Australian Government

Office of the Australian Information Commissioner

Guide to undertaking privacy impact assessments

May 2020

OAIC

Contents

Introduction to privacy impact assessments

About this Guide

The *Guide to undertaking privacy impact assessments* (PIA Guide) has been prepared by the Office of the Australian Information Commissioner (OAIC) to describe a process for undertaking a privacy impact assessment (PIA). The PIA Guide is intended to provide guidance to all Australian Privacy Principle (APP) entities.[1]

APP 1 requires APP entities to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs and enable them to deal with enquiries or complaints about privacy compliance. In this way, the APPs require 'privacy by design', an approach whereby privacy compliance is designed into projects dealing with personal information right from the start, rather than being bolted on afterwards. Conducting PIAs helps entities to ensure privacy compliance and identify better practice.

The PIA Guide sets out a suggested ten step process for undertaking a PIA (see 'Undertaking a PIA', below). It can be used alongside existing project management and risk management methodologies or as a process in its own right. When considering the PIA process both government agencies and private sector organisations could consider whether the process set out in this Guide could be adapted to suit specific business needs or functions of the entity. While different entities might use different processes when they undertake PIAs, ideally these processes will address each of these steps in some way.

This Guide refers to PIAs being undertaken for 'projects'. This term is used loosely and is intended to cover the full range of activities and initiatives that may have privacy implications, including:

- policy proposals
- new or amended legislation
- new or amended programs, activities, systems or databases
- new methods or procedures for service delivery or information handling
- changes to how information is stored.

What is a privacy impact assessment?

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

[1] 'APP entities' include private sector organisations and Australian government agencies. Refer to the Glossary for full definitions of 'agency' and 'organisation' under the *Privacy Act 1988*.

PIAs are an important component in the protection of privacy, and should be part of the overall risk management and planning processes of APP entities.

Undertaking a PIA can assist entities to:

- describe how personal information flows in a project
- analyse the possible impacts on individuals' privacy
- identify and recommend options for avoiding, minimising or mitigating negative privacy impacts
- build privacy considerations into the design of a project
- achieve the project's goals while minimising the negative and enhancing the positive privacy impacts.

While PIAs assess a project's risk of non-compliance with privacy legislation and identify controls to mitigate the risk, a PIA is much more than a simple compliance check. It should 'tell the full story' of a project from a privacy perspective, going beyond compliance to also consider the broader privacy implications and risks, including whether the planned uses of personal information in the project will be acceptable to the community.

Why do a PIA?

A large part of a project's success will depend on whether it meets legislative privacy requirements and community privacy expectations. Privacy issues that are not properly addressed can impact on the community's trust in an entity and undermine the project's success. It is in your entity's interest to consider undertaking a PIA for any projects that handle personal information.

Risks of not undertaking a PIA include:

- non-compliance with the letter or the spirit of relevant privacy laws, potentially leading to a privacy breach and/or negative publicity
- loss of credibility by the entity through lack of transparency in response to public concern about handling personal information
- damage to an entity's reputation if the project fails to meet expectations about how personal information will be protected
- identification of privacy risks at a late stage in the project development or implementation, resulting in unnecessary costs or inadequate solutions.

Potential benefits of undertaking a PIA include:

- ensuring that the project is compliant with privacy laws
- reflecting community values around privacy and personal information in the project design
- reducing future costs in management time, legal expenses and potential negative publicity, by considering privacy issues early in a project

- identifying strategies to achieve the project's goals without impacting on privacy
- demonstrating to stakeholders that the project has been designed with privacy in mind
- promoting awareness and understanding of privacy issues inside the organisation or agency
- contributing to broader organisational or agency risk management processes
- building community awareness and acceptance of the project through public consultation.

A PIA may also assist an entity to demonstrate its compliance with its privacy obligations and its approach to managing privacy risk in the case of a future complaint, privacy assessment or investigation relating to the privacy aspects of a project. APP 1.2 requires APP entities to take reasonable steps to implement practices, procedures or systems that will ensure that the entity complies with the APPs. A PIA can assist in identifying the practices, procedures or systems that will be reasonable to ensure that new projects are compliant with the APPs.

Is a PIA necessary?

For any project that will involve the handling of personal information, you should consider undertaking a threshold assessment (discussed below under 'Undertaking a PIA') to determine whether it will be necessary to undertake the rest of the steps involved in a PIA. Under the *Privacy Act 1988* (Privacy Act), information does not always have to include details such as an individual's name to qualify as personal information. It may include other information that can identify an individual or allow their identity to be determined.[2] Personal information may be collected directly from an individual or indirectly from another source.[3]

It will also be necessary for agencies to undertake a PIA if directed to do so by the OAIC. Under the Privacy Act, the OAIC can direct an agency to provide a PIA about an activity or function involving the handling of individuals' personal information. Further information is below under 'Role of the OAIC'.

The OAIC strongly encourages entities to conduct PIAs as a matter of course for projects that involve personal information. Undertaking a threshold assessment — the first step in the PIA process, outlined below — can assist entities to determine whether a PIA is necessary for a project, and should be routinely conducted for every project. The greater the project's complexity and privacy scope, the more likely it is that a comprehensive PIA will be required, to determine and manage its privacy impacts.

When to do a PIA

To be effective, a PIA should be an integral part of the project planning process, not an afterthought. It should be undertaken early enough in the development of a project that it is still possible to influence the project design or, if there are significant negative privacy impacts, reconsider proceeding with the

[2] See the Glossary for a full definition of 'personal information'. A more detailed explanation of 'personal information' is in the APP Guidelines — see Chapter B, Key Concepts.

[3] This Guide discusses privacy of personal information, but a PIA may also consider other types of personal privacy, such as bodily, behavioural and communications privacy.

project. A PIA works most effectively when it evolves with and helps to shape the project's development, ensuring that privacy is considered throughout the planning process.

Making a PIA an integral part of a project from the beginning means that you can identify any privacy risks early in the project and consider alternative, less privacy-intrusive practices during development, instead of retrospectively. Also, consistent and early use of a PIA ensures that all relevant staff consider privacy issues from the early stages of a project.

Undertaking a PIA should be seen as a process that does not end with the publication of the PIA report. A PIA may be useful more than once during the project's development and implementation. It should be revisited and updated when changes to the project are considered. If there are substantial changes to how personal information will be handled or changes to an existing project, it may be necessary to undertake another PIA.

Entities should consider whether their existing project management and risk assessment processes incorporate a PIA and if any improvements should be made to these processes. A report prepared for the UK Information Commissioner's Office (ICO), *Privacy impact assessment and risk management*, identifies stages in several commonly used project and risk management processes where a PIA could be introduced, which may assist entities to identify how PIAs can be integrated into their 'business as usual' practices.

The core principles of a PIA can be applied to any project or activity which impacts on the privacy of individuals. Entities, in particular those that conduct regular PIAs, may find it useful to develop their own PIA process, with accompanying guidance, which suits their own business needs and functions. Consistent use of a PIA process will mitigate privacy risks and increase awareness of privacy and data protection issues within the entity.

