a legal or equitable claim**
- **NPP 10.2 to 10.4** conditions are satisfied.

[22] **non-profit organisation** means an organisation that has "...racial, ethnic, political, religious, philosophical, professional trade, or trade union aims."

1 Will sensitive information be collected under a Commonwealth contract?

Yes ❑ No ❑

If yes, specify the reason for collection and the protections to be put in the contract.

If no, go to the next section.

2 If sensitive information is collected, will its collection and management be outsourced?

Yes ❑ No ❑

If yes, which NPP 10 provisions will be relied on, how will the sensitive information be protected and how will compliance be monitored.

If no, go to the next section.

If you have answered "**Yes**" to **questions 1 or 2** above, you may need to get advice about compliance with this NPP.

IPP COMPLIANCE - CONCLUSIONS

Summarise conclusions about the project's overall compliance with the IPPs (and NPPs as necessary), including any necessary changes or refinements to the project. **Modules D and F** will be helpful.

_____ _____

(Proponent) (Privacy Contact Officer)

Date: _____ Date: _____

MODULE F – Compliance Checklist for Organisations

This Checklist is for private sector organisations,[23] including all private health service organisations.[24]

The Checklist will help organisations assess the way personal information will be handled in the project and whether this complies with the organisation's obligations under the Privacy Act.

Organisations can modify this module if necessary and link or attach it to a PIA along with any other relevant organisation-specific processes.

Important information

The National Privacy Principles (NPPs) regulate how organisations (including all private sector health organisation and some small businesses) must manage personal information, including collection, use and disclosure, quality and security, openness, access and correction, identifiers, anonymity, transborder data flows and sensitive information.

Many terms used in the NPPs have specific meanings and organisations should always refer to the Privacy Act's definition.

This module includes a plain English summary of the NPPs. Organisations should always read the full text of the NPPs (linked in each section below) before answering the questions in this module.

Organisations will find the following guidelines helpful:

- The Guidelines to the National Privacy Principles
- The Guidelines on Privacy in the Private Health Sector (for health-related organisations).

If you answer 'NO' to any of the questions in the module, your organisation may need to get more advice about compliance with that NPP from the organisation's privacy unit, legal unit or appropriate external source.

[23] See s 6C(1) of the Privacy Act.
[24] See s 6 of the Privacy Act.

The Checklist

NPP 1 – Collection

What personal information organisations can collect and other considerations including:

- lawful, fair and unintrusive collection
- what individuals should be told about the collection and when
- collecting information from third parties.

1 Is the information collected necessary for one or more of the organisation's functions or activities?

Yes ❑ No ❑

If yes, specify the **purpose** of collection and the **function** or **activity** to which it is directly related. If the collection is **authorised** or **required** by, or under, a specific Act, regulation or determination, specify the authority's details.

Note: this information will also be relevant to **Question 3** about **NPP 1.3** below.

If no, what are the alternatives?

2 Is the collection **lawful** and **fair** and not **unreasonably intrusive**?

Yes ❑ No ❑

If yes, specify how and why.

If no, what are the alternatives?

NPP 1.3: An organisation must take reasonable steps to tell individuals:

- the identity of the organisation and how to contact it
- that individuals can gain access to information about themselves
- why the information is collected
- who the organisation usually gives the information to
- why the organisation is collecting personal information
- any law that requires the collection
- who the information is usually disclosed to
- what will happen if the individual does not give them the information.

3 Will the individual be made aware of the collection and the information required under NPP 1.3?

Yes ❑ No ❑

If yes, specify the reasonable steps, when and the information that will be given.

If no, why not?

4 Will the personal information be collected from the individual concerned?

Yes ❑ No ❑

If yes, how will the information be collected?

If no, why not, including the authority for not doing so (if relevant).

NPP 1.5: Reasonable steps must be taken to ensure that the individual is aware of NPP 1.3 matters when information about them is collected from someone else (unless it would be a serious threat to the life or health of any person).

5 Will **reasonable steps** be taken to tell the individual about NPP 1.3 matters when information is collected from a third party?

Yes ❑ No ❑

If yes, what are they?

If no, why not?

