Office of the Victorian Information Commissioner

Privacy Impact Assessment

Accompanying guide

Freedom of Information | Privacy | Data Protection

Table of contents

Introduction

This guide has been prepared by the Office of the Victorian Information Commissioner (**OVIC**) and is designed to accompany OVIC's privacy impact assessment (**PIA**) template. The PIA guide and template are aimed at Victorian public sector (**VPS**) organisations covered by the *Privacy and Data Protection Act 2014* (**PDP Act**), however these resources may assist anyone undertaking a PIA.

The PIA template and guide are not intended as a purely compliance exercise, but are designed to help you become aware of the privacy impacts of your program of work.

What is a PIA?

A PIA is a process for analysing a program's impact on individuals' information privacy. The process of conducting a PIA can help to identify potential privacy risks and develop risk mitigation strategies to address these privacy impacts before a project or initiative commences.[1]

PIAs can be used to:

- identify whether a program is likely to impact upon the privacy of individuals;
- check whether a program is likely to comply with relevant privacy laws; and
- assist in making decisions about how to adjust a program to mitigate or manage privacy risks.

A PIA is not a one-off exercise. Rather, it should be considered as a core part of your organisation's program planning methodology, enabling your organisation to continually reassess, update, and manage the privacy risks and challenges as they evolve throughout your program's life.

Is a PIA necessary?

In general, if your program is collecting, using, or disclosing any personal information it is best practice to undertake a PIA, regardless of whether it is a new collection of personal information, or a new use of information already held by your organisation.

The simplest threshold assessment of whether or not you should conduct a PIA is: *Does this program involve the handling of personal information?*

If the answer is yes, OVIC recommends you conduct a PIA.

The nature, size, and level of complexity of each program will vary, and the PIA template has been designed to work for all kinds of programs. More complex programs – such as where many parties are involved or a large amount of personal information will be handled – may warrant a more comprehensive PIA process, resulting in a more detailed report. Simpler programs on the other hand may require a less in-depth assessment, and the process of conducting PIAs will usually be quicker.

[1] Some examples of PIAs can be found at https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments#appendix-a-acknowledgments-and-resources

It can be tempting to deem a PIA unnecessary for programs that are smaller in size, or where the privacy impact is assumed to be insignificant. In these instances, OVIC still recommends organisations go through the process of conducting a PIA. If the privacy impacts of a program are truly insignificant, then undertaking the PIA will be a quick, simple process.

In some cases, a seemingly insignificant program may not appear to have any privacy impacts upon first glance; however, the process of undertaking a PIA can reveal risks your organisation may not have otherwise considered. It is always good practice to demonstrate to those individuals whose information is being handled that you have done your due diligence and assessed the potential risks to their privacy.

No matter the size of the program, conducting a PIA can help mitigate against risks that can sometimes be overlooked when we assume that the collection or use of personal information to achieve a certain goal is uncontroversial or that the possible level of harm would be negligible.

Why do a PIA?

Although conducting a PIA is not mandatory under Victorian privacy law, all VPS organisations are required to comply with Part 3 of the PDP Act. The process of undertaking a PIA can assist your organisation in assessing a program against the 10 Information Privacy Principles (**IPPs**), contained in Schedule 1 of the PDP Act.

In instances where organisations consult with OVIC about a program, OVIC will always recommend that the organisation conducts a PIA. Undertaking a PIA before consulting with OVIC will put organisations in a better position to understand where there may be gaps in privacy compliance that need addressing, or on which matters they require further guidance from OVIC.

Assessing a program's privacy impact is not just about legal compliance. Even if a program is legally compliant it does not necessarily mean that the individuals whose information you are handling will not be adversely affected. The process of undertaking a PIA is a great way to assess privacy risks more broadly, and a way to demonstrate your organisation's commitment to, and respect of, individuals' privacy.

A PIA can promote public trust and confidence that privacy has been considered and built into the design and implementation of your program. People care about how their personal information is handled, and they are much more likely to trust and engage with organisations that have good privacy practices. Conducting a PIA can also provide an opportunity to raise awareness of privacy within your organisation, establish accountability for the program and any privacy risks that may arise, and affirm the importance of privacy to your organisation's employees.

While these are good reasons for conducting a PIA, you should also undertake PIAs for the benefit and from the perspective of the individuals whose personal information you are collecting and using. PIAs are a good way to identify and mitigate any potential harms that may come to your organisation, but importantly, the harms that may also come to individuals.

> **Top tip**
>
> Sometimes the hardest part of the PIA process is not the assessment itself, but rather convincing those working on a program that a PIA is necessary and worth the time. If this is the case, refer back to the 'Why do a PIA?' section and remind the team that there are many benefits to conducting a PIA that extend beyond legal compliance.

When should a PIA be done?

To get the most out of the PIA process, OVIC recommends organisations conduct a PIA as early as possible in the design of a program. Conducting a PIA early in the program design process can help identify risks upfront and make it easier and cheaper to address or manage them. It can often be much more time consuming and expensive to remedy privacy issues further down the track, as they may not become apparent until after a privacy breach has occurred. PIAs can also highlight opportunities where processes may benefit from being revisited to make them more effective or privacy-enhancing.

Undertaking a PIA early will help you to build privacy into your program from the beginning, rather than adding on privacy-enhancing features after the program has been implemented.

Conducting a PIA in the early design stages of a program may mean that you do not have all the information necessary to complete a thorough privacy analysis. If this is the case, you might consider conducting an initial PIA, and then updating it iteratively as more information becomes available.

It may be the case that an existing program was implemented without first having gone through the process of conducting a PIA. In such instances, OVIC recommends that organisations conduct a retrospective PIA to analyse the privacy impacts of the program and highlight any practices that would benefit from improvement. It is never too late to conduct a PIA.

OVIC encourages organisations to treat PIAs as living documents, rather than as once-off exercises. If a program is long-running, has different phases, or changes over time, it is worth revisiting the PIA to review its currency and update the assessment accordingly. For example, if enabling legislation or privacy law changes over time, new information elements are collected, or a new system is implemented to run the program, the PIA should be updated to account for the changes.

PIAs are best incorporated into your organisation's 'business as usual' processes. Rather than creating new procedures, fitting a PIA into established assurance, risk management and policy development processes can help integrate PIAs into your organisation's standard practice and minimise the creation of excessive or unnecessary work. In undertaking a PIA, you may be able to leverage exisiting processes and materials, avoiding duplication and simplifying privacy asssessments.