Role of the OAIC

Agencies

The Privacy Act gives the Information Commissioner a power (that is exercisable by the Privacy Commissioner) to direct an agency to provide a PIA to the OAIC, if the Commissioner considers that a proposed activity or function of the agency might have a significant impact on the privacy of individuals.[4] This includes when the agency proposes to:

- engage in a new activity or function, or
- substantively change an existing activity or function. This includes a substantive change to the system that delivers an existing function or activity.

There are two main circumstances in which consideration is likely to be given to exercising this power:

- when the OAIC, in the course of providing policy advice to an agency on a proposed agency activity or function, considers that the activity or function might have a significant impact on the

[4] See s 33D of the Privacy Act.

privacy of individuals and recommends a PIA be conducted and the agency does not conduct one

- when the OAIC otherwise becomes aware of an agency's proposed activity or function (for example, through a media report) and considers that it might have a significant impact on the privacy of individuals and the agency has not conducted a PIA.

Agencies who are directed to give the OAIC a PIA are required to prepare a written assessment that:

- identifies the impact that the activity or function might have on the privacy of individuals; and
- sets out recommendations for managing, minimising or eliminating that impact.

Further information on when and how the OAIC might exercise the power to direct agencies to provide a PIA is available in the OAIC's *Privacy regulatory action policy* and *Guide to the OAIC's privacy regulatory action*.

However, the OAIC expects agencies would recognise the benefits of conducting a PIA and that a PIA direction would not generally be required. While the OAIC has no formal role in the development, endorsement or approval of PIAs that have not been directed by the OAIC, it may, subject to available resources, be able to assist agencies with advice during the PIA process.

Organisations

The OAIC does not have a role in the development, review, endorsement or approval of the PIA process for private sector organisations. The OAIC's power to direct agencies to undertake a PIA does not apply to private sector organisations.[5] However, as outlined above, there are many potential benefits that organisations may experience by conducting a PIA. Undertaking a PIA provides an opportunity for organisations to demonstrate a commitment to good privacy practice, as well as compliance with privacy legislation. The OAIC encourages organisations to undertake PIAs for projects that involve handling of personal information, and share their findings publicly.

[5] Section 33D (7) of the Privacy Act requires that a review will be undertaken within five years of the commencement of the reforms to the Privacy Act to consider whether the power to direct a PIA should also apply in relation to organisations.

Undertaking a PIA

This section sets out 10 steps for undertaking a PIA, and guidance on completing each step:

1. Threshold assessment
2. Plan the PIA
3. Describe the project
4. Identify and consult with stakeholders
5. Map information flows
6. Privacy impact analysis and compliance check
7. Privacy management — addressing risks
8. Recommendations
9. Report
10. Respond and review.

Different entities might have their own processes for undertaking PIAs, or choose to use a different methodology. The PIA process is a flexible one, and it can be integrated with an entity's existing approach to managing projects. The PIA Guide identifies 10 key elements of PIAs which the OAIC suggests should be included in any process.

If the OAIC directs an agency to undertake a PIA (see 'Role of the OAIC', above), the agency would be expected to address each of these elements when completing the PIA for the OAIC to consider it has adequately complied with the OAIC's direction. As noted above, the OAIC does not have the power to direct a private sector organisation to conduct a PIA in the same way.

1. Threshold assessment

The first step in undertaking a PIA is assessing whether a PIA is necessary for the project. Not every project will need a PIA.

If an entity bound by the Privacy Act is developing a project that involves personal information, it must comply with that Act. Your entity 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.

A threshold assessment helps you work out, early in the project, whether a PIA is necessary. There is no hard-and-fast rule about whether a PIA will be necessary, and each project must be considered individually. This assessment allows projects with no or minimal information privacy implications to be identified relatively easily and quickly.

The first question to ask when assessing whether a PIA is needed is, 'Will any personal information be collected, stored, used or disclosed in the project?'

Generally, if personal information is involved in the project, some form of PIA may be necessary. Depending on how personal information is handled in the project, the PIA process might be quite brief; see 'Plan the PIA' for more information on different approaches to PIAs for projects with minimal or low-risk handling of personal information. 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. A PIA may not be necessary if the project does not propose any changes to existing information handling practices, if the privacy implications of these practices have been assessed previously and controls are current and working well.

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. For example, if a project uses de-identified information, a PIA could explain how and why this information will be used and how the entity conducting the project will prevent the future re-identification of the information. You might also find it useful to undertake a PIA to show how the project will deal with other kinds of personal privacy not covered by the Privacy Act, such as bodily, behavioural and communications privacy.

Regardless of whether you proceed to a PIA, you should keep a record of the threshold assessment. This could include the following information:

1. Brief description of the project
2. Consideration of whether the project involves the collection, storage, use or disclosure of personal information:
    - brief description of the personal information (if any) that will be collected, used or disclosed (such as name, address, date of birth, health information and so on)
    - the key privacy elements — for example:
        - the general purposes for which information will be collected, used and disclosed
        - any authority under which personal information is collected
        - the nature and sensitivity of the personal information.
    - if the project is going to modify an existing program, a description of the changes, if any, to the way personal information will be handled
    - the views of any stakeholders about the impact of the project on information privacy
    - if the project does not involve any changes to personal information handling practices, a description of how privacy risks involved in these practices have been assessed and are being managed.
3. Whether, based on the threshold assessment, you will proceed to undertake a PIA
4. Details of the person or team responsible for completing the threshold assessment.

2. Plan the PIA

Planning the PIA is an important stage of the PIA process. Planning should consider a range of elements, including:

- how detailed the PIA needs to be, based on a broad assessment of the project and its privacy scope
- who will conduct the PIA
- the timeframe for the PIA
- the budget and other resources available for the PIA
- the extent and timing of stakeholder and public consultations
- steps that will need to be taken after the PIA, including implementation of recommendations and ongoing monitoring.

Some of these elements are self-explanatory, while others are discussed in more detail below.

The planning process should take into account that the PIA is a process which will need to continue beyond the development of recommendations and the preparation of the PIA report to include implementation and monitoring. Further information is below under 'Respond and review'.

Assessing the project's scope

The project's nature and stage of development will have an impact on how detailed the PIA process needs to be. A project may be at a conceptual or a more advanced stage of development, be an 'incremental' program (altering a well-established existing program) or a significant new one, and have a limited or broad scope.

The size or budget for a project is not a useful indicator of its likely privacy impact, and even a small-scale project may have significant privacy implications. When assessing the project's privacy scope, you will need to look at its key attributes, including:

- the quantity of personal information handled
- whether sensitive information[6] is involved
- the size or complexity of the project
- whether the project will involve cross-organisation/agency or cross-sector information sharing
- the likely community and/or media interest in the privacy aspects of the project.

A project's privacy scope can increase depending on the risk of privacy impacts, for example, in circumstances where:

- personal information handling will be or has been outsourced
- new legislation or new technology will be needed for handling or storing the personal information

[6] 'Sensitive information' is defined in the Glossary and is explained in more detail in the APP Guidelines — see Chapter B, Key Concepts.

- personal information will be aggregated in databases
- the personal information will be used for data-matching
- entirely new collections of personal information are planned
- a new method of using or disclosing personal information is planned
- provision of personal information will be compulsory
- the handling of personal information will have an impact on key aspects of an individual's life (such as livelihood, housing, reputation, health), or individuals may experience adverse outcomes (such as fines, reduction or cancellation of entitlements) as a result of the collection or use of their personal information.