6 If the collection is **authorised** or **required** by law, will the individual be advised?

Yes ❑ No ❑

If yes, which law and how?

If no, why not?

7 Will the individual be advised about the **usual disclosures**?

Yes ❑ No ❑

If yes, what are these disclosures, who are they made to and how will you advise the individual?

If no, why not?

8 Does the collection include **sensitive**[25] information?

Yes ❑ No ❑

If yes, you must also answer the questions at **NPP 10, sensitive information**.

[25] Section 6 of the Privacy Act.

If no, go to **NPP 2 (use and disclosure)** below.

NPP 2 – Use and disclosure

Organisations may generally only use or disclose personal information for the primary purpose of collection **unless special conditions apply**.

An organisation does not always need an individual's consent to use and disclose personal information (but conditions must be met).

There are special rules about the use and disclosure of health information (including genetic information) and direct marketing.

Note: Generally:

- **use** is what happens to the personal information inside the organisation (it includes putting the information in a publication)
- **disclosure** is releasing personal information from the organisation's control
- **consent** means express consent or implied consent.[26]
- This principle applies to information collected by an organisation from a related body corporate as if the primary purpose for collection is the same as the primary purpose of the original collection by the related body corporate.

1 Is the use or disclosure for a **secondary purpose**?

Yes ❑ No ❑

If yes, describe the secondary purpose.

If no, describe the primary purpose.

[26] NPP Guidelines have more information about implied and express consent (see Key Concepts).

2 Do **all** of the following apply to the **use or disclosure**?

(a) The secondary purpose is **related** to the primary purpose of collection.

(b) Any sensitive information is **directly related** to the primary purpose of collection.

(c) The individual **reasonably expects** the organisation to use or disclose the information for the **secondary purpose**.

Yes ❑ No ❑

If yes, go to the next question.

If no, specify any point that does not apply and why.

3 Will the organisation have the individual's **consent** to the secondary use?

Yes ❑ No ❑

If yes, specify the kind of consent (implied or express), how consent will be achieved and describe the other purpose(s). If you are going to rely on **implied consent**, specify why.

If no, why not and describe the other purposes.

Note: your answer at **Question 2** above may be useful here.

4 Will a record be kept of whether the consent was **express** or **implied**?

Yes ❑ No ❑

Note: This is not strictly an NPP requirement, but it is **good privacy practice.**

If no record will be kept, why not?

5 Is the information for the secondary purpose of **direct marketing**?

Yes ❑ No ❑

If yes, please answer **Questions 5–10** below.

If no, go to **Question 11**.

Note: this information is not sensitive information.

6 Will it be **impracticable** for the organisation to seek the **individual's consent** before that direct marketing use?

Yes ❑ No ❑

If yes, specify why.

If no, go to **Question 7**.

7 Will the individual be given the opportunity **to request** that direct marketing not be sent?

Yes ❑ No ❑

If yes, specify how this will be done.

If no, why not.

8 Will each direct marketing communication **include a prominent notice** telling the **individual that they may ask not to receive** further direct marketing?

Yes ❑ No ❑

If yes, specify.

If no, why not?

9 Does **each** direct marketing communication **include** the organisation's business address and telephone number and/or relevant electronic contact details?

Yes ❑ No ❑

If yes, specify.

If no, why not?

10 Will there be **guidance/processes** in place to help the organisation manage its direct marketing obligations?

Yes ❑ No ❑

If yes, what guidance/processes.

If no, why not?

11 Is the use or disclosure of health information **necessary** for research, the compilation or analysis of statistics or relevant to public health or safety?

Yes ❑ No ❑

If yes, specify.

If no, go to **Question 13**.

12 If you answered **yes** to **Question 11** do **all** of the following apply?

(a) It is impracticable to seek consent before the use or disclosure.

(b) The use or disclosure accords with section 95A guidelines.

(c) The organisation reasonably believes that the **recipient of the health information** will not disclose it or other personal information derived from it.

Yes ❑ No ❑

If yes, specify.

If no, why not?

13 Is the use or disclosure necessary to **lessen or prevent:**

(a) a **serious and imminent threat** to an individual's life health or safety?

