When do agencies need to conduct a privacy impact assessment?

## Overview

The [*Privacy (Australian Government Agencies – Governance) APP Code 2017*](https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/australian-government-agencies-privacy-code/) (the Code) requires Australian Government agencies subject to the *Privacy Act 1988* (Privacy Act) to conduct a privacy impact assessment (PIA) for all ‘high privacy risk projects’.[[1]](#footnote-1)

This resource:

* provides guidance on how you can screen for high privacy risk projects by completing a threshold assessment to determine whether a PIA is required
* sets out the benefits of conducting a PIA, even when a project does not meet the ‘high privacy risk’ threshold, and
* includes a template to assist you complete a threshold assessment.

This resource should be read in conjunction with the OAIC’s [*Guide to undertaking a privacy impact assessment*](https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/) (PIA Guide) and [PIA e-learning course](https://www.oaic.gov.au/s/elearning/pia/welcome.html). The OAIC has also developed an adaptable PIA tool, which has been designed to guide you through the PIA process, report its findings and respond to recommendations.

### What is a privacy impact assessment?

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

PIAs can help ensure compliance, facilitate a privacy-by-design approach and identify better practice. PIAs demonstrate a commitment to accountable and transparent privacy practices and build public trust and confidence in an agency’s programs and policies. The Code recognises this value by requiring agencies to conduct a PIA for all high privacy risk projects. More information about the benefits of undertaking a PIA is provided below.

Importantly, not all PIAs need to be long or complex. Instead, the approach taken in a PIA should be proportionate to the level of risk. A PIA is intended to be a flexible and scalable tool, which can be adapted based on the size, complexity and risk level of your project.

### What is a threshold assessment?

A threshold assessment is a preliminary assessment to help you determine your project’s potential privacy impacts and give you a sense of the risk level, including whether it could be a ‘high privacy risk project’ requiring a PIA under the Code.

You should undertake a threshold assessment if your project involves new or changed ways of handling personal information.

A threshold assessment is not intended to establish the actual level of risk – that is the job of the PIA to assess in more detail. Instead, the purpose is to screen for factors that point to the potential for a high privacy risk, which will require a PIA to be conducted under the Code.

Not every project will need a PIA. A threshold assessment will quickly and easily identify projects with no, or minimal, information privacy implications.

Regardless of whether you proceed to a PIA, you should keep a record of the threshold assessment. The template below can help with this. The Code does not require you to publish a record of threshold assessments but there are benefits in doing so, including promoting public trust and confidence that you have considered privacy issues during the development of your project.

## How to use the threshold assessment template

The template is designed to help you:

1. identify whether your project involves new or changed ways of handling personal information, and
2. screen for factors that may point to the potential for a high privacy risk project.

If your project has the potential of being high privacy risk, you will need to complete a PIA to consider the risk in more detail (including the likelihood and severity of potential risk). Further information is provided below on each part of the template.

### Part 1: Does the project or initiative involve new or changed ways of handling personal information?

Part 1 of the template requires you to determine and record whether a project involves new or changed ways of handling personal information. This question requires a thorough understanding of all aspects of a project.

#### What is a ‘project’?

The term ‘project’ covers the full range of activities and initiatives undertaken by agencies that may have privacy implications. This could include:

* new policy proposals
* new or amended legislation or delegated legislation
* new or changed programs or activities
* implementing IT systems or databases or increasing the number of users of those systems
* new or changed methods or procedures for service delivery or information handling
* implementing artificial intelligence technologies, including automated decision-making processes
* restructures or changes to business-as-usual activities.

#### What is ‘personal information’?

‘Personal information’ is information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable (s 6(1) of the Privacy Act). The term ‘personal information’ encompasses a broad range of information held by your agency that could identify an individual, including employee information.

You can use the checklist in the OAIC’s [*What is personal information?*](https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/) resource to assess whether this definition applies to the information you plan to handle in a project.

#### What is a ‘new or changed way of handling personal information’?

This should be interpreted broadly and in accordance with its natural meaning.

‘Handling’ refers to how your agency manages personal information throughout all stages of the information lifecycle, and includes collection, use, disclosure, storage, destruction and de-identification.

You will need to be certain that any information handling in the project is similar to an existing practice in terms of nature, scope, context, purpose and risk before deciding that your project does not involve a new or changed way of handling personal information.

If your project involves a new or changed way of collecting, using, disclosing, storing, destroying or de-identifying personal information, you will need to consider whether your project has the potential to be a high privacy risk project (see below).