> **Top tip**
>
> Implement document version control so you can track the life of the PIA and how it has been updated throughout the life of the program.

Who should do a PIA?

The PIA process can be undertaken by anyone with knowledge of the program being assessed, however it is a good idea to have the process completed by the individual who is best placed to assess the risk for a particular program, given their knowledge of program within the unique operating environment of the organisation. It can also be useful to include someone who is familiar with privacy in the process.

You do not need to be a privacy specialist, a Privacy Officer or a lawyer to conduct a PIA. This guide and OVIC's PIA template have been designed for use by any employee of an organisation.

Privacy Officer

When going through the process of conducting a PIA, it is recommended that you consult with and seek the advice of your organisation's Privacy Officer. They will be best placed to understand your organisation's processes and legislative requirements, and may be able to assist in identifying unseen privacy risks, or clarify misunderstandings of privacy legislation. If your organisation does not have a Privacy Officer, your legal team may also be able to assist.

Who else should be involved?

Internal stakeholders

It is often the case that a program will span over several areas within an organisation, and in conducting the PIA you may need to work with other areas to gather information and understand their operating environment. Other areas responsible for information may also need to be consulted. Examples include (but are not limited to) records management, ICT, human resources, information security, legal, and policy.

Working with other relevant internal stakeholders across your organisation can also be useful to help you identify privacy risks that may arise in other business units that are both directly and indirectly involved in the program.

External stakeholders

If your organisation is conducting a PIA for a program that interacts with or affects other organisations, including contracted service providers (**CSPs**), it may be necessary to consult with these stakeholders. If a CSP is being contracted to provide a service for your program, it is important to consider consulting with the CSP when conducting a PIA.

The community's expectations of how their information should be handled and public perception of the program should also be considered in the PIA process. For particularly large or potentially invasive programs, your organisation may wish to consider undertaking public consultation, for example by inviting submissions or holding public forums.

External consultants

If your program is particularly complex (for example, there are many parties, the information flows are complicated, or there are a number of overlapping pieces of legislation), it may be worth considering hiring an experienced specialist to conduct the PIA (for example, a law firm), or consulting with a privacy expert. Having an external consultant involved in the PIA process can offer an independent perspective of the privacy risks involved, and can be a good idea if the program raises contentious issues or could be perceived as privacy-invasive.

However, even where an external specialist is consulted, it is good practice to involve internal staff in the process. This will ensure that the PIA accurately reflects how the program will operate, and is informed by an understanding of your organisation's operating environment. Involving staff will also make undertaking PIAs internally easier in the future.

Consulting with OVIC

Organisations are not obliged to consult with or share their PIA templates or reports with OVIC. If your organisation wishes to do so, it may be worth engaging with OVIC in the early stages of a program's development. However, as an independent regulator, OVIC cannot conduct the PIA for your organisation, nor can we endorse programs or privacy protections that you may have in place. If you choose to consult with OVIC, our staff will review the PIA template or report and provide general feedback on potential issues under the PDP Act or areas that may warrant further attention.

OVIC strongly encourages you to engage with your organisation's Privacy Officer and seek their input before sharing your PIA template or report with us.

Publishing your PIA

Your organisation may wish to consider publishing completed PIA templates or reports where appropriate, which can have several benefits. As well as demonstrating your program's compliance with the PDP Act and good privacy practices, publishing your program's PIA template or report can help enhance the public and other stakeholders' trust and confidence in your organisation.

However, you should consider the privacy and security implications before publishing a PIA template or report. For instance, all personal information and any specific details of security processes or commercially sensitive information that may introduce risk to your organisation should be removed before making the template or report available to the public.

Internal PIA register

Where appropriate, it is also a good idea to keep an internal central register of PIAs that your organisation conducts, regardless of whether or not you decide to publicly publish the resulting template or report. Maintaining a register has many benefits: it allows your organisation to keep track of all the PIAs that have been conducted, and allows employees to refer to previous PIA templates or reports to assist in conducting their own PIA. A register also provides organisational memory – it allows individuals who may not have been involved in the PIA process or who are new to the organisation to learn from the PIAs and identify areas of best practice.

Similarly, however, there may be privacy and security considerations to keep in mind when deciding to make a PIA template or report available to employees within your organisation – it may not be appropriate for all business units across the organisation to access a particular template or report, for example because of sensitive or restricted content.

How to use these documents

The PIA template includes references to relevant paragraphs and page numbers in this guide to provide further context, examples and information about the questions the template asks you to answer.

The PIA template is a suggested model for documenting and reporting on the PIA process. You should feel free to adapt the template and add additional information as required. You may not need to answer every question or section of the PIA template, as some parts may not be applicable or relevant to your specific program. For example, if your program does not collect any new personal information, you may not need to answer the questions relating to collection.

What is a program?

This guide refers to undertaking a PIA in relation to a 'program'. This term is used broadly and is intended to cover the full range of an organisation's activities that may have privacy implications, such as legislation, a project or initiative, a service, application, platform, policy, database or procedure. The PIA template is designed to be scalable to one-off projects, ongoing initiatives, and amendments to established processes.

> **Top tip**
>
> In some cases, your program may involve the use or development of a new platform, application or service, but does not actually collect any personal information. In these cases, you should think about how the platform, application or service itself will be used more broadly. If it enables or is intended to allow users to collect personal information, consider doing a PIA.

A note on health information

In Victoria, health privacy is covered by the *Health Records Act 2001* (**HR Act**) and the Health Privacy Principles (**HPPs**), rather than the PDP Act. If your program involves health information, you will need to ensure that you take the HPPs into consideration.

The PIA template and this guide do not assess the privacy of health information, however, if your program involves the collection or use of health information you may wish to adapt this template to include an assessment of health privacy. You should seek advice on complying with the HR Act from the Health Complaints Commissioner,[2] who regulates the handling of health information in Victoria.

In some cases, the federal *Privacy Act 1988* (Cth) (**Privacy Act**) and the Australian Privacy Principles may also apply to health information held by private sector health service providers. This is particularly important to note if your program is engaging third parties such as private sector health service providers. For more information on complying with the Privacy Act contact the Office of the Australian Information Commissioner.[3]

[2] For more information go to https://hcc.vic.gov.au/ or contact the Health Complaints Commissioner.
[3] For more information go to https://www.oaic.gov.au/.