(b) a **serious threat** to public health or safety?

Yes ❑ No ❑

If yes, specify.

If no, go to **Question 15**.

14 Is the information **genetic information** obtained when providing a health service to the individual?

Yes ❑ No ❑

If yes, specify.

If no, go to **Question 18**.

15 If you answered **yes to Question 14** do **all** of the following apply?

(a) The use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of a **genetic relative** of the individual that the genetic information relates to (the threat does not need to be imminent).

(b) The use or disclosure accords with the section 95AA guidelines.

(c) The **recipient** (of the disclosure) **is a genetic relative** of the individual.

Yes ❑ No ❑

If yes, specify.

If no, why not?

16 Will there be **guidance/processes** in place to help the organisation determine the permitted **uses or disclosures of genetic information**?

Yes ❑ No ❑

If yes, what guidance/process.

If no, why not?

17 Is the individual's **health information** to be disclosed to a **responsible person** because some physical or legal incapability prevents the individual from giving consent to the disclosure?

Yes ❑ No ❑

If yes, specify the reason and the responsible person/s.

If no, specify.

18 Will there be **guidance/processes** in place to help the organisation determine the type of disclosure referred to in **Question 17**?

Yes ❑ No ❑

If yes, what guidance/processes.

If no, why not.

19 Will there be **guidance/processes** in place to help the organisation determine use or disclosure as a necessary part of an **investigation** into suspected unlawful activity or **reporting concerns**?

Yes ❑ No ❑

If yes, what guidance/process.

If no, why not.

20 Is the use or disclosure **required or authorised** by law?

Yes ❑ No ❑

If yes, specify.

If no, specify the alternative (other provisions may apply).

21 If **yes**, will there be **guidance/processes** in place to help the organisation determine whether a use or disclosure is **required** or **authorised** by or under law, before invoking an NPP 2.1(g) exemption?

Yes ❑ No ❑

If yes, what **guidance/processes**.

If no, why not.

22 Will there be **guidance/processes** in place to help the organisation determine whether a use or disclosure is **reasonably necessary for one or more of the functions listed in NPP 2.1(h) by or on behalf of an enforcement body**?

Yes ❑ No ❑

If yes, what **guidance/processes**. **Note:** the organisation is required to make a written note of the use or disclosure.

If no, why not?

23 Will there be **guidance/processes** in place to help the organisation determine whether it can disclose personal information to a person responsible for another person (see NPP 2.4 – 2.6)?

Yes ❑ No ❑

If yes, what **guidance/processes**.

If no, why not?

NPP 3 – Data quality and NPP 4 – Data security

An organisation must take steps to ensure the personal information it holds is accurate, complete and up-to-date, and is kept secure from unauthorised use or access.

Note: If you want to modify your organisation's information technology (IT), you may also have to manage other organisation-specific processes. Include a summary or copy of any process in the PIA.

The unit responsible for the organisation's IT maintenance and security should complete any assessments about new or existing systems. The unit manager should sign off on the assessment.

1 Will **reasonable steps** be taken to make sure that personal information collected, used or disclosed is **accurate, complete and up-to-date**?

Yes ❑ No ❑

If yes, what steps?

If no, why not?

2 Will there be quality **guidance/processes** in place?

Yes ❑ No ❑

If yes, what **guidance/processes**?

If no, why not?

3 Will there be **reasonable technical security** in place to protect against loss, unauthorised access, use, modification or disclosure and other misuse?

Yes ❑ No ❑

If yes, what security and how will information be protected?

If no, why not?

4 Will there be **reasonable physical security** in place to protect against loss, unauthorised access, use, modification or disclosure, and against other misuse?

Yes ❑ No ❑

If yes, what security and how will it the information be protected.

If no, why not.

5 Will there be **physical and technical security guidance/processes** in place?

Yes ❑ No ❑

If yes, what are they?

If no, why not?

6 Will there be **authorisation controls and procedures** in place (for addition, change or deletion of personal information)?

Yes ❑ No ❑

If yes, what are they?

If no, why not.

7 Will there be an **ongoing audit process** to track system use, including back-up materials? **Example:** When and who and what collection protections will be built in?