#### What next?

If your project does involve new or changed ways of handling personal information, select ‘yes’ and complete part 2 of the template.

If your project does not involve new or changed ways of handling personal information, select ‘no’ and include a description of why a PIA is not necessary.

As a matter of best practice, you could include a description of whether the privacy implications associated with the project have previously been assessed and are being managed. For example, where a project is not new, the privacy risks may have already been considered as part of a threshold assessment, a PIA or other risk-assessment process and the privacy controls are current and working well.

### Part 2: Determining whether there is the potential for a high privacy risk

Part 2 of the template will help you to screen for factors that point to the potential for a high privacy risk project.

#### What is a ‘high privacy risk project’?

The Code provides that a project may be a high privacy risk project if an agency reasonably considers that the project involves any new or changed ways of handling personal information that are ‘likely to have a significant impact on the privacy of individuals’.

You need to screen for privacy risks even where there is legal authority for the new or changed way of handling personal information. This could include projects that engage an exception to the Australian Privacy Principles (APPs) or other laws (including codes and regulations). Even if a project is compliant with the relevant legislation, individuals whose information you are handling may still be adversely impacted. Similarly, you will also need to screen for privacy risks if you are developing new legislation to modify the operation of one or more APPs or which seeks to rely on the required or authorised by law exception to the APPs.

#### What is a ‘significant impact’?

A privacy impact in this context is anything that could adversely affect individuals’ information privacy. Impacts include intrusions, such as the collection of new or additional types of personal information, or when the handling of personal information results in an individual losing control over their personal information.

An impact on the privacy of individuals will be ‘significant’ if the consequences of the impact are considerable, taking into account their nature and severity.

The consequences of a privacy impact could be significant for one individual or a group of individuals, for example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft. The consequences of the potential privacy impacts for a group of individuals may vary based on their individual circumstances, so you should consider whether some individuals may be more significantly impacted than others.

Sometimes projects can have a significant collective impact on society, rather than impacting on people individually. These collective impacts are likely to lead to broad public concern, for example, increased surveillance and monitoring activities, or the establishment of sensitive information sharing arrangements between the Commonwealth and other entities.

There is no definitive threshold to determine when an impact is ‘significant’ given each project will differ in nature, scope, context and purpose. Accordingly, agencies are advised to screen for factors that may raise a project’s risk profile. The table in part 2 of the template is designed to assist with this.

#### Screening for factors that point to a high privacy risk

As mentioned above, a threshold assessment is not intended to establish that a project (or any feature of it) is actually ‘high privacy risk’ – that is the job of the PIA to assess in detail. Instead, a threshold assessment will screen for factors that point to the potential for a high privacy risk, rather than conducting a comprehensive risk and impact analysis.

Part 2 of the template includes a non-exhaustive list of general and activity-based risk factors which may point to the potential for a high privacy risk project. The template asks you to consider whether your project will involve:

* handling large amounts of personal information
* handling sensitive information
* sensitivities of the context in which the project will operate
* handling personal information of individuals who are known to be vulnerable
* handling personal information in a way that could have a serious consequence for an individual or a group of individuals
* activities of a long or permanent duration
* the following activity-based risk factors:
* using or disclosing personal information for secondary purposes
* disclosing personal information outside your agency
* using or disclosing personal information for profiling or behavioural predictions
* using personal information for automated decision-making
* systematic monitoring or tracking of individuals
* collecting personal information without notification to, or consent of, the individual
* data matching (linking unconnected personal information)
* developing legislation to modify the operation of one or more APPs or which seeks to rely on the required or authorised by law exception to the APPs.

You should consider these factors, or any other relevant factors not listed in the template, in the context of your particular project. These factors do not always mean that a project is high risk or that the risk cannot be mitigated, just that there is the potential that the project may be high risk and so a PIA is required to assess the level of risk in more detail.

Whether your project has the potential to be a high privacy risk project is a contextual assessment based on the circumstances. It is the responsibility of each agency to be able to justify why a new or changed way of handling personal information does not have the potential to be high privacy risk.

Taking these factors and contextual elements into account, if you do consider that there is the potential that your project is a high privacy risk project, you must undertake a PIA.

It is important to note that this does not mean that your project cannot proceed. Rather, a PIA will ensure that privacy risks and impacts that may be associated with your project are identified and mitigated.

A PIA will also help you consider whether any limitation on the right to privacy is reasonable, necessary and proportionate to your objective. This may assist with the development of Human Rights Compatibility Statements for legislative projects.