The structure of the PIA template

OVIC has structured the PIA template to mirror the information lifecycle common to many programs, to make it simple to visualise the information flows from the time the information is first collected to when it is disposed.

Often, conducting a PIA won't be a linear process. For example, you may realise partway through that a particular element of the program has not been designed yet and you are unable to complete a section of the template until a later time. Do not be concerned if you find yourself doing things in a slightly different order than set out in the template.

> **Top tip**
>
> Where you reference other documents in the PIA template that relate to the program, such as policies, process documents, or additional information about the program, attach these documents to give further context about the PIA process to the reader.

The structure of this accompanying guide

This guide is divided into four sections to mirror the structure of the PIA template:

- **Part 1** provides the context to your PIA process and forms the basis of your PIA template or report. It covers the description of your program, the scope of the PIA, your organisation's legal authority to collect the personal information for your program, any stakeholder engagement undertaken in relation to your program, and the information flow diagram.
- **Part 2** relates to the privacy analysis table of the PIA template. It provides guidance on the information that should be included as you complete the privacy analysis, and considerations that may assist you as you answer the questions contained in the table.
- **Part 3** addresses the risk assessment section of the PIA template. It provides an explanation of the different columns of the risk assessment table in the PIA template, and guidance on completing the table.
- **Part 4** covers various elements to finalise the PIA template, such as the endorsement, identifying any actions to complete arising from the PIA process, and information about the document itself.

Part 1

1. Description of the program and parties

1.1 This section of the PIA template provides important context for the rest of the assessment. It provides the basis for the privacy analysis in Part 2 of the PIA template.

The program description should be detailed enough to allow anyone reading the report to understand the project. It should be written in plain English, with any technical language or jargon clearly explained.

1.2 OVIC encourages organisations to undertake a PIA as early as possible in the process and treat it as a living document. This helps to embed privacy in the design and development of your program. If your program is still at an early stage of development at the time of undertaking the PIA process, it may not be possible to prepare a detailed description or be completely certain of particular details. You may decide to complete a preliminary processin the first instance, and a more thorough PIA process once further information is available.

1.3 The following subheadings have been provided to assist in breaking up the program description into key areas. While these subheadings are a guide only, you should attempt to consider each of the areas below when completing the program description.

Detailed description of the program, including its context, purpose and objectives

1.4 The description should provide an overview of the program and how it fits within the context of your organisation. It should be written in such a way that anyone who is unfamiliar with the program can gain a decent understanding of what the program is and why it is being done.

For example, the individuals endorsing the PIA template or report might not have been closely involved in the program development. It will be important for them to have a detailed understanding of the program before they endorse the document.

1.5 This section should also include information regarding:

- The purpose of the program and why it is being introduced – did a policy or legislative change prompt the program?
- The aims of the program – what objectives does the program intend to achieve? Will the program change the way things are currently done?
- How these aims fit within your organisation's broader objectives.

1.6 If you have other documents that provide background to the program, you may wish to attach these to the PIA template or report to provide additional information and context.

How the program will operate

1.7 The description should include information about:

- the different components of the program and how it will work, including which areas or employees of your organisation are involved in running the program;
- who is responsible for the program;
- how it interacts with other programs or systems within your organisation;
- any important milestones in the project or when significant decisions will be made that may have a bearing on the program; and
- from whom or where your organisation is collecting information, including personal information.

1.8 This section should also identify the duration of the program (for example, whether it is ongoing or if there is an end date), and any timeframes regarding its implementation (including pilots).

1.9 If your program includes the use of a technical platform, service or application, this section should include an overview of the product, what it does, and specifically which functions your program will or will not be using. Your assessment should focus not only on the platform or service alone but also on the uses to which the platform or service may be put by users.

The expected benefits of the program

1.10 The description should include a discussion about the expected benefits of the program for your organisation and other stakeholders, such as the public. Including the expected benefits of the program will help in instances where your organisation is required to make an assessment about whether the potential privacy risks are adequately balanced by its expected benefits.

Other parties and their roles, including contracted service providers

1.11 In some cases, there may be other parties involved in a program. For example, your program may be collecting personal information via a third party platform, or organisations may engage third parties such as CSPs that collect, use, or handle personal information to perform a function on your organisation's behalf.

1.12 This section should outline and describe all the different parties involved, their roles, and what personal information they will be collecting (if any), and how they will be using or handling that information. You may also wish to explain why it is necessary to have a third party involved in the program, and if relevant, whether the third party is bound by the PDP Act, or other privacy legislation.

For more information on CSPs and privacy, refer to OVIC's *Guidelines for outsourcing in the Victorian Public Sector Checklist*[4] and the *Accompanying Guide*.[5]

[4] Available at https://ovic.vic.gov.au/resource/guidelines-for-outsourcing-in-the-victorian-public-sector-checklist/
[5] Available at https://ovic.vic.gov.au/resource/guidelines-for-outsourcing-in-the-victorian-public-sector-accompanying-guide/

2. Scope of the PIA

What the PIA will and will not cover

2.1 As the process of undertaking a PIA will vary each time you do one, it is important to be clear on the scope of your assessment. Doing this will help to ensure that the privacy analysis in Part 2 assesses only the elements of the program that are intended to be covered. Being clear about the scope will help clarify the answers to many of the privacy analysis questions.

2.2 This section should explain exactly what part or phase of the program the PIA covers and, where necessary for clarity, what it does not cover. The program's nature and stage of development will have an impact on the scope of the PIA. For instance, some programs may be incremental and take place over many stages; in these cases, organisations may choose to conduct multiple PIA processes. This should be made clear in this section.

2.3 Some questions to consider when completing this section include:

- What are the areas that this PIA will cover, and what is outside the scope of this PIA?
- Does this PIA cover the entire program, or just one part or phase? For example, does it relate only to the initial set up of a program, or the ongoing use of a program? Does the program only cover the pilot stage, or the entire program?
- Is there a public interest determination, temporary public interest determination, information usage arrangement or certification in place that affects the operation of the program? For more information on these mechanisms, see OVIC's *Guidelines to Public Interest Determinations, Temporary Public Interest Determinations, Information Usage Arranngements and Certification*.[6]

Other relevant PIAs

2.4 If the PIA is not intended to cover a program in its entirety, this section should identify if other PIA processess for other parts of the program have been undertaken, or if any other PIAs will be conducted at a later date that are relevant to this program.