Yes ❑ No ❑

If yes, what process and how will it protect information privacy**.**

If no, why not.

8 Will **audit mechanisms** identify inappropriate system access?

Yes ❑ No ❑

If yes, how and the consequences.

If no, why not.

9 Will reasonable steps be taken to destroy or de-identify personal information no longer needed for any use or disclosure under NPP 2?

Yes ❑ No ❑

If yes, what steps.

If no, why not.

10 Will there **guidance/processes** in place to help determine when and how destruction or de-identification of personal information will take occur?

Yes ❑ No ❑

If yes, what guidance/processes?

If no, why not?

NPP 5 – Openness

An organisation must have a policy on how it manages personal information and make it available to anyone who asks for it.

1 Will the organisation have a clearly expressed, documented policy available to anyone who asks for it?

Yes ❑ No ❑

If yes, specify the policy and how it will be made available on request.

If no, why not.

2 Will reasonable steps be taken to let a person know generally, what sort of personal information the organisation holds, for what purposes and how it collects, holds, uses and discloses that information?

Yes ❑ No ❑

If yes, what steps and how the information will be made available.

If not, why not.

3 If **yes**, will there be **guidance/processes** in place to help the organisation determine how, when and what information will be made available?

Yes ❑ No ❑

If yes, what **guidance/processes**.

If no, why not?

NPP 6 – Access and correction

Individuals have a general right:

- to access their personal information
- to have the information corrected if it is inaccurate, incomplete or out-of-date.

1 Will **guidance/processes** be put in place to generally provide the individual with access to information the organisation holds about them?

Yes ❑ No ❑

If yes, specify the guidance/processes, including how the individual will be made aware of how to get access.

If no, why not.

2 Will **reasonable steps** be taken to correct information that is not accurate, complete and up-to-date?

Yes ❑ No ❑

If yes, what steps.

If no, why not.

3 Will there be **guidance/processes** in place to help the organisation determine when it may be necessary to invoke an NPP 6.1 or NPP 6.2 exemption?

Yes ❑ No ❑

If yes, what guidance/processes.

If no, why not.

4 Will **guidance/processes** be put in place to help the organisation consider (if reasonable) the **use of an intermediary**?

Yes ❑ No ❑

If yes, what guidance/processes**.**

If no, why not.

5 Will **guidance/processes** be put in place to help the organisation determine any **charges for access**[27]?

Yes ❑ No ❑

If yes, what guidance/processes (including the circumstances when an organisation may decide not to charge for access)**.**

If no, why not.

[27] Note that a charge must not apply just for lodging a request for access (NPP 6.4(b)).

6 Will **reasonable steps** be taken to attach a statement if the **individual and organisation disagree** about the accuracy of the information the organisation holds?

Yes ❑ No ❑

If yes, what steps.

If no, why not.

7 Will **guidance/processes** be put in place to ensure accuracy, currency and completeness before information is used?

Yes ❑ No ❑

If yes, what processes.

If no, why not.

8 Will **guidance/processes** be put in place to help tell the individual about why access or correction is to be denied?

Yes ❑ No ❑

If yes, what guidance/processes.

If no, why not.

NPP 7 – Identifiers

An **organisation**, must not:

- adopt as its own, an **identifier**[28] assigned by an agency to an individual
- use or disclose an agency identifier, unless necessary to fulfil an agency obligation, or for **law enforcement and similar purposes**.

1 Is the organisation a **prescribed organisation** for NPP 7 purposes?

Yes ❑ No ❑

If yes, specify the prescribing instrument and its relevance to any disclosures**.**

If no, answer **questions 2 to 4** below.

2 Will an agency disclose any **assigned identifiers** to the organisation for any purpose?

Yes ❑ No ❑

If yes, specify the agency and purposes.

If no, go to **NPP 8** below.

3 Will steps be taken to ensure that the organisation **does not adopt** a Commonwealth identifier as its own?

Yes ❑ No ❑

If yes, what steps will be taken and how will compliance be monitored.

If no, why will it be appropriate for the organisation to adopt the identifier and how will it comply with the Privacy Act.