#### What next?

If you answer ‘yes’ or ‘potentially’ to any of the questions in part 2 of the template, there is the potential that your project is a high privacy risk project and a PIA must be completed.

If you are uncertain whether there is the potential for a high privacy risk, you should consult your agency’s privacy officer and other relevant stakeholders where necessary. If you are still unsure, you should err on the side of caution and conduct a PIA.

If you do not consider that your project has the potential to be a high privacy risk project, you should record your decision in the template and store the template where it can be referred to in the future.

The OAIC strongly encourages agencies to conduct PIAs as a matter of course for projects that involve any new or changed ways of handling personal information, regardless of their potential risk profile.

## Benefits of conducting a PIA

PIAs are more than just a compliance exercise. Privacy issues that are not properly addressed can impact on the community’s trust in an agency and undermine the project’s success. The process of undertaking a PIA is a good way to assess privacy risks more broadly, and a way to demonstrate your agency’s commitment to, and respect of, individuals’ privacy. There may be many circumstances where a PIA would not be required under the Code, but an agency would still decide to undertake a PIA as a matter of best practice for these additional benefits.

The risk of not undertaking a PIA include:

* non-compliance with the privacy laws, potentially leading to a privacy breach and/or negative publicity
* loss of credibility through lack of transparency in response to public concern about handling personal information
* damage to an agency’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.

The 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 agency
* contributing to broader agency risk management processes
* building community awareness and acceptance of the project through public consultation and publication of the PIA (where appropriate).

As mentioned above, not all PIAs need to be long or complex. Instead, the approach taken in a PIA should be proportionate to the level of risk. PIAs can be incorporated into your agency’s business as usual activities – they often fit into existing assurance, risk management and policy development processes. Integrating PIAs into your agency’s standard processes may help you to avoid duplication or unnecessary work by leveraging, or updating, existing processes to help consider privacy risks associated with future projects.

## Threshold assessment template

You are encouraged to take a flexible approach and adapt this template to suit your agency’s particular circumstances. For example, you may wish to add additional factors to the table in part 2 that point to the potential for your project to be a high privacy risk project based on your agency’s functions and activities.

### Project Details

|  |  |
| --- | --- |
| Project name |  |
| Name of agency |  |
| Date |  |
| Project manager |  |
| Threshold assessment drafter |  |
| Description of the project | *Include a brief description of the project including whether it is a new or existing project. If it is an existing project, describe the proposed changes to the project.* |
| Set out a brief description of the types of personal information being handled as part of the project | *Brief description of the personal information that will be handled (including personal information that will be collected, used or disclosed, stored, destroyed, de-identified).* |
| What is the purpose of the personal information handling/legal authority? | *Describe the function or activity of the agency that this project is directly related to or is reasonably necessary for. What is the legal authority (if any) for the proposed information handling activity?* |
| Stakeholders | *List the internal and external stakeholders who have an interest in, or will be affected by, the project. It may be necessary to consult with other areas within your agency, partner agencies or other organisations. You may also approach your agency’s Privacy Officer for assistance with completing a threshold assessment or to discuss the project’s approach to personal information handling.* |

### Part 1: Does the project or initiative involve new or changed ways of handling personal information?

|  |  |  |  |
| --- | --- | --- | --- |
|  | No | It is not necessary to complete a PIA. Record the decision and file this assessment with your Privacy Officer.   |  | | --- | | *Outline why it is not necessary to complete a PIA. If the project is not new, you could include a description of how privacy risks have previously been assessed and are being managed*. | |
|  | Yes | Complete Part 2 of the assessment below. |

### Part 2: Determining whether there is the potential for a high privacy risk

Consider the following questions and record each answer as ‘yes’, ‘no’ or ‘potentially’. The purpose of these questions is to you help you screen for factors which point to the potential for a high privacy risk project. It’s important to note that these questions are non-exhaustive, and you should also consider whether there are any other relevant factors that may indicate that your project is a high privacy risk project.