> **Top tip**
>
> When looking at different aspects of a program separately, the privacy risks may seem small or insignificant; however, the program as a whole may have significant privacy impacts that you may not be able to identify as a result of a limited PIA scope.
>
> If the scope of your PIA is limited to a particular aspect or stage of your program, consider the potential impacts of the broader program – other elements of the program may have privacy impacts that are not identified or covered in this PIA.

[6] Available at https://ovic.vic.gov.au/resource/guidelines-to-public-interest-determinations/

Multiple parties

2.5 If there is more than one party involved in the program (for example, another organisation or a CSP), it is important that the scope identifies whether the PIA assesses only your organisation's handling of personal information, or covers the obligations of all parties involved in the program.

2.6 Multiple organisations may decide to undertake a joint PIA. Generally, separate privacy assessments should still be conducted for each party involved, as the information handled by each party may vary, and different privacy obligations and legal authorities may apply. A joint PIA process should clearly distinguish between the privacy assessments for each party.

> **Top tip**
>
> If the scope of your PIA is not clear upfront, creating an information flow diagram can help to clarify the scope and other parties involved in the program. See section 5 below for more information.

3. Legal authority

3.1 Identifying the legal authority that your organisation has to collect, use or disclose personal information is an important part of the PIA process. Your organisation's legal authority will often stem from enabling legislation, which outlines your organisation's functions and powers. In some cases, there may be another law that provides authority for your organisation to perform certain functions or activities.

3.2 If you have legal authority under your organisation's enabling legislation or another piece of legislation to collect, use or disclose personal information for the purposes of this program, cite the relevant legislation and section within that Act. It is also worth highlighting how this program will enable your organisation to facilitate this function.

3.3 If you cannot identify a specific provision in enabling legislation that authorises your organisation to handle personal information for your program, you may have authority under the IPPs in the PDP Act. However, where possible, you should always seek to rely on your organisation's enabling legislation in the first instance.

3.4 There may be other legislation or regulations to consider in addition to your organisation's enabling legislation and the PDP Act. For example, your organisation may need to take the *Charter of Human Rights and Responsibilities Act 2006*[7] into account when considering the design, development, and implementation of your program. Other privacy or information sharing laws, such as the HR Act, the Privacy Act,[8] or the *Victoria Data Sharing Act 2017*[9] may also be relevant in some cases.

> **Top tip**
>
> If you are not sure about which legislation allows your program to collect, use and disclose personal information, your organisation's legal team or Privacy Officer may be able to assist you with this.

[7] Available at http://www.legislation.vic.gov.au/
[8] Available at https://www.legislation.gov.au/
[9] Available at http://www.legislation.vic.gov.au/

4. Stakeholder consultation

4.1 Conducting a PIA can help demonstrate to stakeholders that a program has been designed with privacy in mind. However, ensuring that your program complies with the law may not always be enough. Consulting with key stakeholders helps to ensure that your program is not only legally compliant, but also consistent with stakeholders' expectations.

4.2 Consultation may include:

- internal stakeholders, such as other business units within your organisation;
- external stakeholders, such as CSPs that may be involved or engaged for the program; and
- other third parties that may be impacted by the program, such as other organisations that may be directly or indirectly involved in the program.

Community expectations

4.3 You should also consider community attitudes to, and expectations of, privacy. If your program is likely to impact upon individuals, their expectations should be factored into the PIA process and the program design more broadly. In some instances, public consultation may be appropriate, especially where a substantial amount of personal information is being handled, or where sensitive information is involved.

4.4 Public consultation can also contribute to community awareness of the program, increase public confidence, and have positive impacts on community support for the program. If your program is legally compliant with the IPPs, but the community lacks trust in the way your organisation handles their personal information, this potentially stands to damage the long-term effectiveness of the program and reputation of your organisation.

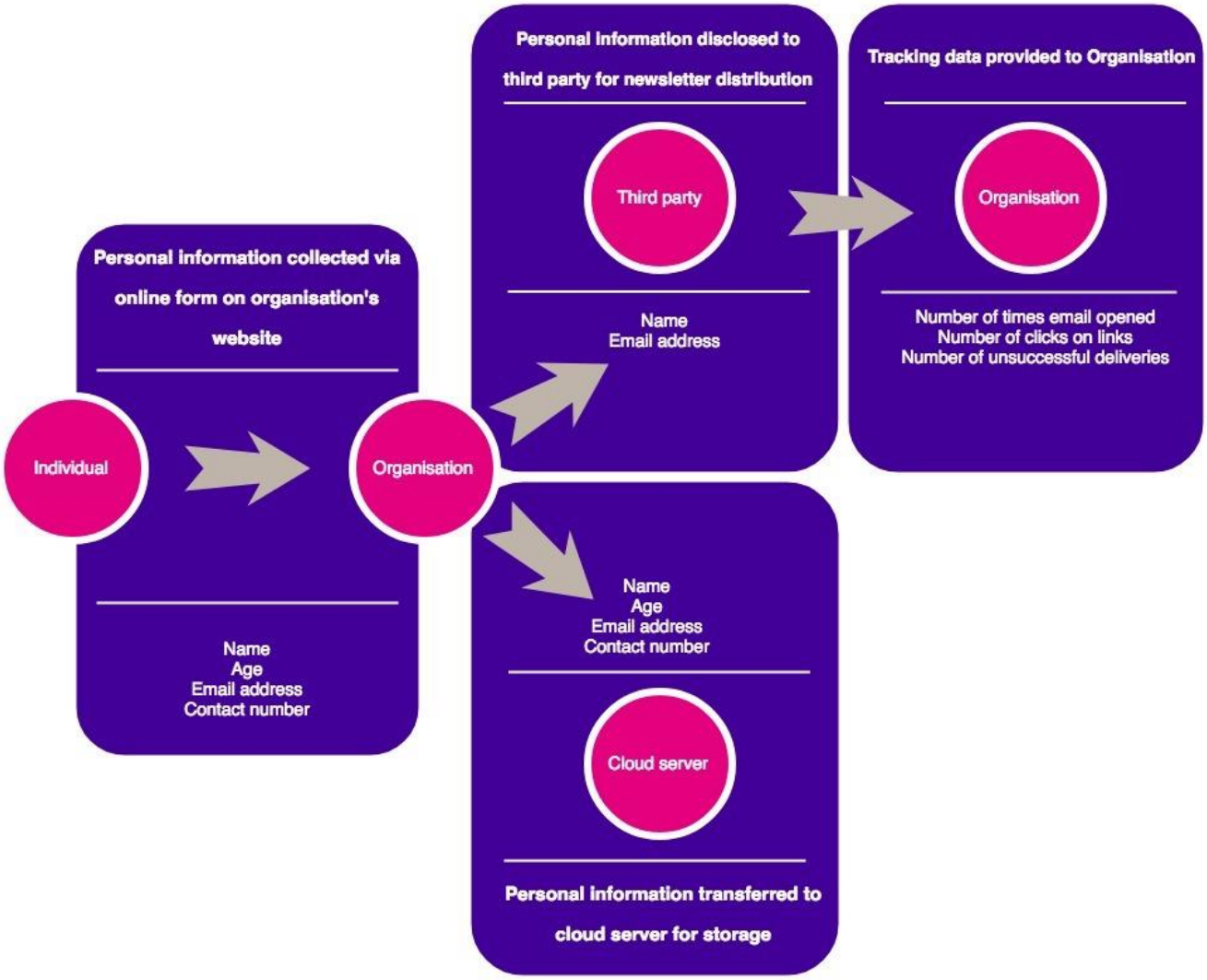
4.5 This section of the PIA template should outline and describe any stakeholder consultation that has occurred, or will occur, as part of your program. You may also wish to describe the outcomes of consultation, and attach any relevant documents, where possible.

