Privacy Impact Assessment Tool

[Privacy Impact Assessment Tool 2](#_Toc105080705)

[Part 1: Plan the PIA 3](#_Toc105080706)

[Description of the project and parties 3](#_Toc105080707)

[Stakeholder identification 3](#_Toc105080708)

[Map information flows 3](#_Toc105080709)

[Part 2: Privacy impact analysis and compliance check 4](#_Toc105080710)

[Privacy impact analysis 4](#_Toc105080711)

[APP 1 — Open and transparent management of personal information 4](#_Toc105080712)

[APP 2 — Anonymity and pseudonymity 6](#_Toc105080713)

[APP 3 — Collection of solicited personal information 6](#_Toc105080714)

[APP 4 — Dealing with unsolicited personal information 8](#_Toc105080715)

[APP 7 — Direct marketing 8](#_Toc105080716)

[APP 10 — Quality of personal information 8](#_Toc105080717)

[APP 11 — Security of personal information 9](#_Toc105080718)

[APP 12 — Access to personal information 10](#_Toc105080719)

[Part 3: Privacy management — addressing risks 11](#_Toc105080720)

[Summary of risks and recommendations 12](#_Toc105080721)

## Privacy Impact Assessment Tool

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

The term ‘project’ covers the full range of activities and initiatives that may have privacy implications.

Additional resources may be found at [*Guide to undertaking privacy impact assessments*](https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/)and [PIA eLearning course](https://www.oaic.gov.au/privacy/training-resources/e-learning-undertaking-a-privacy-impact-assessment/). Additional resources are also listed below.

|  |  |
| --- | --- |
| Name of project |  |
| Name of business |  |
| Date |  |
| Contact person | Name:  Email: |

## Part 1: Plan the PIA

### Description of the project and parties

[Delete the text below and add your description of the project and parties]

This section should include a broad, ‘big picture’ description of the project, including:

* the project’s overall aims
* the project’s scope and extent
* the extent and type of information that will be collected,
* how the security of the collected information is to be protected
* how the information will be used

### Stakeholder identification

[Delete the text below and add your description of your stakeholder consultation process.]

This section should include:

* a list of internal and external stakeholders who may have their information collected or used (generic terms for groups of people are acceptable, i.e. employees)

### Map information flows

[Delete the text below and insert your information flow diagram or description.]

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, and how it will be held/stored and protected, and who will have access to it. A flow diagram that shows the flow of information involved in the project can be used rather than a text explanation in this section.

## Part 2: Privacy impact analysis and compliance check

### Privacy impact analysis

[Delete the text below and insert your description of the positive and negative privacy impacts of your project]

This section should identify and critically analyse how the project impacts upon privacy, both positively and negatively.

### APP 1 — Open and transparent management of personal information

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

|  |
| --- |
| What reasonable steps been taken to implement practices, procedures and systems that will ensure an individual’s personal information remains confidential? |
|  |

|  |
| --- |
| Is the organisation’s privacy policy meeting the following requirements?   * Is clearly expressed, understandable and up-to-date * is freely available at no cost. |
|  |

|  |
| --- |
| What privacy policy statement will be added to your social media site?  *Place a copy of this intended privacy statement in the space below.* |
|  |

|  |
| --- |
| Are there procedures and systems in place for handling privacy inquiries and complaints?  *Identify the process (internal and external) for making a privacy inquiry or complaint, including who is responsible for complaint handling. Is it visible, comprehensive and effective?* |
|  |

### 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.

|  |
| --- |
| Will individuals have the option of not identifying themselves or of using a pseudonym? If not, explain why it is impracticable for you to deal with individuals who have not identified themselves or who have used a pseudonym.  *Describe how individuals will be provided with the option of not identifying themselves or of using a pseudonym. Alternatively, explain why it is impracticable for you to deal with individuals who have not identified themselves (for example, if you need to deliver purchased goods to an individual, you may need to know their name if the individual needs to sign for delivery). See Chapter 2 of the APP Guidelines for more information about when it may be impracticable to deal with an individual who is not identified.* |
|  |

### APP 3 — Collection of solicited personal information

Any personal information collected (other than sensitive information) must be reasonably necessary for (or if your entity is an agency, reasonably necessary for, or directly related to) one or 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.