4 Will steps be taken to ensure that the organisation does not use or disclose Commonwealth identifiers, beyond its obligations to the agency?

Yes ❑ No ❑

---

[28] Under NPP 7.3, an **identifier** includes:
"...a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999*) is not an identifier."

If yes, what steps will be taken and how will compliance be monitored.

If no, why not, why will it be necessary for the organisation to use or disclose Commonwealth identifiers and how will it will comply with the Privacy Act.

5 Will **guidance/processes** be put in place to help determine how Commonwealth identifiers should be handled?

Yes ❑ No ❑

If yes, what guidance/processes**.**

If no, why not.

NPP 8 – Anonymity

Where possible, organisations must allow individuals to do business without having to identify themselves.

1 Will individuals have the option of not identifying themselves for any specified transactions?

Yes ❑ No ❑

If yes, how and describe the transactions.

If no, why not and describe the transactions.

NPP 9 – Transborder data flows

An **organisation** in Australia or an external Territory may only transfer personal information to a foreign country if:

- the recipient is subject to a law, binding scheme or contract similar to the NPPs
- the individual **consents** to the transfer
- the transfer is **necessary for the performance of a contract** between the individual and the organisation, or for **necessary pre-contractual measures** taken in response to the individual's request
- the transfer is necessary for the conclusion or performance of a contract, in the interest of the individual, between the organisation and a third party
- **all** of the following apply:
    - the transfer benefits the individual
    - it is **impractical to obtain consent**
    - if it were practical, the individual would be likely to consent

the organisation has taken **reasonable steps** to ensure that the information will not be held, used or disclosed by the recipient inconsistently with the NPPs.

1 Will personal information be transferred to a foreign country?

Yes ❑ No ❑

If yes, specify:

- the **NPP 9** provisions that will be relied on for the transfer
- any contractual provisions
- the countries or third parties that will be involved
- how compliance will be monitored.

NPP 10 – Sensitive information

An **organisation** must not collect **sensitive information** about an individual unless:

- the individual has **consented**
- the collection is **required by law**
- the collection is **necessary to prevent or lessen a serious and imminent threat to the life or health of an individual**, where the individual is **physically or legally incapable of giving consent** or **cannot communicate consent**
- if the information is collected in the **course of the activities** of organisations[29], provided the conditions in NPP 10.1(d)(i) and (ii) are met
- the collection is **necessary for the establishment, exercise or defence of a legal or equitable claim**
- **NPP 10.2 to 10.4** conditions are satisfied.

1 Will sensitive information be collected in this project?

Yes ❑ No ❑

If yes, specify the information, the reason for collection, the NPP 10 provision the organisation is relying on and why.

If no, go to **Module G.**

[29] **non-profit organisation** means an organisation that has "...racial, ethnic, political, religious, philosophical, professional trade, or trade union aims."

2 Will the collection and management of sensitive information be outsourced?

Yes ❑ No ❑

If yes, which NPP 10 provisions will be relied on, how will the sensitive information be protected and how will compliance be monitored.

If no, go to **Module G.**

If you answered "**Yes**" to **question 2**, you may need to get advice.

3 Will there be **guidance/processes** in place to help the organisation determine the handling of sensitive information?

Yes ❑ No ❑

If yes, what guidance/processes.

If no, why not.

Contractual obligations

1 Has the organisation entered into any **contractual obligations** with an Australian Government, State or Territory agency, other organisation or foreign government, agency or body?

Yes ❑ No ❑

If yes, specify the entity and the obligations.

If no, go to **Module G.**

2 Does the contract include requirements inconsistent with NPPs 7-10?

Yes ❑ No ❑

If yes, specify the proposed inconsistencies and the reasons.

If no, go to Question 3.

3 Will the agreement with a State/Territory government or agency/body or the arrangement with a foreign government, agency, body or organisation include:

- explicit undertakings that the recipient will afford the same privacy restrictions and protections as the information receives under the NPPs.

Yes ❑ No ❑

If yes, specify the proposed undertakings, any Privacy Act protections excluded and how adherence will be monitored.

If no, why not.