5. Information flow diagram

5.1 A visual representation is a useful way to provide a clear outline of your program's information flows across the organisation or between different parties. An information flow diagram or table should clearly map out each stage of the program and where possible, identify the information elements involved. If information is being shared or disclosed with another party, the diagram or table should identify the recipient party and what information they are receiving.

5.2 Where multiple organisations are involved, the diagram or table should identify how each organisation is involved in the program.

5.3 See an example of an information flow diagram below:



Part 2

Part 2 of the PIA template involves an assessment of the program against a set of privacy and information handling considerations.

Assessing privacy impacts should not just be about legal compliance. While it is important for a program to adhere to the IPPs in the PDP Act, it is equally important to be aware of other privacy considerations that go beyond the legislation. The questions in the privacy analysis table under Part 2 of the PIA template encourage organisations to approach privacy as an important part of good information management practices, not simply a compliance activity.

The privacy analysis table broadly follows an information lifecycle approach, with questions grouped according to the different stages of the information lifecycle: collection, data security, use and disclosure, access and correction, and data destruction. This approach will allow you to think about your program's information flows from the time that personal information is collected, to when it is disposed.

The table also includes questions to prompt you to identify whether any privacy risks arise at each stage of the information lifecycle. Some examples of potential privacy risks to watch out for are included under the relevant sections of this guide. However, it is important to bear in mind that these are examples only and may not constitute a risk to your organisation in every case – risk should be assessed on a case by case basis.

As you complete the privacy analysis, you should keep in mind that the PDP Act is default legislation. This means that if there is a provision in other legislation that is inconsistent with the provisions or IPPs within the PDP Act, that other legislation overrides the PDP Act to the extent of the inconsistency (that is, other provisions in the PDP Act would still apply (section 6 of the PDP Act)).

A short guide to the IPPs is included in Appendix 1 to help you understand the privacy obligations under the PDP Act. For the full text of the IPPs visit the OVIC website.[10]

6. Identifying information elements

6.1 This section of the guide relates to questions 1 – 5 in the privacy analysis table of the PIA template.

These questions will help you to consider if the information involved in your program is capable of identifying an individual.

Personal Information

6.2 When assessing privacy impacts the first consideration is whether personal information will be involved in the program. Section 3 of the PDP Act defines personal information as:

> **Personal information** means information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act 2001 applies.

[10] See https://ovic.vic.gov.au/resource/the-information-privacy-principles/

6.3 Information does not have to directly identify an individual in order to be considered personal information under the PDP Act. If a person's identity can be reasonably ascertained from the information, it may constitute personal information.

6.4 Further, a piece of information does not have to be able to identify an individual on its own to be considered personal information. An individual's identity may be reasonably ascertained if a piece of information can be linked with other information, or if reasonable steps can be taken to make the individual's identity apparent. For example, position titles and location data could be linked with other information to reveal an individual's identity, and may therefore constitute personal information.

For more information about personal information, including types of information that may be identifying, see OVIC's *Guidelines to the Information Privacy Principles*.[11]

6.5 When completing question 1 of the privacy analysis table, list each piece of personal information that is involved in your program. This will help you to identify whether every element of personal information is necessary for your program. You may wish to attach to the PIA other documents you already have that list this information.

6.6 In some cases, your program may involve information that is non-personal or does not appear to be capable of identifying an individual. This might include, for example, information about vehicle data, or data obtained from personal devices. Similarly, however, this information could be linked with other information to reasonably ascertain individuals' identities, or how the information is used within the context of the program may give rise to the possibility of ascertaining or inferring individuals' identities.

Sensitive Information

6.7 Due to the nature of sensitive information, the IPPs contain specific provisions relating to the circumstances in which sensitive information can be collected, used and disclosed (IPP 10 – sensitive Information). While there are many types of information that individuals may consider to be sensitive or delicate, Schedule 1 of the PDP Act defines sensitive information as:

> **Information or an opinion about an individual's—**
>
> a) racial or ethnic origin
>
> b) political opinions
>
> c) membership of a political association
>
> d) religious beliefs or affiliations
>
> e) philosophical beliefs
>
> f) membership of a professional or trade association
>
> g) membership of a trade union
>
> h) sexual preferences or practices
>
> i) criminal record—
>
> that is also personal information.

[11] Available at https://ovic.vic.gov.au/resource/guidelines-to-the-information-privacy-principles/

6.8 When completing question 3 of the privacy analysis table, include an explanation of why each piece of sensitive information is needed for your program, in addition to identifying how the collection of this information is authorised. You may wish to attach to the PIA template or report other documents you already have that list this information.

