Australian Government — Office of the Australian Information Commissioner

Privacy Impact Assessment Tool

May 2020

[Privacy Impact Assessment Tool 2](#_Toc39068908)

[Part 1: Plan the PIA 3](#_Toc39068909)

[Description of the project and parties 3](#_Toc39068910)

[Scope of this privacy impact assessment 3](#_Toc39068911)

[Stakeholder identification and consultation 4](#_Toc39068912)

[Map information flows 4](#_Toc39068913)

[Part 2: Privacy impact analysis and compliance check 5](#_Toc39068914)

[Privacy impact analysis 5](#_Toc39068915)

[Ensuring compliance 5](#_Toc39068916)

[APP 1 — Open and transparent management of personal information 7](#_Toc39068917)

[APP 2 — Anonymity and pseudonymity 8](#_Toc39068918)

[APP 3 — Collection of solicited personal information 9](#_Toc39068919)

[APP 4 — Dealing with unsolicited personal information 11](#_Toc39068920)

[APP 5 — Notification of the collection of personal information 11](#_Toc39068921)

[APP 6 — Use or disclosure of personal information 12](#_Toc39068922)

[APP 7 — Direct marketing 14](#_Toc39068923)

[APP 8 — Cross-border disclosure of personal information 15](#_Toc39068924)

[APP 9 — Adoption, use or disclosure of government related identifiers 16](#_Toc39068925)

[APP 10 — Quality of personal information 16](#_Toc39068926)

[APP 11 — Security of personal information 17](#_Toc39068927)

[APP 12 — Access to personal information 21](#_Toc39068928)

[APP 13 — Correction of personal information 22](#_Toc39068929)

[Other considerations 23](#_Toc39068930)

[Part 3: Privacy management — addressing risks 24](#_Toc39068931)

[Summary of risks and recommendations 25](#_Toc39068932)

[Part 4: Respond and review 26](#_Toc39068933)

[Respond to recommendations 26](#_Toc39068934)

[Sign-off 26](#_Toc39068935)

[Update PIA if required 27](#_Toc39068936)

[Further information 27](#_Toc39068937)

[Other OAIC resources 27](#_Toc39068938)

[Other resources 27](#_Toc39068939)

[Disclaimer 27](#_Toc39068940)

## 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 Office of the Australian Information Commissioner (OAIC) has developed this tool to assist Australian Privacy Principle (APP) entities conduct a PIA, report its findings and respond to recommendations. Entities are encouraged to take a flexible approach and adapt this tool to suit the size, complexity and risk level of their project. The term ‘project’ covers the full range of activities and initiatives that may have privacy implications.

This tool should be used in conjunction with the OAIC’s [*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 entity |  |
| Date |  |
| PIA version number |  |
| PIA Drafter | Name:  Email: |
| Project Manager | Name:  Email: |
| Has the Privacy Officer of your entity been consulted in the drafting of this PIA? |  |
| Privacy Officer | 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
* 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 (for example, are you changing or expanding an existing program or project?)
* 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 later in the PIA).
* other parties (e.g. contracted service providers) and their roles, including the types of information they will be collecting and how they will use or disclose that information.

### Scope of this privacy impact assessment

[Delete the text below and add your description of the PIA scope]

The project’s scale and scope will determine how detailed the PIA process needs to be. For example, if your project will only involve minor changes or adjustments to an existing project or process, your PIA may end up only being a couple of pages long. On the other hand, if your project will result in significant changes to your business-as-usual practices, including changes to the way personal information is handled, then the PIA may need to consider a broader range of issues. As outlined above, there is no single way of doing a PIA and entities are encouraged to adapt this tool to suit the nature of their project.

When describing the project’s privacy scope, you will need to look at its key attributes, including:

* the quantity and type of personal information handled (consider whether your objectives can be met without collecting some, or all, of the personal information elements proposed for the project)
* whether sensitive information 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
* whether other PIA’s and/or risk assessments relevant to the project can be leveraged, or updated, to consider privacy risks associated with your current proposal.

### Stakeholder identification and consultation

[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 are, or might be, interested in or affected by the project being considered
* an outline of any internal and external stakeholder consultation that will be, or has already been, undertaken in relation to the project
* where relevant, a summary of the outcomes of any consultation
* where relevant, the reasons why stakeholders, or certain stakeholders, were not consulted
* whether the PIA development process can be used as part of a consultation strategy
* whether the PIA or a summary of the PIA can be published.