| Will the project involve: | Yes | No | Potentially |
| --- | --- | --- | --- |
| **Handling large amounts of personal information?**  *Consider the amount of personal information and the number of individuals that will be impacted by your project.* *Even if you consider that each individual will only have a small chance of suffering a negative impact, handling personal information on a large scale can increase the privacy risk associated with your project. You should also consider whether your project will result in significant increases in the volume of personal information being handled through new or existing channels.* |  |  |  |
| **Handling sensitive information?**  *Sensitive information includes, but is not limited to, information about an individual’s racial or ethnic origin, political opinions, religious beliefs or affiliations, criminal records, sexual preferences or practices, biometric information, health information and genetic information.*  *The privacy risk associated with your project can increase if sensitive information is involved given the potential for adverse consequences for an individual, or those associated with the individual, if it is mishandled (for example, discrimination, mistreatment, humiliation or embarrassment).* |  |  |  |
| **Sensitivities based on the context in which the project will operate?**  *Consider the context and circumstances surrounding the project. Are there prior concerns over this type of handling or activity? Is the project likely to have community support? Is the handling of personal information novel in any way? What is the current state of technology in this area and has there been any previously identified security or technology flaws? Are there any current issues of public concern that you should factor in? What is the nature of your relationship with individuals that may be impacted by the project? How much control will they have over the handling of their personal information? Would they expect you to use their personal information in this way?* |  |  |  |
| **Handling personal information of individuals who are known to be vulnerable?**  *Consider whether the activity may have greater sensitivities or disproportionate impacts on vulnerable populations and certain groups of individuals. This could include children and seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.*  *An individual’s circumstances, or the increased power imbalance between the individual and an agency, may mean, for example, they are unable to easily consent to, or oppose, the handling of their personal information, understand its implications, or exercise control over their personal information.* |  |  |  |
| **Handling personal information in a way that could have a significant impact on the individuals concerned?**  *Consider the potential consequences for the individuals concerned. For example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft.* |  |  |  |

#### Activity-based risk factors

| Will the project involve: | Yes | No | Potentially |
| --- | --- | --- | --- |
| **Disclosing personal information outside of your agency?**  *Consider whether your project will involve sharing personal information with another agency, organisation or to any individuals other than the individual to whom the information relates. This might include the use of contractors or sub-contractors. Also consider whether your project will require the disclosure of personal information overseas.* |  |  |  |
| **Using or disclosing personal information for profiling or behavioural predictions?**  *This includes valuation or scoring, profiling and predicting (including in relation to economic situation, health, personal preferences or interests, reliability or behaviour, location or movements).* |  |  |  |
| **Using personal information for automated decision-making?**  *This might include the use of artificial intelligence technologies or data analytics techniques on personal information to produce insights for policy-making or improved service delivery. It might also include using automated decision-making to make decisions that affect the rights, entitlements and opportunities of an individual.* |  |  |  |
| **Systematic monitoring or tracking of individuals?**  *For example, the introduction or enhancement of a surveillance system, the monitoring of communications, tracking an individual’s geolocation or behaviour.* |  |  |  |
| **Collecting personal information without notification to, or consent of, the individual?**  *This might include collecting personal information about an individual from a third party without the individual’s knowledge or consent. It might also include collecting personal information compulsorily under an existing, or proposed, legislative authority.* |  |  |  |
| **Data matching (linking unconnected personal information)?**  *For example, a new data matching program combining, comparing or matching personal information obtained from multiple sources.* |  |  |  |
| **Developing legislation to modify the operation of one or more APPs or which seeks to rely on the required or authorised by law exception to the APPs?**  *This might include legislation or delegated legislation that seeks to modify the operation of one or more APPs in certain circumstances. It might also include legislation that seeks to rely on the required or authorised an exception to the APPs (such as legislation authorising the use or disclosure of personal information).* |  |  |  |

### Decision & declaration

If you have answered ‘Yes’ or ‘Potentially’ to any of the questions in part two, a PIA should be completed. If you are uncertain as to whether you have considered all relevant risks, you are strongly encouraged to seek support from your agency’s privacy officer to ensure your assessment is thorough and complete. If still unsure, err on the side of caution and conduct a PIA.

Based on your answers above, is a PIA required?

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Yes | | Yes, there are (or potentially are) high privacy risk elements to this project. | | |
|  | No | | No, a PIA is not necessary. This project does not carry any high privacy risks or involve a new or changed way of handling personal information. | | |
| Assessor Sign-off | | | | | | |
| Name | |  | | Position | Date | |
|  | | | |  |  | |
| Approver Sign-off | | | | | | |
| Name | |  | | Position | Date | |
|  | | | |  |  | |
| Privacy Officer Sign-off | | | | | | |
| *Privacy Officer engaged?* | | | | | Date | |
|  | | | | |  | |

1. *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Cth)s 12 [↑](#footnote-ref-1)