Generally, the greater the privacy scope of the project, the more likely it will be that the PIA will need to be more detailed, to better determine and manage the project's privacy impacts.

Examples of PIA processes for different types of projects

There is no single way of doing a PIA or setting out a PIA report and entities are encouraged to take a flexible approach. The structure and length of a PIA report will be proportionate to the nature of the project and the nature of the organisation carrying out the project. Reports should be easy to follow and thorough without being needlessly repetitive or jargonistic. Steps set out separately in this Guide may be combined or re-ordered in a report if this assists with readability and reduces the need to re-explain or repeat material. For example, an explanation of personal information flows and privacy risks could be presented alongside proposed mitigation strategies.

Some examples of how detailed the PIA process might be for different types of projects are below. These examples are not exhaustive.

Example A: Incremental projects of limited scope

If a project is incremental and relatively limited in privacy scope, only a short PIA may be needed (for 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 that is not sensitive).

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 that 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.

For example, information flows can only be mapped based on 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, preparing preliminary reports and interim recommendations will provide early visibility of privacy risks and assist in ensuring privacy is considered and addressed in the design of the project.

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, it is best practice to undertake a preliminary PIA early in the concept/design stage to mitigate any potential privacy impacts before they become entrenched in the planning process.

Identifying who will conduct the PIA

Generally, whoever is managing the project would be responsible for ensuring the PIA is carried out. The nature and size of the project will influence the size of the team needed to conduct the PIA, and how much the team needs to draw on external specialist knowledge.

A PIA is unlikely to be effective if it is done by a staff member working in isolation. There could be a team approach to conducting a PIA, making use of the various 'in-house' experts available, such as the privacy officer or equivalent, and outside expertise as necessary. A range of expertise may be required, including information security, technology, risk management, law, ethics, operational procedures and industry-specific knowledge. Seeking external input from experts not involved in the project can help to identify privacy impacts not previously recognised.

Some projects will have substantially 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.[7]

The team conducting the PIA needs to be familiar with the Privacy Act, any other legislation or regulations that might apply to personal information handling (for example, state or territory legislation), and the broader dimensions of privacy.

Consultation

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 attitudes to and expectations of privacy. Affected individuals are likely to be key stakeholders, so public consultation is important, particularly where a substantial amount of personal information is being handled or where sensitive information is

[7] A number of privacy consultancies and law firms offer PIAs as a service.

involved. Public consultation also adds to community awareness about the project and can increase confidence in the way the project (and the entity) is handling personal information.

The extent and timing of the consultation will vary depending on the stage of the project. Consultation is discussed further below under 'Identify and consult with stakeholders'.

3. Describe the project

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

- the project's overall aims
- how these aims fit with the organisation or agency's broader objectives
- the project's scope and extent
- any links with existing programs or other projects
- who is responsible for the project
- timeframe for decision-making that will affect the project's design
- some of the key privacy elements — for example, the extent and type of information that will be collected, how security and information quality are to be addressed, and how the information will be used and disclosed (these will be explored in more detail in subsequent stages of the PIA).

The project description should be kept fairly brief, and should not include analysis of the privacy implications, as this will be addressed in later stages of the PIA. This information is important as it provides context for the rest of the PIA. Information about the project prepared for the threshold assessment can also be usefully included at this stage. If the project is still at an early stage, it may not be possible to prepare a detailed description, but this can be updated as more becomes known about the project.

The project description should be sufficiently detailed to allow external stakeholders to understand the project, and should be written in plain English, avoiding overly technical language or jargon.

4. Identify and consult with stakeholders

Stakeholders are those who are or might be interested in or affected by the project being considered. An entity will have internal stakeholders and external stakeholders, including regulatory authorities, clients, advocacy organisations, service providers, industry experts, academics and others. The stakeholder list should identify both categories of stakeholders, and individuals and organisations within each of these categories. It may be necessary to add to the stakeholder list as the project progresses.

Identifying the project's stakeholders will assist when undertaking consultation on the PIA. It may not be necessary to consult with all the identified stakeholders, depending on the scale and likely privacy impacts of the project, but some form of consultation should occur as part of the PIA.

Consulting with stakeholders may assist in identifying privacy risks and concerns that have not been identified by the team undertaking the PIA, and possible strategies to mitigate these risks. Consultation may also offer stakeholders the opportunity to discuss risks and concerns with the entity and to gain a better understanding of, and provide comment on, any proposed mitigation strategies. Importantly, consultation is also likely to provide confidence to the public that their privacy has been considered. Failure to consult may give rise to criticism about a lack of consultation in relation to the project.

For consultation to be effective, stakeholders will need to be sufficiently informed about the project, be provided with the opportunity to provide their perspectives and raise any concerns, and have confidence that their perspectives will be taken into account in the design of the project. Many consultation models are available, including telephone or online surveys, focus groups and workshops, seeking public submissions, and stakeholder interviews. Different models will be appropriate for different stakeholder groups and different stages of the project, and careful consideration should be given to which consultation model/s will be appropriate in the circumstances.

Consultation does not necessarily need to be a separate step as it can be useful to consult throughout the PIA process. It is important that some form of targeted consultation is undertaken, even if widespread public consultation is not possible (for example, if a private organisation is concerned about sharing commercially sensitive information widely), such as with groups representing relevant sectors of the population, or advocacy groups with expertise in privacy.

5. Map information flows

After you have prepared a broad outline of the project's nature and scope, you need to describe and map the project's personal information flows. The analysis should be sufficiently detailed to provide a sense of what information will be collected, used and disclosed, how it will be held and protected, and who will have access to it.

To map information flows effectively, you will need to communicate with other staff and project stakeholders. If you try to map information flows 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 problems later on that may be difficult or expensive to remedy.

Detailed information mapping should include:

- whether identity verification will be necessary
- what personal information will be collected and how it will be collected
- its use and disclosure
- the processes for ensuring information quality
- security safeguards that are (or will be) in place
- the ability individuals have to access and correct their personal information.

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

Areas for consideration when you are mapping the information flows are outlined below. These points 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 in the privacy impact analysis stage. They will also be useful for the preparation of the PIA report.

If appropriate, consider using diagrams depicting the flow of information, or tables setting out the key information for different types of personal information to be used in the project.

Necessity of identity verification

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
- 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 entities, and what protections could be put in place to prevent other uses or adoptions
- other information that may need to be verified, such as an individual's qualifications.

Collection

Identify and describe:

- the personal information to be collected, including any sensitive information
- how the collection relates to the agency or organisation's functions or activities
- why the personal information, including the particular items and kinds of information, is 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
- if the method of collection may be unreasonably intrusive for some individuals (for example, seeking personal information from individuals in a public area where others may overhear).

Detail the collection process, including:

- how the information will be collected (for example, hard copy forms, electronic forms, online transactions, CCTV etc)
- whether unsolicited personal information may be used in the project
- where the information will be collected from (for example, directly from the individual, from other individuals or entities, or from publicly available sources)

- how an individual's circumstances will be taken into account when the personal information is being collected (for example, if they might require support to understand why the information is being collected)
- any legislation or other authority on which you are relying to collect the information
- collection alternatives that have been considered and rejected (for example, using de-identified information)
- how often the personal information is to be collected (once only or ongoing)
- any limits on the nature of the information to be collected (for example, information over a certain age)
- any potentially sensitive or intrusive methods of collection (for example, photographs, fingerprinting, drug testing, collection of genetic information)
- any covert methods of collection (such as surveillance) and why they are necessary and appropriate. Note that covert collection is generally highly privacy invasive, and should only take place in limited circumstances.