### 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 diagram or table that shows the flow of information involved in the project can be inserted in this section or attached as an appendix.

## 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, including:

* the risk of privacy impacts on individuals (both serious and more minor) as a result of how personal information is handled. Consider any known vulnerabilities that may arise in relation to individuals that will be involved or impacted by your project (for example, will your project have implications for children or other potentially vulnerable cohorts like people with a disability?)
* 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 ability to control their personal information and choices about who has access to it
* compliance with privacy law
* how the use of personal information in the project aligns with community expectations and values about privacy.

A PIA doesn’t set out to identify and eliminate every possible privacy risk, however, it should identify any genuine risks that may be associated with your project, assess how serious those risks are, and consider ways that those risks can be mitigated. Undertaking a PIA should help you to identify and focus on the most serious and the most likely problems.

### Ensuring compliance

[Depending on the scope and complexity of your project, it may not be necessary for you to consider every APP. Delete the text below and the sections of the table that are not relevant to your project. The explanatory text in italics that accompanies some of the questions below should also be deleted]

The table in this section is designed to help you assess whether your project complies with each of the APPs. Some guidance questions are provided below and you should document and provide specific details about either how your project complies with the APP or why you are not required to comply with an APP, and any considerations you took into account.

These questions are not exhaustive and are provided as a guide only. You should think about potential privacy risks even when not explicitly prompted in the table and note any identified risks in Part 3 of this tool. You should also refer to the APP Guidelines, which provide a comprehensive guide to interpreting and applying the APPs.

You may need to consider other issues, including other legislation and rules that apply to your entity (such as secrecy provisions), considering the nature of your project. 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.

As you go through your compliance check, you should consider the privacy risks and, where possible, come up with alternatives to avoid or mitigate those risks. This will help to inform any recommendations you make to address the risks that have been identified in the PIA process.

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

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

|  |
| --- |
| Have reasonable steps been taken to implement practices, procedures and systems that will ensure compliance with the APPs and any binding registered APP code for the purposes of the project?  *See the OAIC’s* [*Privacy Management Framework*](https://www.oaic.gov.au/privacy/guidance-and-advice/privacy-management-framework-enabling-compliance-and-encouraging-good-practice/) *for the steps the OAIC expects you to take to meet your obligations under APP 1.2. Agencies should also consider their obligations under the Privacy (Australian Government Agencies – Governance) APP Code 2017. Consider whether any adjustments or additions need to be made to your practices, procedures and systems for the purposes of this project.* |
|  |

|  |
| --- |
| Do you have an APP privacy policy which:   * is clearly expressed, understandable and up-to-date * covers the matters listed in APP 1.4 * is freely available at no cost (for example, on your website).   *Identify the document(s) and provide a link where available or include as an attachment to this PIA. See the OAIC’s* [*Guide to developing an APP privacy policy*](https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-developing-an-app-privacy-policy/) *for more information.* |
|  |

|  |
| --- |
| Will the APP privacy policy need to be updated to reflect a new collection, use or disclosure of personal information for the purposes of this project?  *Your analysis under APP 3 and APP 6 should inform whether updates to your entity’s APP privacy policy are required (see 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.* |
|  |

|  |
| --- |
| Are you required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves?  *Identify the law that requires or authorises you to deal with identified individuals.* |
|  |

| Are there categories of individuals affected by the project who are likely to seek to interact with your entity anonymously or using a pseudonym?  *For example, an individual may prefer to deal anonymously or pseudonymously with you for various reasons including to access services (such as counselling or health services) without this becoming known to others, or to keep their whereabouts secret from a former partner or family member.* |
| --- |
|  |

### 

### 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.

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.