6.9 For more information about sensitive information, see OVIC's *Guidelines to the Information Privacy Principles*.[12]

Health Information

6.10 While the PDP Act does not apply to health information, it is useful for organisations to understand the distinction between personal information and health information when undertaking a PIA. The PDP Act and the IPPs will not apply to health information; if your program involves health information, you should consider your organisation's obligations under the HR Act, and where applicable, the federal Privacy Act (see page 8 above).

> **Health information** is defined in the *Health Records Act 2001* as:
>
> a) information or an opinion about -
>
> (i) the physical, mental or psychological health (at any time) of an individual; or
>
> (ii) a disability (at any time) of an individual; or
>
> (iii) an individual's expressed wishes about the future provision of health services to him or her; or
>
> (iv) a health service provided, or to be provided to an individual – that is also personal information; or
>
> b) other personal information collected to provide, or in providing, a health service; or
>
> c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
>
> d) other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or of any of his or her descendants – but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act.

Unique Identifiers

6.11 The PDP Act has specific requirements for the assignment, adoption, use and disclosure of unique identifiers (IPP 7 – Unique Identifiers).

> **Unique identifier** means an identifier (usually a number) assigned by an organisation to an individual to uniquely identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name, but does not include an identifier within the meaning of the Health Records Act 2001.

[12] Available at https://ovic.vic.gov.au/resource/guidelines-to-the-information-privacy-principles/

6.12 An example of a unique identifier is a tax file number, a driver's licence number, a passport number or a Centrelink Customer Reference Number.

For more information about unique identifiers, see OVIC's *Guidelines to the Information Privacy Principles.*[13]

De-identified information

6.13 Section 3 of the PDP Act provides a definition of de-identified information:

> **De-identified**, in relation to personal information, means personal information that no longer relates to an identifiable individual or an individual who can be reasonably identified.

6.14 In some cases, a program may involve the collection of information that is de-identified. It is important to consider whether there is a risk that this information could be re-identified to reveal individuals' identities, for example by matching it to another dataset that does contain identifying information about individuals.

6.15 The risk of re-identification will vary on a case by case basis. For example, disclosing de-identified information in an open data context (such as making it publicly available) may attract a higher level of risk, particularly where that information is unit-level record data, compared to that same information being used or disclosed in a secure environment with access limited to certain individuals.

6.16 Although it may appear from the outset that your program does not involve any personal information, de-identified information may in fact constitute personal information due to the possibility of re-identification.

6.17 If your program involves de-identified information, consider the potential for re-identification and make sure to describe this when answering question 5 of the privacy analysis table. OVIC also recommends considering whether de-identified information could be treated as personal information, as best practice. For more information about de-identification and the risk of re-identification, refer to OVIC's *Protecting unit-record level personal information* report[14] and *De-identification and privacy – Considerations for the Victorian public sector*.[15]

6.18 The Victorian Centre for Data Insights (**VCDI**)[16] also has useful information about de-identification in its *De-identification Guideline*.[17] If your program involves the use of de-identified information for data analytics and insights, it may be beneficial to consult the VCDI for additional advice.

[13] Available at https://ovic.vic.gov.au/resource/guidelines-to-the-information-privacy-principles/
[14] Available at https://ovic.vic.gov.au/wp-content/uploads/2018/07/Protecting-unit-record-level-personal-information.pdf
[15] Available at https://ovic.vic.gov.au/resource/de-identification-and-privacy-considerations-for-the-victorian-public-sector/
[16] For more information about the VCDI, go to https://www.vic.gov.au/datainsights.html
[17] Available at https://www.vic.gov.au/datainsights/data-sharing.html

7. Collection of personal information

Personal information collected should be necessary

7.1 This section of the guide relates to questions 6 – 8 of the privacy analysis table in the PIA template.

7.2 Under IPP 1 – Collection, your organisation should only collect personal information if it is necessary to fulfil its functions or activities. In practice, this means you should only be collecting personal information if it is necessary for the operation of your program, not because it might be useful to have for the future. If the information is necessary, your program should only collect the minimum amount of personal information needed.

For example, if you need to know where an individual lives, consider whether collecting their city, town or postcode is sufficient for the purposes of the program, rather than collecting their entire residential address.

For more information on what is considered 'necessary', refer to OVIC's *Guidelines to the Information Privacy Principles*.[18]

7.3 For each element of personal information collected for the program, explain why that piece of information is being collected. Knowing the purpose for collecting information is a key part of good information management, as it will inform who can access that information, how it will be used, and how identified risks will be managed. It will also help you explain to individuals why you need the personal information you collect from them.

7.4 If your program is collecting sensitive information, ensure that you have the legal authority to collect this type of information under your enabling legislation, or in accordance with the provisions of IPP 10 – Sensitive Information. Under IPP 10, sensitive information can only be collected in certain circumstances, such as with the individual's consent or where the collection is required under law.

> **Top tip**
>
> When relying on consent to collect or use personal information, ensure that the consent obtained is meaningful. Meaningful consent has five elements: it must be voluntary, specific, informed, current, and given by someone with capacity. For more information on consent, refer to OVIC's *Guidelines to the Information Privacy Principles.*

[18] Available at https://ovic.vic.gov.au/resource/guidelines-to-the-information-privacy-principles/

7.5 You should also consider whether your program needs identifying information at all. If you don't need to know someone's identity for the purposes of your program, it is best practice not to collect this information. This aligns with IPP 8 – Anonymity, which states that, where practicable, individuals should have the option of not identifying themselves when transacting with an organisation. Not collecting identifying information will also lower the potential for privacy risks to arise.

> **Examples of potential privacy risks when collecting personal information**
>
> - Personal information is collected without a clear legal authority or purpose.
> - Personal information is collected even though it is not required for the program.
> - ICT systems used mandate the personal information collected (such as mandatory fields that are not necessary).

Method of collection

7.6 This section of the guide relates to questions 9, 10 and 12 of the privacy analysis table in the PIA template.

7.7 Your program should collect personal information in a way that is lawful and fair, and via the least intrusive method available (IPP 1.2). For more information about IPP 1.2 refer to OVIC's *Guidelines to the Information Privacy Principles.*[19]

7.8 If your program collects personal information via a third party (for example an online platform), it is important to consider that party's information handling practices. When completing question 9 of the privacy analysis table, you should identify whether those parties and platforms will also be collecting that information and where possible, explain how they store and manage it (including who has access to it and for how long they will keep it). You might also wish to consider attaching or linking to the privacy policies of these third parties in the PIA template.