Identify and describe information (notice) about collection to be given to the individual and how it will be given, including:

- Purpose and authority
  - why the personal information is being collected
  - whether the collection is authorised or required by law, and if so, which law.
- 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 or disclosures that are made by those people or organisations
  - proposed uses or disclosures of the information for purposes other than the purpose of collection.
- Choice
  - whether there are choices for individuals about how their personal information is handled, and if so, whether you will inform them.

Use

Identify and describe how you intend to use the information:

- all the planned uses of the personal information, including infrequent uses
- how all these uses relate to the purpose of collection

- measures in place to prevent uses for secondary purposes or to ensure that any secondary uses are permitted under the APPs.

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

- whether consent is required for the secondary use
- if the use is related or directly related to the purpose of collection
- whether an individual can refuse consent for secondary uses and still be involved in the project
- any consequences for individuals who refuse consent
- how individuals will be involved in decisions if new, unplanned purposes for handling personal information occur during the project.

Data linkage or matching, which involves aggregating or bringing together personal information that has been collected for different purposes, has additional privacy risks. If your project will involve data linkage or matching, 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 entities)[8]
- how data-matching, linking or cross-referencing might be done
- any decisions affecting the individual that might 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 the information
- audit trails and other oversight 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.

Disclosure

Identify and describe:

- to whom, how and why the personal information will be disclosed
- whether the disclosed information will have the same privacy protections after it is disclosed
- whether the information is to be published, or disclosed to a register, including a public register
- whether an individual will be told about the disclosure and what choices they have (such as publishing or suppressing their information)
- whether the disclosure is authorised or required by law, and if so, which law

[8] See also the OAIC's guidance material on data-matching, available at www.oaic.gov.au

- whether the personal information will be disclosed to overseas recipients.

Information quality

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 and the risks of using inaccurate information
- the processes that ensure only relevant, up-to-date and complete information will be used or disclosed, including by any contracted service providers
- how personal information updates will be given to others who have previously been given personal information about an individual.

Security

Assess the project against your agency or organisation's IT, telecommunications and physical security measures.[9]

Identify and describe:

- security measures that will protect the personal information from loss, unauthorised access, use, modification, disclosure or other misuse (including for contracted service providers)
- how information will be transferred between sites
- how personal information will be protected if it will be managed by someone else
- who will have access
- who will authorise access
- the systems that will prevent and detect misuse or inappropriate access
- what action will be taken if there is a data breach.[10]

Retention and destruction

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

---

[9] See the OAIC's Guide to securing personal information for further information on reasonable steps entities are required to take under the Privacy Act to protect the information that they hold.

[10] See Data breach preparation and response — a guide to managing data breaches in accordance with the *Privacy Act 1988* (Cth) for more information on responding to data breaches.

- how compliance with this policy and any relevant legislation about record destruction will be assessed.

Access and correction

Identify and describe:

- how individuals can access their personal information, including any costs to the individual
- how the individual can have their personal information corrected, or annotations made, if necessary
- how decisions will be made about requests from individuals for access to or correction of their information.

6. Privacy impact analysis and compliance check

Once you have mapped the information flows, you need to identify and critically analyse how the project impacts upon privacy, both positively and negatively.

Privacy impact analysis investigates:

- the risk of privacy impacts on individuals (both serious and more minor) as a result of how personal information is handled
- whether privacy impacts are necessary or avoidable
- whether there are any existing factors that have the capacity to mitigate any negative privacy impacts
- how the privacy impacts may affect the project's broad goals
- the project's effect on an individual's choices about who has access to their personal information
- compliance with privacy law
- how the use of personal information in the project aligns with community expectations.

Ultimately, the privacy impact analysis should attempt to determine whether the project has acceptable privacy outcomes, or unacceptable privacy impacts. This analysis should include any stakeholder or public consultation results that may assist you to work out how to improve the project's privacy outcomes.

The analysis should include consideration of the content of the information and the context in which the information is collected. A negative privacy impact may not appear to be significant, but it is important to note that even minimal personal information, handled inappropriately, may impact on someone's privacy in ways an entity did not intend.

It is also important to note that some types of personal information are more sensitive than others, such as genetic, health or criminal conviction information.

Some key questions to consider are:

- Do individuals have to give up control of their personal information?
- Will the project change the way individuals interact with the entity, such as through more frequent identity checks, costs, or impacts on individuals or groups who do not have identity documents?
- Will decisions that have consequences for individuals be made as a result of the way personal information is handled in the project (such as decisions about services or benefits)?
- Is there a complaint-handling mechanism? If yes, is it visible, comprehensive and effective?
- How will you handle any privacy breaches?
- Are there audit and oversight mechanisms in place (including emergency procedures) in case the system fails?
- Does the project recognise the risk of function creep? (For example, is there an interest in using the personal information collected for the project for other purposes that might occur in the future?)
- How valuable would the information be to unauthorised users? (For example, is it information that others would pay money for or try to access via hacking?)
- Is any intrusion or surveillance fully justified and in proportion to the project's anticipated benefits? Is it the only way of achieving the aims of the project, and done in the least intrusive manner? Is it subject to legislative or judicial authority? What auditing and oversight measures are in place?
- How consistent is the project with community values about privacy? (You are likely to need to undertake some form of consultation in order to assess this, but could also look at community responses to similar projects, or research into community attitudes about privacy).[11]

Ensuring compliance

While a PIA is more than a compliance check, it is essential to consider compliance with privacy legislation and any other privacy law relevant to your agency or organisation. This guide provides guidance on ensuring compliance with the Privacy Act, but there may also be other privacy-related legislation and rules that apply to your entity, such as secrecy provisions or information handling obligations in other legislation. It is also important to note that, even if the project appears to be compliant with privacy legislation, there may still be other privacy risks that need to be addressed, such as community expectations.

You will need to consider whether your project complies with each of the APPs. A summary of each APP is below, but you should read the full text of the APPs[12] before completing this section. For each APP, consider whether your project complies and identify any risks to compliance. You should document and provide specific details about either how your project complies with the APP or why

[11] For example, the OAIC's Community Attitudes to Privacy research.

[12] Available at Read the Australian Privacy Principles

you are not required to comply with an APP, and any considerations you took into account. The Guidelines to the APPs[13] provide a comprehensive guide to interpreting and applying the APPs.

Some guidance questions are provided below. These questions cover some of the same issues that you considered when you mapped the information flows, but focus more closely on compliance with the Privacy Act. Responding to the questions set out for each APP may assist you in assessing whether the way personal information will be handled in your project is compliant.

These questions are not exhaustive and are provided as a guide only. You may need to consider other issues, taking into account the nature of your project. Consider making recommendations as you go through your compliance check (see 'Recommendations' below).