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 agency, is the information being collected necessary for, or directly related to, one or more of your functions or activities?  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 (eg. name, date of birth, address) and explain why each item is necessary for one or more of your functions or activities. This should be a very granular assessment. You should clearly and specifically describe the relevant function or activity and why each item of personal information is reasonably necessary for (or, for agencies, directly related to) that specific function or activity. 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, which could also trigger your notification obligations under the Notifiable Data Breach scheme. Holding large amounts of personal information may also increase the risk of unauthorised access by internal or external sources. Security issues are considered further below under APP 11.*  *Also consider whether your APP privacy policy will need to be updated if the project will involve a new collection of personal information and record this under APP 1 above.*  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 be 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. |
| --- |
|  |

| For the collection of sensitive information, can you rely on any of the exceptions in APP 3.3 or APP 3.4?  *Explain which exception you are relying on for the collection of any 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 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 from the individual concerned? If not, do any of the exceptions in APP 3.6 apply?  *Describe how, and from which other sources, the personal information will be collected. Also, explain which exception you are relying on to collect personal information about the individual from another source.*  Warning icon: **Privacy risk**: There may be a risk of the information being inaccurate, out-of-date or incomplete if collected from another source. |
| --- |
|  |

| If the collection of personal information will be outsourced, will measures be in place to ensure compliance with APP 3and prevent over collection of information?  *Describe how you will ensure that any third party that collects personal information on your behalf complies with APP 3 (for example, by entering an enforceable contractual arrangement).* |
| --- |
|  |

### 

### 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 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.

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.

| 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 not to notify the individual?  *Describe the steps taken to notify the individual OR explain why steps are not being taken. Include a link or attach collection notices where appropriate.* |
| --- |
|  |

| If personal information is collected from another source, will the individual be notified? What steps will be taken to notify of each of the APP 5.2 matters?  *Describe the steps taken to notify the individual OR explain why steps are not being taken. Include a link or attach collection notices where appropriate.*  Warning icon: **Privacy risk**: If you are collecting personal information from another source, there may be a risk that an individual is not aware that you have collected their personal information. Ensure that any third-party notifies, or makes an individual aware, of the relevant APP 5 matters on your behalf (such as through an enforceable contractual arrangement). |
| --- |
|  |

### 

### 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).

| Does the project use or disclose personal information (including sensitive information) for a secondary or additional purpose?  *Describe the secondary purpose and explain how it is authorised, by either asking the individual to consent, or by applying one of the exceptions to the requirement for consent in APP 6.2. Also consider whether your APP privacy policy will need to be updated if the project will involve a new use or disclosure of personal information and record this above under APP 1.* |
| --- |
|  |

| 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? |
| --- |
|  |

| Will the individual be notified of any additional use(s) or disclosure of their personal information?  *Explain how the individual will be given notice of the secondary use(s) or disclosure of their information, or why notice is not required (eg. additional notice may not be required if the proposed use or disclosure is consistent with the notice originally provided at the point of collection).*  Warning icon: **Privacy risk**: If relying on APP 6.2(a) to use or disclose personal information for a secondary purpose, but your project involves a new way of handling personal information, there may be a risk that individuals would not reasonably expect their personal information to be used for the new purpose. Carefully consider whether additional notification is required. |
| --- |
|  |

| If you’re disclosing personal information to another entity (eg. if you are outsourcing some of your functions, or as part of an ongoing data sharing arrangement), will measures be put in place to protect the information and will compliance with APP 6 be monitored?  *Describe the measures (such as an enforceable contractual arrangement or other information sharing agreement) that will be put in place to ensure compliance with APP 6 and protect the personal information that is being disclosed/shared. If no measures will be put in place, explain why (for example, the disclosure is a once-off and permitted by one of the exceptions under APP 6).* |
| --- |
|  |

### 

### 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. APP 7 may also apply to an agency in the circumstances set out in s 7A of the Privacy Act.

| 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 7 does not apply to the extent that the Do Not Call Register Act 2006 and the Spam Act 2003 apply. APP 7 will still apply to the acts or practices of an organisation that are exempt from these Acts.* |
| --- |
|  |

### 

### 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).

| Will any personal information be disclosed to an overseas recipient?  *Describe what information will be transferred, to whom the information will be transferred, in which jurisdiction the information will be stored, and how the information will be transferred.* |
| --- |
|  |

| Will reasonable steps be taken under APP 8.1 to ensure the overseas recipient does not breach the APPs (other than APP 1) in relation to the information?  *Explain the arrangements in place with overseas recipients to ensure that personal information is handled in accordance with the APPs. For example, provide details of any enforceable contractual arrangement.* |
| --- |
|  |

| Alternatively, does an exception under APP 8.2 apply?  *Explain how one of the exceptions in APP 8.2 apply to the transfer. For example, is the disclosure required or authorised by or under an Australian law or a court/tribunal order?* |
| --- |
|  |