7.9 If it is reasonable and practicable, your program should collect personal information directly from the individual concerned (IPP 1.4). This will mean that individuals know what information you are collecting about them, and will help to ensure the information collected is accurate, complete and up to date, which can assist with meeting IPP 3 – Data Quality. For example, this may include confirming with an individual that their personal information is correct at the time of collection to ensure that it is accurate and complete.

7.10 There are some instances where it may not be practicable or reasonable to collect information directly from an individual (IPP 1.5). An example of indirect collection is when an individual discloses personal information about their family members or other parties to an organisation, in an application for welfare benefits.

[19] Available at https://ovic.vic.gov.au/resource/guidelines-to-the-information-privacy-principles/

7.11 If your program involves indirect collection, your PIA template or report should explain why the information cannot be collected directly from the individual.

> **Examples of potential privacy risks when collecting personal information**
>
> - The consequences if personal information is collected via unreasonably intrusive means that the individual or community does not expect.
> - The collection of personal information may be considered unfair if the individual was wrongly under the impression that the collection was required by law.
> - The risk that personal information collected indirectly from third parties is inaccurate, incomplete or out of date.

Notice of collection

7.12 This section of the guide relates to questions 11 and 13 of the privacy analysis table in the PIA template.

7.13 When completing questions 11 and 13 of the privacy analysis table, describe when and how your collection notice will be provided to individuals.

7.14 If you are collecting an individual's personal information for your program, you are generally required to tell that individual about the collection and explain why their information is being collected. Your collection notice should be easy to read and understand, and should be provided at or before the time of collection, or as soon as practicable after. IPP 1.3 contains a list of details that must be included in a collection notice.

If your organisation is a law enforcement agency, you may not have to provide notice to individuals in certain circumstances (section 15 of the PDP Act).

7.15 If your program involves collecting personal information about an individual indirectly from a third party, you should still take reasonable steps to notify that person about the collection, unless doing so would pose a serious threat to the life or health of any individual (IPP 1.5). If this is the case, you should note this in the PIA template or report.

7.16 Depending on the context of your program, a single collection notice may become too long and complex. In this case, you may wish to consider adopting a layered approach to providing notice by providing an initial summary of the key points, and pointing the individual to further documents for more information about the collection. If your program decides to take a layered approach to providing notice, make sure to note this in the PIA template or report.

> **Top tip**
>
> Remember, a collection notice is different to a privacy policy. Collection notices are specific to each individual instance of collection. For more information about collection notices, refer to OVIC's Guidelines to the Information Privacy Principles.

Assigning or adopting unique identifiers

7.17 This section of the guide relates to questions 14 and 15 of the privacy analysis table in the PIA template.

7.18 If your program involves assigning a unique identifier, you should only do so if it is necessary to enable your organisation to carry out any of its functions efficiently (IPP 7.1). If you are collecting a unique identifier assigned by another organisation to adopt as your own, ensure that this is authorised under one of the exceptions under IPP 7.2.

7.19 If your program does assign or adopt another organisation's unique identifier, your response to question 14 of the privacy analysis table should clearly explain the purpose for assigning or adopting that unique identifier – how is the unique identifier necessary, and what would the effect be if unique identifiers were not used? The legal basis for assigning or adopting unique identifiers should also be identified, noting that IPP 7 places limitations around this.

7.20 If your program requires individuals to provide unique identifiers in order to obtain a service (for example a driver's licence number), consider whether this is authorised under IPP 7.4, which places limitations around when this can be done. You should also consider whether your organisation's enabling legislation, or other legislation, allows your program to require that individuals provide a unique identifier in order to receive a service.

7.21 When completing questions 14 and 15 of the privacy analysis table, you should also explain how the unique identifier will be used and whether it will be matched to other information that your organisation may already hold about an individual. More information about unique identifiers can be found in OVIC's *Guidelines to the Information Privacy Principles*.[20]

> **Examples of potential privacy risks when collecting personal information**
>
> - The collection notice is not easily accessible to some people (for example, individuals for whom English is not their first language, or people with visual impairments or limited capacity to understand the notice).
> - Individuals may be unhappy if they become aware that an organisation has collected their personal information from another source, without their knowledge.

8. Security of personal information

8.1 This section of the guide relates to questions 17 – 20 of the privacy analysis table in the PIA template.

8.2 Protecting the security of personal information is important. Under IPP 4 – Data Security, your organisation is required to take reasonable steps to protect the personal information it holds from misuse and loss, and from unauthorised access, modification or disclosure (IPP 4.1). For the purposes of IPP 4.1, the security of personal information should be viewed through a human rights

[20] Available at https://ovic.vic.gov.au/resource/guidelines-to-the-information-privacy-principles/

lens, with a focus on the individual. Decisions about the security of personal information should therefore be made with due consideration to their impact on individuals' right to privacy.

8.3 When completing the PIA template or report, you should clearly detail the steps your organisation will take, or the measures already in place, to protect the personal information that is collected, used, disclosed and stored for the program. The measures that your organisation takes to protect personal information under IPP 4.1 should be proportionate to the potential consequences (to both your organisation and affected individuals) if the information was compromised.

8.4 If there are third parties or CSPs involved in your program, it is also a good idea to consider how these external parties will protect the personal information they hold (if any). You should also keep in mind other security obligations your organisation has, which may be detailed in policies, procedures or other legislation. If your program needs to adhere to other security requirements, make sure to note this in the PIA template or report.

Reasonable steps

8.5 When determining what steps are reasonable under IPP 4, there is no one size fits all. What is considered 'reasonable' will depend on your organisation's individual circumstances and the risks you need to manage. The measures that you implement for this program (or your organisation more broadly) should be appropriate to those circumstances and risks.

8.6 Security should also be viewed holistically. Your organisation may decide to adopt several measures across governance and multiple security domains, however they should be viewed as interrelated and the steps taken should be considered as a whole – one measure may have little impact on an individual's privacy, but when combined with other measures the steps may in fact have significant consequences for privacy.

8.7 Some factors to consider when determining reasonable steps may include:

- the amount and sensitivity of the personal information collected, used, and disclosed for your program;
- the likelihood of the information being subject to a breach;
- the possible adverse impacts for individuals in the case of a breach;
- the confidentiality, integrity and availability of the information; and
- whether a mitigating measure itself is privacy invasive.