APP 1 — open and transparent management of personal information

The APP entity must have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way. The APP entity must:

- *take reasonable steps to implement practices, procedures and systems that will ensure it complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints*
- *have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information*
- *take reasonable steps to make its APP Privacy Policy available free of charge and in an appropriate form (usually on its website)*
- *upon request, take reasonable steps to provide a person or body with a copy of its APP Privacy Policy in the particular form requested.*

Questions to consider:

- Have reasonable steps been taken to implement practices, procedures and systems that will ensure compliance with the APPs and any binding registered APP code?
- Do you have an APP Privacy Policy which:
  - is clearly expressed and up-to-date
  - covers the matters listed in APP 1.4
  - is freely available at no cost (for example, on your website)?
- Have reasonable steps been taken to ensure that procedures and systems are in place for handling privacy inquiries and complaints?

[13] Available at Australian Privacy Principles Guidelines

APP 2 — anonymity and pseudonymity

Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter, unless an exception applies.

Questions to consider:

- Will individuals have the option of not identifying themselves or of using a pseudonym when participating in the project?
- Are you required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves?
- Is it impracticable for you to deal with individuals who have not identified themselves or who have used a pseudonym?
- Are there categories of individuals affected by the project who are likely to seek to interact with your agency or organisation anonymously or using a pseudonym?

APP 3 — collection of solicited personal information

Any personal information collected (other than sensitive information) must be reasonably necessary for (or if the APP entity is an agency, reasonably necessary for or directly related to) one or more of the APP entity's functions or activities.

An APP entity must not collect sensitive information about an individual unless one of the exceptions listed in APP 3.3 or APP 3.4 applies, such as if the individual consents and the information is reasonably necessary for (or if the APP entity is an agency, reasonably necessary for or directly related to) one of more of the entity's functions or activities.

Personal information can only be collected by lawful and fair means.

Personal information about an individual must only be collected from the individual unless one of the exceptions in APP 3.6 applies.

Questions to consider — personal information:

- If you are an agency, is the information being collected necessary for or directly related to one or more of your functions?
- If you are an organisation, is the information being collected necessary for one or more of your functions?
- Is the collection authorised or required by an Australian law or a court/tribunal order?
- Will the information be collected by lawful and fair means?
- Will the personal information be collected from the individual concerned? If not, do any of the exceptions in APP 3.6 apply?

Questions to consider — sensitive information:

- Can you rely on any of the exceptions in APP 3.3 or APP 3.4 for the collection of sensitive information? For example, has the individual consented or is the collection required or authorised by or under an Australian law or a court/tribunal order?
- Will there be guidance or processes in place to assist with the handling of sensitive information?
- If the collection and management of sensitive information will be outsourced, will measures be in place to protect the sensitive information and will compliance with APP 3 be monitored?

APP 4 — dealing with unsolicited personal information

Where an APP entity receives unsolicited personal information, it must determine whether it would have been permitted to collect the information under APP 3. If so, APPs 5 to 13 will apply to that information. If the information could not have been collected under APP 3, and the information is not contained in a Commonwealth record, the APP entity must destroy or de-identify that information as soon as practicable, but only if it is lawful and reasonable to do so.

Questions to consider:

- Are there practices, procedures and systems in place for dealing with the receipt of unsolicited personal information that will ensure compliance with APP 4?

APP 5 — notification of the collection of personal information

An APP entity that collects personal information about an individual must take reasonable steps to notify the individual, or otherwise ensure the individual is aware, of the matters listed in APP 5.2.

The matters include:

- *the APP entity's identity and contact details*
- *the fact and circumstances of collection*
- *whether the collection is required or authorised by law*
- *the purposes of collection*
- *the consequences if personal information is not collected*
- *the APP entity's usual disclosures of personal information of the kind collected by the entity*
- *information about the APP entity's APP Privacy Policy*
- *whether the APP entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.*

An APP entity must provide notification before, or at the time it collects personal information. If this is not practicable, notification should be provided as soon as practicable after collection.

Questions to consider:

- Consider each of the matters listed in APP 5.2. Will steps be taken to notify the individual of each matter? If steps are not being taken in relation to a matter, is it reasonable in the circumstances not to notify the individual?

- Are practices, procedures and systems in place to ensure reasonable steps are taken to tell the individual about the matters listed in APP 5.2 at or before (or if not practicable, as soon as practicable after) the time of collection?
- If the information is collected directly from the individual, will notice be given to the individual (such as by displaying the notice on a form, providing a link on a web page or advising the individual over the phone) and the individual asked to confirm they have been notified of the APP 5 matters before providing their personal information?

APP 6 — use or disclosure of personal information

An APP entity can only use or disclose personal information for the particular purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies, such as where the individual has consented to the use or disclosure of the information.

Note that APP 6 does not apply to organisations using or disclosing personal information for the purpose of direct marketing (refer to APP 7), or government related identifiers (refer to APP 9).

Questions to consider:

- If the use or disclosure is for a secondary purpose, will the individual be asked to provide consent? Will you keep a record of the consent?
- If the individual will not be asked to consent, do any of the other exceptions to the requirement for consent in APP 6.2 apply?
- If you are an agency, is it possible that personal information may be used or disclosed because it is reasonably necessary for an enforcement related activity? If so, are procedures in place to ensure a written note of the use or disclosure is made in compliance with APP 6.5?

APP 7 — direct marketing

An organisation must not use or disclose personal information for the purpose of direct marketing unless an exception applies, such as where the individual has consented.

Where an organisation is permitted to use or disclose personal information for the purpose of direct marketing, it must always:

- *allow an individual to request not to receive direct marketing communications (also known as 'opting out'), and*
- *comply with that request.*

An organisation must provide its source for an individual's personal information, if requested to do so by the individual.

Questions to consider if you are an organisation using or disclosing personal information for the purpose of direct marketing:

- Do any of the exceptions permitting the use or disclosure of personal information for the purpose of direct marketing as set out in APP 7.2 or APP 7.3 apply?

- If sensitive information is to be used or disclosed for the purpose of direct marketing, will the individual be asked to consent? Consider APP 7.4.
- If you are a contracted service provider for a Commonwealth contract, is the use or disclosure necessary to meet an obligation under the contract? Consider APP 7.5.
- If use or disclosure of personal information for the purpose of direct marketing is permitted under APP 7, will individuals be given the opportunity to request not to receive direct marketing communications?
- Does your organisation have any guidance or processes in place to help manage your direct marketing obligations?
- Have you considered your obligations under the *Do Not Call Register Act 2006* and the *Spam Act 2003*?

APP 8 — cross-border disclosure of personal information

Before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the information, unless an exception applies, such as the individual has given informed consent.

An APP entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (see s 16C of the Privacy Act).

Questions to consider:

- If personal information is to be disclosed to an overseas recipient, will reasonable steps be taken to ensure the overseas recipient does not breach the APPs (other than APP 1) in relation to the information?
- Does an exception under APP 8.2 apply? For example, is the disclosure required or authorised by or under an Australian law or a court/tribunal order?
- If no exception applies, are appropriate arrangements in place with overseas recipients to ensure that personal information is handled in accordance with the APPs?

APP 9 — adoption, use or disclosure of government related identifiers

An organisation must not adopt, use or disclose a government related identifier of an individual as its own identifier of the individual unless an exception applies.

Questions to consider:

- Is any planned adoption, use or disclosure of government related identifiers permitted under an exception in APP 9? For example, is it required or authorised by or under an Australian law or a court/tribunal order?