### 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.

APP 9 does not apply to the handling of government related identifiers by agencies. However, agencies should still give careful consideration to any proposed creation, adoption, use or disclosure of government related identifiers and the potential privacy impacts this may have, including community expectations around how government should handle these identifiers.

| If you are an organisation, is any planned adoption, use or disclosure of government related identifiers permitted under an exception in APP 9?  *Describe the identifier, the purpose for adopting, using or disclosing it and how this is authorised. 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.

| 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 to ensure these steps are followed? |
| --- |
|  |

| What steps will 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?  Warning icon: **Privacy risk**: Carefully consider 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 or disclosing inaccurate information. |
| --- |
|  |

### 

### 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.

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.* |
| --- |
|  |

| Are there access security and monitoring controls in place to protect against internal and external risks and ensure that personal information is only accessed by authorised persons?  *Describe the access security controls (such as identity management and authentication, password practices, audit logs/trails and access monitoring) that have been, or will be, implemented for the project, including any policies and procedures. Consider who will have access to the data and ensure access is limited to those staff (or other third parties) necessary to enable your entity to carry out its functions and activities (ie. access should be strictly on a ‘need-to-know’ basis). Include links or attachments where appropriate.*  Warning icon: **Privacy risk**: Inadequate access security and monitoring controls may lead to the ‘trusted insider risk’, which can occur when staff mishandle personal information while carrying out their normal duties. |
| --- |
|  |

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

| Have you considered standards that may apply to your industry or sector? If you have decided not to adopt a widely used standard, document your reasons below.  *You should consider using relevant international and Australian standards, policies, frameworks and guidance on information security. This includes any which are particular to your sector or industry. Australian Government agencies must apply the Attorney-General’s Department’s*[*Protective Security Policy Framework*](https://www.protectivesecurity.gov.au/Pages/default.aspx)*and the Australian Signals Directorate’s*[*Australian Government Information Security Manual*](http://www.asd.gov.au/infosec/ism/index.htm)*.*  *You may also want to consult the*[*ISO/IEC 27000 series of information security management standards*](http://www.iso.org/iso/home/standards/management-standards/iso27001.htm)*and the*[*ISO/IEC 31000 series of risk management standards*](https://www.iso.org/iso-31000-risk-management.html)*published by both*[*the International Organization for Standardization*](http://www.iso.org/iso/home.htm)*and the*[*International Electrotechnical Commission*](http://www.iec.ch/)*, parts of which have been adopted by Standards Australia.* |
| --- |
|  |

| If you have outsourced personal information handling as part of this project, what steps will be taken to ensure personal information is protected by third party providers?  *Describe the measures (such as conducting due diligence on the services to be provided and contractual provisions relating to security requirements) that will be taken to ensure third party providers protect any personal information handled on your behalf.*  Warning icon: **Privacy risk**: Failing to conduct appropriate due diligence on the services to be provided is inconsistent with your obligations under APP 11 and can lead to an increased risk of a data breach if the third-party provider does not have adequate security measures in place. |
| --- |
|  |

| Do you have a data breach response plan in place? If so, describe at a high level 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. You should consider whether changes to your existing data breach response plan need to be made as a result of this project.* |
| --- |
|  |

| If you have outsourced personal information handling as part of this project, have you considered your obligations under the Notifiable Data Breaches (NDB) scheme and how you will manage your relationship with the third party?  *Describe how you will ensure you comply with the NDB scheme in the event a third-party provider experiences a data breach (such as including contractual terms to allocate responsibility for identifying, assessing and notifying as required).* |
| --- |
|  |