NPP Compliance – Conclusions

Summarise conclusions about the project's overall compliance with the NPPs, including any necessary changes or refinements to the project. **Modules D and G** will be helpful.

_____ _____

(Proponent) (Privacy Contact Officer)

Date: _____ Date: _____

MODULE G – Privacy Management

Here are some actions that agencies and organisations can take when dealing with negative privacy impacts identified in the PIA.

- **Balancing interests:** Put yourself in the individual's shoes. How would an ordinary individual react when their personal information is affected by the project? There should be an appropriate balance between the goals of the project and the interests of the organisation and affected individuals.

- **Minimum standards:** Ensure a minimum standard of privacy protection for individuals (the principles may not apply in all circumstances or situations).

  Note:

  - the transfer of personal information across public or private sectors or jurisdictions

  - whether privacy protection and regulatory oversight is adequate.

- **Proportionality:** The privacy infringement should be in proportion to, or balanced with any benefits. Will the benefits be achieved?

- **Transparency and accountability:** Privacy measures should always be transparent to individuals (through adequate notice and privacy policies). Organisations are accountable for how they manage personal information, including effective complaint-handling, audits and oversighting.

- **Flexibility:** Take into account the diversity of individuals affected by the project. **For example:** Do some have heightened sensitivities to particular personal information that others do not?

- **Deliverable promises:** Privacy protections should be included in law or other binding obligations, and built into new technology.

- **Privacy Enhancing Technology:** Consider available privacy enhancing technologies and the impact of privacy invasive technologies.

- **Review after implementation:** Did the project meet its primary objectives? How will the project's privacy impacts be assessed?

Example: Internal audit; implementation assessment, Australian National Audit Office, or OPC audit or Parliamentary committee scrutiny?

APPENDIX A

Acknowledgements and Resources

Acknowledgements

In preparing this guide in 2006 and its revision in 2010, the Office acknowledges the work on privacy impact assessment and building privacy in by design that has been and is continuing to be undertaken by a number of others around the world, particularly the work of privacy and information commissioners in New Zealand, Canada, the United Kingdom and the work of Professor David Flaherty.

PIA Resources

Canada

The Treasury Board of Canada Secretariat's PIA e-learning tool includes some useful suggestions for elements that might form part of a PIA Report.

New Zealand

Office of the Privacy Commissioner (New Zealand), *Privacy Impact Assessment Handbook*.

Online resources collated by the New Zealand Privacy Commissioner's Office.

United Kingdom

The ICO launched its Privacy Impact Assessment (PIA) handbook (Version 2) in June 2009.

United States of America

The Privacy Office of the Department of Homeland Security has released official guidance for use in drafting PIAs.

Victoria (Australia)

Office of the Victorian Privacy Commissioner – Privacy Impact Assessments – a guide.

PIA Reports

A small sample of PIA reports or summaries published by some national and international government agencies and organisations follows.

The Office does not specifically endorse any of these resources or encourage a particular format for PIA reports. This information simply gives organisations some idea about different PIA approaches.

Australia

- Department of Health and Ageing - Privacy Impact Assessment for the IMCA Initiative (2009)
- NEHTA Healthcare Identifier Service PIA recommendations
- Australian Bureau of Statistics – PIA for a Proposal for Enhancing the Population Census (2005)
- Attorney-General's Department PIAs for Auscheck initiative
- AGIMO Gatekeeper - PIA (2006).

Canada

- Alberta Screening Directive updated report (2009)
- Summary of Foreign Affairs Canada's PIA for the Facial Recognition Project (2006)
- Canadian Institute of Health Information NHEX report (2002)
- Veterans Affairs Canada PIA index.

New Zealand

- Privacy impact assessment for the Linked Employer-Employee Data (LEED)-Ministry of Social Development (MSD) Data Integration Project (2008)
- Privacy impact assessments on the National Student Index number (NSI) and National Student Number (NSN).

United Kingdom

- Phorm Inc PIA report regarding behavioural targeted advertising (2008) - private sector
- The Office for National Statistics PIA report on the 2011 Census.

United States of America

The Privacy Office of the Department of Homeland Security gives examples of official PIA Reports of significant initiatives within its Department.