APP 10 — quality of personal information

An APP entity must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete.

An APP entity must take reasonable steps to ensure that the personal information it uses and discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

- Will reasonable steps be taken to ensure that any personal information collected is accurate, up-to-date and complete? Will guidance or processes be in place to ensure these steps are followed?
- Will reasonable steps be taken to ensure that any personal information being used or disclosed is accurate, current, complete and relevant, having regard to the purpose of the use or disclosure? Will guidance or processes be in place to ensure these steps are followed?

APP 11 — security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that the information is de-identified, unless an exception applies.[14]

- Will reasonable steps be taken to ensure that the personal information to be collected is protected from unauthorised access, modification or disclosure? Consider whether reasonable steps will be taken to ensure technical and physical security is in place to protect against misuse, interference and loss, and whether there will be technical and physical security guidance/processes in place.
- Will control procedures be in place requiring authorisation before personal information is added, changed or deleted?
- Will audit mechanisms identify inappropriate system access?
- Will reasonable steps be taken to destroy or de-identify the personal information which is no longer needed for any authorised purpose?
- If reasonable steps will not be taken to destroy or de-identify the personal information which is no longer needed for any authorised purpose, do any of the exceptions apply (for example, the information is part of a Commonwealth record or the APP entity is required by law or a court/tribunal order to retain the information)?
- Will guidance or processes be in place to help determine when and how destruction or de-identification of personal information will occur?
- Is staff training adequate to fulfil the reasonable steps required?

[14] See the OAIC's Guide to securing personal information for further information on reasonable steps entities are required to take under the Privacy Act to protect the information that they hold.

APP 12 — access to personal information

An APP entity that holds personal information about an individual must give the individual access to that information on request, unless an exception applies.

Questions to consider:

- Will processes be put in place to:
  - generally provide an individual with access to information being held about them
  - deal with requests for access within the appropriate time (for agencies, 30 days; for organisations, within a reasonable period after the request is made)
  - give access in the manner requested, if reasonable and practicable
  - ensure compliance with APP 12.5 and 12.6, relating to providing other means of access where a request is refused
  - ensure compliance with APP 12.7 and APP 12.8, relating to access charges
  - ensure a written notice is given to an individual whose access request is refused, in accordance with APP 12.9 and APP 12.10?
- Will individuals be made aware of how to access their personal information?

APP 13 — correction of personal information

An APP entity must take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.

This requirement applies where:

- *the APP entity is satisfied the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held, or*
- *the individual requests the entity to correct the information.*

There are minimum procedural requirements in relation to correcting personal information, including when an APP entity must:

- *take reasonable steps to notify other APP entities of a correction*
- *give notice to the individual which includes reasons and available complaint mechanisms if correction is refused*
- *take reasonable steps to associate a statement with personal information it refuses to correct*
- *respond to a request for correction or to associate a statement, and*
- *not charge an individual for making a request, correcting personal information or associating a statement.*

Questions to consider:

- Will individuals be made aware of how to request correction of their personal information?
- Will reasonable steps be taken to correct information that is not accurate, out of date, incomplete, irrelevant or misleading, having regard to the purpose for which the information is held?
- Are processes in place for responding to requests from individuals to correct personal information?
- Are processes in place for identifying and correcting personal information that is inaccurate, out of date, incomplete, irrelevant or misleading?
- Will individuals be informed about the reasons if a request for correction is denied?
- Are processes in place for associating a statement with personal information if a request for correction is denied?

7. Privacy management — addressing risks

Through the privacy impact analysis and compliance check, you may have identified risks to privacy in the project's current design. Risks to privacy can arise in many circumstances, for example, from collecting more information than is needed, using intrusive means of collection, or disclosing sensitive details more widely than is justified or necessary. These risks may be to individual privacy, to an entity's compliance and reputation, or both.

At this stage, you need to consider what options may allow you to remove, minimise or mitigate any negative privacy impacts identified through the privacy impact analysis.

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

A number of factors should be taken into account when considering strategies for dealing with negative privacy impacts identified in the privacy impact analysis stage, including:

- necessity — minimising the collection of personal information to what is strictly necessary
- proportionality — any negative privacy impact should be in proportion to, or balanced with, any benefits to be achieved from the project
- transparency and accountability — privacy measures should be transparent to individuals, through adequate collection notices and privacy policies
- implementation of privacy protections — consider how organisational/agency policies and procedures can support privacy, as well as practical elements such as staff training
- flexibility — take into account the diversity of individuals affected by the project, and whether they may respond or be affected differently to the sharing of their personal information
- privacy by design — privacy protections should be included in law or other binding obligations, and built into new technologies

- privacy enhancing technologies — consider whether any privacy enhancing technologies can be used in the project, and the impact of privacy invasive technologies.

Strategies to reduce or mitigate privacy risks may include technical controls (for example, access control mechanisms, encryption, design changes), more operational controls (for example, organisational/agency policies or procedures, staff training, oversight and accountability measures) or communication strategies (for example, privacy notices). Some examples of possible mitigation strategies for common privacy risks are below. This is not a comprehensive list of possible risks to privacy; rather, it is intended to provide an indication of the types of strategies that you might consider.

Privacy risks and mitigation strategies

Possible risks	Suggested mitigation strategies
Anonymity and pseudonymity: Individual's personal information will be collected when it is not required (for example, to provide information)	Consider whether you can use information that does not identify a person. If it is necessary to distinguish between different people, consider whether you can use pseudonyms instead.
Collection: Personal information will be collected without a clear purpose, which could increase the risk of unauthorised uses and disclosures.	Ensure that you have clearly identified and documented the purposes for which you will be collecting and using personal information, and that others in your organisation or agency are aware of these purposes.
Collection: Unjustifiably intrusive methods will be used to collect personal information	Consider other, less intrusive options for collecting the information. If these options are not suitable, the reasons should be documented in the PIA report.
Notification of collection: Collection notice will not be provided to all individuals, for example those using non-standard communication channels	Ensure that the collection notice is consistent and accessible across all methods of collection, including hard-copy forms, online forms and via telephone. Provide a post-collection notice where notice prior to or at the time of collection is not practicable.
Notification of collection: Collection notice may not be accessible to all consumers, for example those from culturally and linguistically diverse backgrounds	Ensure that the collection notice is available in a range of formats and an appropriate range of languages for the target group.
Collection, use or disclosure: Consent for collection, use or disclosure of information may not be valid	Review the process by which you plan to seek consent. Ensure that the consent will be truly voluntary, informed, current and specific, and given by a person with the capacity to provide consent.
Use or disclosure: Individuals may be surprised or upset by a secondary use or disclosure, resulting in privacy complaints and/or negative publicity	Undertake further stakeholder consultation to test community expectations about your proposed uses and disclosures. Consider whether it is possible to seek consent for secondary uses and disclosures.