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

| Will personal information be destroyed or de-identified once it 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)?  *Explain whether an exception applies that requires you to retain the information.* |
| --- |
|  |

| If applicable, how will personal information be destroyed once it is no longer required?  *Describe the method of destruction and explain how that method is secure.*  Warning icon: **Privacy risk**: There is a risk of unauthorised disclosure if personal information is not securely and irretrievably destroyed. |
| --- |
|  |

| If applicable, how will personal information be de-identified once it is no longer required?  *Describe the method of de-identification that will be used and whether the de-identified information will be used for any other purpose. See the OAIC’s* [*De-identification and the Privacy Act*](https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/) *for further information.*  Warning icon: **Privacy risk**: If de-identifying personal information once it is no longer required, consider whether there is a risk that the information can be re-identified. |
| --- |
|  |

| If you have outsourced personal information handling as part of this project, what will happen to information held by third party providers?  *Describe any arrangements (for example, any contractual provisions) in relation to third parties’ obligations to retain and dispose of personal information.*  Warning icon: **Privacy risk**: If there are no arrangements in place relating to third parties’ retention and disposal of personal information, there is a risk that personal information could be used by the third party for unauthorised purposes at the conclusion of the contract. |
| --- |
|  |

### 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.

| 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? |
| --- |
|  |

### 

### 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. The requirement to take reasonable steps applies in two circumstances: where an APP entity is satisfied that personal information it holds is incorrect, or at the request an individual to whom the personal information relates. There are minimum procedural requirements in relation to correcting personal information.

| How can individuals seek correction of their personal information? How will individuals be made aware of how to correct their personal information?  *Describe how individuals can seek correction of their personal information and how they will be made aware of this. If engaging third parties such as contracted service providers, consider whether there are arrangements in place to allow correction of personal information held by third parties.* |
| --- |
|  |

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

| Are there process in place for associating a statement with personal information if a request for correction is denied? |
| --- |
|  |

| Are processes in place for identifying and correcting personal information that is inaccurate, out of date, incomplete, irrelevant or misleading?  *Describe the steps that will be taken, or the measures that are in place, to ensure the ongoing integrity of the information.* |
| --- |
|  |

### 

### Other considerations

| Will any training be provided to staff to ensure the appropriate collection, handling and security of the personal information as part of this project?  *Describe the type of training staff will receive.* |
| --- |
|  |

| Does the project comply with your entity’s other information handling or information management policies? |
| --- |
|  |

| 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? |
| --- |
|  |

| Will this PIA be published? |
| --- |
|  |

| Are there any other broader privacy considerations associated with this project?  *You might find it useful to show how the project will deal with other kinds of personal privacy not covered by the Privacy Act, such as bodily, behavioural and territorial privacy.*  *If you are an agency developing legislation or a new policy proposal with privacy impacts, consider whether any limitation on the right to privacy is reasonable, necessary and proportionate to your objective. For example, if you are developing legislation that seeks to rely on the required or authorised exception to the APPs (such as legislation authorising the use or disclosure of personal information), consider whether the proposed legislation is reasonable, necessary and proportionate to your objective. This may assist with the development of Human Rights Compatibility Statements for legislative projects.* |
| --- |
|  |

## Part 3: Privacy management — addressing risks

Through the privacy impact analysis and compliance check in Part 2, you may have identified risks to privacy in the project’s current design. The following table is a standard risk assessment template.

**The OAIC recommends that you use your entity’s own risk assessment framework where possible**. 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
* 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.

## Part 4: 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 PIA report.

### Respond to recommendations

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Action | Action Owner | Timeframe | Date Action completed |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Sign-off

A PIA does not necessarily require formal sign-off, but your entity may require it, or you may consider it is necessary in the circumstances, particularly if the PIA recommends significant changes to the nature of a project, or if it recommends accepting significant risks.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Position | Signature | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Update 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.

## Further information

### Other OAIC resources

[Guide to undertaking privacy impact assessments](https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/)

[PIA e-Learning course](https://www.oaic.gov.au/privacy/training-resources/e-learning-undertaking-a-privacy-impact-assessment/)

[Guide to securing personal information](https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/)

[Data breach preparation and response guide](https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/)

Agencies should also consider the [FOI Guidelines](https://www.oaic.gov.au/freedom-of-information/foi-guidelines/) and [Processing requests for amendment of annotation of personal records](https://www.oaic.gov.au/freedom-of-information/guidance-and-advice/processing-requests-for-amendment-of-annotation-of-personal-records/)

### Other resources

Keep up to date with the latest advice from the [Australian Cyber Security Centre](https://www.cyber.gov.au/).

Agencies should ensure continued compliance with the [Protective Security Policy Framework](https://www.protectivesecurity.gov.au/) and information management requirements from the [National Archives of Australia](https://www.naa.gov.au/information-management).

### Disclaimer

The information in this document is general in nature and does not constitute legal advice.