| If you are an organisation, is the information being collected necessary for one or more of your functions or activities?  *List each item of personal information that will be collected (e.g. name, date of birth, address) and explain why each item is necessary for one or more of your functions or activities. You should only collect the minimum amount of personal information that is necessary for the relevant function or activity (‘data minimisation’).*  *Data minimisation is an important concept that can help reduce the privacy impacts for individuals that may be associated with your project. Minimising the amount of data that you collect can also help to mitigate security risks. For example, collecting more personal information than is necessary may increase the risk of harm to an individual in the event of a data breach. Holding large amounts of personal information may also increase the risk of unauthorised access by internal or external sources.*  Warning icon: Privacy risk: If some personal information is not reasonably necessary for the project, there may be a risk of over collection. For example, it may not be necessary to collect all personal information on an individual’s driver licence when the purpose of collection is to verify the individual’s age. |
| --- |
|  |

| Will the information be collected by lawful and fair means?  *Describe the means by which personal information will be collected.*  Warning icon: **Privacy risk**: Your method of collection may be ‘unfair’ if it involves intimidation, deception or is unreasonably intrusive. For example, it would usually be unfair to collect personal information covertly without the knowledge of the individual (however, this will depend on the circumstances). |
| --- |
|  |

| Will the personal information be collected only from the individual concerned?  Warning icon: *Describe how, and from which other sources, the personal information will be collected.* Privacy risk: There may be a risk of the information being inaccurate, out-of-date or incomplete if collected from another source. |
| --- |
|  |

### 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.

| 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 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.

| 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? |
| --- |
|  |

### APP 10 — Quality of personal information

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

An organisation 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.

| What steps will you take to ensure the personal information collected is accurate, up to date and complete? Will guidance or processes be in place in your website or social media channel to ensure these steps are followed? |
| --- |
|  |

### APP 11 — Security of personal information

An organisation 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 organisation no longer needs personal information for any purpose for which the information may be used or disclosed, the entity must take reasonable steps to destroy the information or ensure that the information is de-identified, unless an exception applies.

The OAIC’s [*Guide to Securing Personal Information*](https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/)sets out the reasonable steps the OAIC expects entities to take to protect personal information.

| Are there technical security measures in place to protect the personal information that will be collected, used and/or disclosed as part of this project?  *Describe the technical controls (such as software security, encryption, whitelisting and blacklisting, backing up, email security etc) that have been, or will be, implemented for the project, including any relevant policies and procedures. Include links or attachments where appropriate.*  Warning icon: **Privacy risk**: If there are inadequate technical security measures in place, consider whether there is a risk that the information will not be properly protected, leading to misuse, interference, loss, unauthorised access, modification or disclosure. Consider the nature of the personal information collected and how valuable it would be to unauthorised users? |
| --- |
|  |

| Are there physical security measures in place to protect the personal information that will collected, used and/or disclosed as part of this project?  *Describe the physical security measures that have been, or will be implemented, for the project, including any relevant policies and procedures. Include links or attachments where appropriate.* |
| --- |
|  |

| Have you completed a separate security risk assessment?  *If so, please refer to or attach a copy of the assessment to this PIA.* |
| --- |
|  |

| Do you have a data breach response plan in place? If so, describe the steps that you will take in the event of a data breach or attach your response plan.  *See the OAIC’s* [*Notifiable data breaches*](https://www.oaic.gov.au/privacy/notifiable-data-breaches/) *page which sets out information to help APP entities prepare for and respond to data breaches. A brief overview of how you will handle a data breach needs to be outlined below.* |
| --- |
|  |

| How long will you retain the personal information collected, used and/or disclosed as part of this project?  *Describe any relevant retention and disposal policies and procedures.* |
| --- |
|  |

### APP 12 — Access to personal information

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

| How can individuals request access to their personal information? How will individuals be made aware of how to access their personal information?  *Describe how individuals can request access, and who is responsible for handling such requests. If engaging third parties such as contracted service providers, consider whether there are arrangements in place to allow access to personal information held by third parties.* |
| --- |
|  |

| Are processes in place for responding to requests from individuals to access their personal information? |
| --- |
|  |

## Part 3: 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. The following table is a standard risk assessment template. Identify three risks from your above analysis and complete a risk assessment table outlining your organisation’s response.

You may delete the table below and insert your own risk assessment table.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| # | Description of the risk | Impact / Consequence rating | Likelihood rating | Risk rating | Accept risk (Y/N) | Risk management strategy | Residual impact / consequence rating | Residual likelihood rating | Residual risk rating | Risk owner |
| 1 | ‘The risk of... event … caused by … how … resulting in … impact(s) …’ | Rate the impact of the risk to your organisation. | Determine the likelihood of the risk occurring. | Assign an overall risk rating. | Identify whether your organisation will accept the risk or not. | Detail the measures taken (or to be taken) to mitigate and manage the risk. Where relevant, include the timeframe for implementing the strategy and identify who is responsible for it. | Rate the impact of the risk to your organisation after security measures have been applied. | Rate the likelihood of the risk occurring after security measures have been applied. | Assign an overall risk rating after security measures have been applied. | Assign a risk owner who will be responsible for monitoring and reviewing the risk. |
| # | Insert additional rows as required |  |  |  |  |  |  |  |  |  |

### Summary of risks and recommendations

[Delete the text below and add your summary of findings.]

This section should summarise the findings arising from the PIA process, including:

* Outcome of the 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 the privacy risks identified