Possible risks	Suggested mitigation strategies
Disclosure: De-identification of personal information before disclosure may not prevent re-identification	Review de-identification procedures to ensure that sufficient details are removed so that the recipient of the information will not be able to re- identify it, or combine it with other information to establish an individual's identity.
Information quality: Poor quality information may lead to inappropriate decisions that have a negative impact on the individuals concerned.	Check the reliability of tools used to collect or process personal information. Consider establishing regular checks of tools and procedures for human data processing. Identify and document procedures for how often personal information will be reviewed and updated.
Information security: The organisation or agency does not have basic information security standards in place.	Review the OAIC's Guide to information security and identify what additional steps your organisation or agency needs to take to ensure protection of personal information.
Information security: Information is saved onto personal storage devices, increasing the risk of accidental loss of personal information.	Control the use of portable storage devices through organisational/agency policies and technical controls.
Access and correction: Individuals are not able to easily access and correct their personal information.	Identify how access and correction procedures can be made more straightforward. Consider providing individuals with routine access to their personal information.

8. Recommendations

A number of recommendations for the future of the project may emerge from the stages above. These recommendations should identify avoidable impacts or risks and how they can be removed or reduced to a more acceptable level. For example, recommendations could address:

- changes that would achieve a more appropriate balance between the project's goals, the interests of affected individuals and the entity's interests
- privacy management strategies, discussed above in 'Privacy management — addressing risks', that will reduce or mitigate privacy risks
- the need for further consultation
- whether the privacy impacts are so significant that the project should not proceed.

Recommendations might also go beyond project-specific matters to overall privacy risk management for the entity conducting the project.

Recommendations should be set out in the PIA report (discussed in more detail below). It should be clear who the recommendations are addressed to, for example to different areas of the organisation

or agency, particular members of the project team, or those in positions of authority within the organisation or agency. Recommendations should also include a timeframe for implementation.

9. Report

A report that sets out all the PIA information is an important output of the PIA process. Key elements for inclusion in a PIA report include:

- project description
- PIA methodology
- description of information flows
- outcome of privacy impact analysis and compliance checks, including positive privacy impacts and privacy risks that have been identified, and strategies already in place to protect privacy
- recommendations to avoid or mitigate privacy risks
- description of any privacy risks that cannot be mitigated, the likely community response to these risks, and whether these risks are outweighed by the public benefit that will be delivered by the project
- if necessary, more detailed information (for example about consultation processes and outcomes) can be provided in appendices.

The OAIC has developed a PIA tool[15] to help you conduct a PIA, report its findings and respond to recommendations. Entities are encouraged to take a flexible approach and adapt the tool to suit the size, complexity and risk level of their project. A suggested format for a PIA report is also provided in the table below. In addition, links to sample PIA reports and templates developed by other organisations are at Appendix A.

Suggested PIA Report Format

Section heading	Content
Executive summary	Depending on the length of the PIA report, it may be valuable to provide an Executive Summary. This should include: • the purpose of the PIA • brief project description and key information flows • summary of findings • recommendations or existing strategies to address identified privacy risks.
PIA methodology	This section should outline the approach taken to undertaking the PIA, including any stakeholder consultation. (Refer to 'Plan the PIA', and 'Identify and consult with stakeholders'.)

[15] Available at oaic.gov.au/pia-tool

Section heading	Content
Project description	In this section, describe the key features of the project, including any relevant background or the rationale for the project. Outline how personal information will be handled in the project, including through diagrams illustrating information flows if appropriate. Information flows can also be addressed in more detail in the next section if required. This section should be kept fairly short, and should not contain any analysis of privacy implications, as this will be addressed in later sections. (Refer to 'Describe the project', and 'Map information flows'.)
Analysis	This section should identify: • the project's impacts (positive and negative) on privacy • privacy risks that may arise from the project, including whether the project complies with privacy legislation • any strategies that are already in place to remove, minimise or mitigate privacy risks • recommendations about additional strategies required to remove, minimise or mitigate privacy risks. It may be appropriate to present an assessment of the project against each of the APPs or any other legal obligations relating to privacy. It is important to remember, however, that the PIA is more than a compliance check, and that other questions may also need to be addressed. If the analysis is lengthy due to the complexity of the project or significant privacy impacts, it may be appropriate to split this information into separate sections; for example: • including information on privacy impacts and risks, existing strategies, and recommendations in separate sections • presenting separate analyses for discrete parts of the project or information flows. (Refer to 'Privacy impact analysis and compliance check', 'Privacy management — addressing risks' and 'Recommendations'.)

Section heading	Content
Conclusion	This section should summarise the overall findings and outline the conclusions of the PIA, including whether the privacy safeguards currently in place or identified in the recommendations will be sufficient to protect personal information handled in the project. It should also outline the next steps in the PIA process (refer to 'Respond and review'). Agencies who have been directed to undertake a PIA are required to provide their response to the recommendations contained in the PIA report to the OAIC, and this should be considered in the presentation of the report.
Appendices	Appendices can be used to communicate more detailed information, for example the nature of consultation, who participated in consultation and the outcomes of the project.

It is important that the PIA report is a practical document that can easily be interpreted and applied by the project team and the entity as a whole, as well as being clear to other project stakeholders. While the report should outline the steps that have been followed in undertaking the PIA, it might be appropriate to combine reporting on stages that consider related issues. For example, as outlined in the suggested format above, reporting on the privacy impact analysis could be combined with risk mitigation or avoidance strategies. This would provide readers with a complete picture of how information will be handled in the project, the privacy implications, and how identified risks will be addressed.

The OAIC strongly encourages the publication of PIA reports. This contributes to the transparency of the project's development and intent, and demonstrates to stakeholders and the community that the project has undergone critical privacy analysis, potentially reducing community concerns about privacy. However, the OAIC acknowledges that there may be circumstances when the full release of a PIA report may not be appropriate; for example, if the project is still in its very early stages, or if there are security or commercial reasons for not releasing the full report. Where there are difficulties making the full PIA available, the OAIC encourages the release of a summary or edited version.

10. Respond and review

It is important that action is taken to respond to the recommendations raised in the report, and to continue to review and update the PIA. A PIA should be regarded as an ongoing process that does not end with the preparation of the PIA report.

Respond to recommendations

Responding to recommendations in a PIA is one of the most important aspects of the process and will lead to better privacy outcomes. The project manager and the entity may make a decision not to implement all the recommendations set out in the PIA report. However, they should document which recommendations they intend to implement (or have already implemented), as well as those which

they do not intend to implement and the rationale for this decision. Ideally, the entity's response to the PIA recommendations will be published together with the PIA report. If a PIA report is not published, the entity should consider providing it to significant stakeholders to assist in effective implementation of recommendations.

If the OAIC has directed an agency to undertake a PIA, the OAIC will review the PIA to ensure that the agency has responded to each recommendation by indicating whether or not it intends to implement, or has already implemented, the recommendation, and the rationale for this decision.[16]

It may be helpful to prepare a plan for implementing the recommendations, indicating a specific timeframe for remedying or mitigating the risks that have been identified and identifying who is responsible for the implementation.

Consideration should also be given to ongoing management of any privacy risks inherent in the project. This could be incorporated into an entity's overall risk management strategy.

Independent review/audit

There are benefits to seeking independent review of a PIA. Review of a PIA and its implementation by an independent third party can assist in ensuring that PIAs have been properly carried out and their recommendations implemented (or there is a clear rationale for not implementing the recommendations). External review can have considerable benefits; for example, reviewers may identify failures to fully implement recommendations that could expose entities to serious risks if they are not addressed.

On occasion, the OAIC may review an entity's PIA. For example, where the OAIC directs an agency to give the OAIC a PIA under s 33D of the Privacy Act, the OAIC will generally review the PIA report to ensure that it sufficiently identifies privacy impacts and sets out appropriate recommendations for managing, minimising or eliminating those impacts. During that process the OAIC may provide comments on the PIA's adequacy, recommendations and the agency's response to the recommendations.

If independent review is not undertaken, there is still benefit in undertaking (and documenting) an internal review, addressing the implementation of the mitigation and avoidance measures set out in the recommendations, and whether any further changes are required to reduce privacy risks.

Update the PIA if required

Many projects undergo changes before they are finally implemented. As the project progresses, the PIA should be revisited, and updated or revised if developments in the design or implementation of the project create new privacy impacts that were not previously considered. If the changes are substantial and result in significant new privacy impacts that were not considered in the PIA, it may be necessary to undertake a new PIA, following the steps outlined above.

[16] See the OAIC's Guide to privacy regulatory action — Chapter 8: Directing a privacy impact assessment for more information.

Glossary

Unless otherwise stated, terms used in this Guide have the same meaning as in the Privacy Act. Some of these terms are explained in more detail in the APP Guidelines.[17]

Agency has the meaning set out in s 6 of the Privacy Act:

> agency means:
>
> (a) a Minister; or
>
> (b) a Department; or
>
> (c) a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a Commonwealth enactment, not being:
>
> (i) an incorporated company, society or association; or
>
> (ii) an organisation that is registered under the *Fair Work (Registered Organisations) Act 2009* or a branch of such an organisation; or
>
> (d) a body established or appointed by the Governor-General, or by a Minister, otherwise than by or under a Commonwealth enactment; or
>
> (e) a person holding or performing the duties of an office established by or under, or an appointment made under, a Commonwealth enactment, other than a person who, by virtue of holding that office, is the Secretary of a Department; or
>
> (f) a person holding or performing the duties of an appointment, being an appointment made by the Governor-General, or by a Minister, otherwise than under a Commonwealth enactment; or
>
> (g) a federal court; or
>
> (h) the Australian Federal Police; or
>
> (ha) a Norfolk Island agency; or
>
> (j) the nominated AGHS company; or
>
> (k) an eligible hearing service provider; or
>
> (l) the service operator under the *Healthcare Identifiers Act 2010*.

APPs means the Australian Privacy Principles set out in the Privacy Act.

APP entity means an agency or organisation as defined in the Privacy Act.

Collection refers to collection of personal information by an entity for inclusion in a record or generally available publication.

[17] See Chapter B, Key Concepts.

Commissioner means the Information Commissioner within the meaning of the *Australian Information Commissioner Act 2010*.

De-identified refers to information that is no longer about an identifiable individual or an individual who is reasonably identifiable.

Disclosure generally refers to when an APP entity releases information from its effective control, for example to another entity or individual.

Entity – see 'APP entity'.

OAIC means the Office of the Australian Information Commissioner.

Organisation has the meaning set out in s 6C of the Privacy Act:

> 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.

PIA means privacy impact assessment

Personal information has the meaning set out in s 6 of the Privacy Act:

> personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.

Privacy Act means the *Privacy Act 1988*.

Project, in this Guide, is used to refer to the full range of activities and initiatives that may have privacy implications.

Sensitive information has the meaning set out in s 6 of the Privacy Act:

> sensitive information means:
>
> (a) information or an opinion about an individual's:
>
> (i) racial or ethnic origin; or
>
> (ii) political opinions; or

(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 orientation or practices; 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; or

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.

Use generally refers to handling and management of personal information within an entity.

Appendix A — Acknowledgments and resources

Acknowledgements

In preparing the current version of this guide, and earlier versions in 2006 and 2010, the OAIC 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 Victoria and the work of Professor David Flaherty. The work of David Wright and colleagues has been of particular value in preparing the current version of the PIA Guide.

PIA resources

Some of these resources include report templates, which you may be able to adapt for your agency or organisation.

Victoria (Australia)

Office of the Victorian Privacy Commissioner, Privacy Impact Assessments

New Zealand

Office of the Privacy Commissioner, Privacy Impact Assessment Toolkit (2015)

Canada

Office of the Information and Privacy Commissioner of Alberta, Privacy Impact Assessments

Treasury Board of Canada Secretariat, Directive on Privacy Impact Assessment (2010)

United Kingdom

Information Commissioner's Office, Data Protection Impact Assessments

United States of America

Privacy Office of the Department of Homeland Security, Privacy Impact Assessments — The Privacy Office Official Guidance (2010)

Other resources

Several other resources were consulted in preparing the 2014 version of this guide. These include (but are not limited to):

- Privacy Impact Assessment Framework (PIAF) website (containing various resources including David Wright and Kush Wadhwa, A Step-by-Step Guide to Privacy Impact Assessment, presentation paper for the second PIAF workshop, Poland, 2012
- David Wright and Paul De Hert (eds), Privacy Impact Assessment, Springer, 2012

- Health Information and Quality Authority (Ireland) International Review of Privacy Impact Assessments, 2010.

The International Association of Privacy Professionals has additional resources available to its members.

PIA reports

A small sample of PIA reports or summaries published by some national and international government agencies and organisations follows. While the majority of these examples are from government sources, the OAIC strongly encourages the publication of PIA reports by both agencies and organisations.

The OAIC does not endorse any of these reports or encourage a particular format for PIA reports. This information is provided to give entities some ideas about different PIA approaches.

Australia

- Attorney-General's Department, Privacy Impact Assessment — Extension of Document Verification Service to Private Sector Organisations (2012)
- Australian Bureau of Statistics, Australian Health Survey — Privacy Impact Assessment (2011)
- Comcare, Data-matching program with the Australian Taxation Office (2013)
- Department of Health and Ageing, Privacy Impact Assessment Report — Personally Controlled Electronic Health Record (PCEHR) (2011)
- Department of Health and Ageing and Medicare Australia, Privacy Impact Assessment — Ensuring the Integrity of Medicare: Increased MBS Compliance Audits (2009)

New Zealand

- Immigration New Zealand, Privacy Impact Assessment — Collection and Handling of Biometrics at the Ministry of Business, Innovation, and Employment (2012)
- Immigration New Zealand, Privacy Impact Assessment for Exchange of Information between the New Zealand Department of Labour and the Australian Department of Immigration and Citizenship, as part of the Five Country Conference High Value Data Sharing Protocol (2010)
- Ministry of Agriculture — Biosecurity New Zealand, FarmsOnLine Privacy Impact Assessment (2011)
- Ministry of Justice and New Zealand Police, Privacy Impact Assessment: Report on the Trans-Tasman Criminal History Information Sharing Trial (2013)
- Statistics New Zealand, Privacy Impact Assessment for the Integrated Data Infrastructure (2012)

Canada

- Canadian Institute of Health Information, Privacy Impact Assessments

- Veterans Affairs Canada, Privacy Impact Assessment Index

United Kingdom

- Northern Ireland Statistics and Research Agency, Report of a Privacy Impact Assessment in relation to the 2011 Census Northern Ireland (2010)
- The Scottish Government, Children and Young People (Scotland) Bill, Privacy Impact Assessment Report (2013)

United States of America

- Department of Homeland Security, Privacy Compliance
- Nlets — the International Justice and Public Safety Network, Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field (2011)