8.8 If your organisation is covered by Part 4 of the PDP Act, it will be required to adhere to the Victorian Protective Data Security Framework (**VPDSF**) and Victorian Protective Data Security Standards (**VPDSS**).[21]

8.9 For more information about 'reasonable steps', refer to OVIC's *Guidelines to protecting the security of personal information: 'Reasonable steps' under Information Privacy Principle 4.1*.[22] The VPDSF and VPDSS can also be used as a guide for organisations in determining what constitutes 'reasonable steps' for the purposes of IPP 4.1.

[21] For more information on the VPDSF and VPDSS, see OVIC's website at https://ovic.vic.gov.au/data-protection/what-is-data-protection/

[22] Available at https://ovic.vic.gov.au/wp-content/uploads/2018/07/Guidelines-to-IPP-4.1.pdf

> **Top tip**
>
> The 'reasonable steps' that your organisation takes to protect personal information should encompass good governance and the four security domains: information security, personnel security, ICT security, and physical security.

Security risk assessments

8.10 In addition to undertaking a PIA process, OVIC recommends that organisations conduct a security risk assessment (**SRA**) for their programs. Where possible, you should refer to your organisation's own risk management framework and resources in completing an SRA, if you already have an established process in place. For guidance on completing SRAs, refer to OVIC's VPDSF *Assurance Collection*,[23] or for general risk assessment guidance refer to the Victorian Managed Insurance Authority's (**VMIA**) *Risk Management Framework Practice Guide*[24] for more information.

8.11 Refer to, or attach to your PIA, any relevant organisational security policies and your completed SRA, if one has been done.

> **Examples of potential privacy risks regarding the security of personal information**
>
> - Individuals' personal information is accessible to employees who do not need to access it, increasing the risk of unauthorised disclosure.
> - There is no way to monitor or record who has accessed files containing personal information, increasing the risk of misuse or unauthorised access.
> - Third party platforms used or external third parties engaged to collect personal information do not have an equivalent level of security controls in place, increasing the risk of potential compromise of the information.

9. Use and disclosure of personal information

9.1 This section of the guide relates to questions 21 – 23 of the privacy analysis table in the PIA template.

9.2 Generally, personal information should only be used or disclosed for the primary purpose for which it was collected (IPP 2.1). However, IPP 2.1 also permits organisations to use or disclose personal information for other purposes, in certain circumstances.

If your organisation is a law enforcement agency, it may be exempt from complying with IPP 2.1 if it believes on reasonable grounds that non-compliance is necessary (section 15 of the PDP Act). If this is the case, your PIA template or report should explain how this exemption applies.

[23] Available at https://ovic.vic.gov.au/resource/assurance-collection/
[24] Available at https://www.vmia.vic.gov.au/risk/risk-tools/risk-management-guide

Using personal information for a secondary purpose

9.3 In some cases, your program may not collect any new personal information, but instead use or disclose personal information that is already held by your organisation in a new way. If this is the case, it may be useful when answering question 22 of the privacy analysis table to identify the original purpose for which this information was collected. Your PIA template or report should also explain how the new or additional use of the personal information for your program is authorised under your organisation's enabling legislation, the PDP Act, or other legislation.

9.4 If your organisation does use or disclose personal information for a secondary purpose, you may wish to consider notifying the individuals to whom the personal information relates. While this is not required under the PDP Act, it can promote transparency and accountability, and helps foster positive relationships between your organisation and the community. You should also keep in mind your organisation's policies or enabling legislation as they may have requirements relating to notification. This should be noted in the PIA template or report where applicable.

Information sharing

9.5 This section of the guide relates to questions 24 and 25 of the privacy analysis table in the PIA template.

9.6 If your program involves disclosing personal information to external parties, ensure you are authorised to do so under IPP 2.1 or other legislation. This may include your organisation's own enabling legislation, or other laws relating to information sharing, such as the Victorian Data Sharing Act. Make sure that in sharing information, you do not disregard any confidentiality or secrecy provisions in your enabling legislation that may restrict what you can share.

9.7 You should also consider whether it is organisational policy to record any disclosures to third parties, or if your organisation has recordkeeping obligations under other legislation to record any instances of information sharing. If so, make sure to note this in question 24 of the privacy analysis table.

9.8 If your program transfers personal information to a party outside Victoria (other than your own organisation or the individual to whom the information relates), you will need to consider whether this transfer is authorised. Under the PDP Act, transferring personal information outside Victoria is only permitted in certain circumstances (IPP 9). However, your organisation's enabling or other legislation may also permit the transfer of personal information outside of Victoria. When answering question 25 of the privacy analysis table, make sure you identify the relevant authority that allows the transfer.

9.9 When disclosing or transferring personal information to another party, including a recipient outside Victoria, you should ensure that the means of disclosure or transfer (whether physical or electronic) is secure. The PIA template or report should explain how your organisation will ensure the security of personal information transferred outside Victoria.

For more information on information sharing, refer to OVIC's *Guidelines for sharing personal information*.[25]

[25] Available at https://ovic.vic.gov.au/resource/guidelines-for-sharing-personal-information/

Using or disclosing unique identifiers

9.10 This section of the guide relates to question 26 of the privacy analysis table in the PIA template.

9.11 IPP 7.3 places limitations around when an organisation can use or disclose a unique identifier that has been assigned by another organisation. If your program involves using or disclosing another organisation's unique identifier, make sure that you are authorised to do so under the PDP Act or other legislation and when answering question 26, explain how this use or disclosure is authorised.

Data matching

9.12 This section of the guide relates to question 27 of the privacy analysis table in the PIA template.

9.13 Data matching involves comparing two different sources of data, and in some cases, integrating data sets (including publicly available data sets). If your program involves data matching, consider whether the personal information collected for your program can be used for this purpose, either under the PDP Act as a permitted primary or secondary use, or under your enabling or other legislation. Your PIA template or report should explain why the data matching is occurring, and the legal authority that enables your program to conduct data matching.

You should also consider whether there is any other legislation that your organisation must comply with when undertaking any data matching activities. If so, make sure to note this your PIA template or report.

9.14 If your program involves matching or integrating de-identified information with another data set, it is important to be mindful of the potential risk for the de-identified information to be re-identified as a result of the data matching. OVIC suggests ensuring appropriate safeguards are in place to limit the risk of re-identification.

Data quality

9.15 This section of the guide relates to questions 16 and 29 of the privacy analysis table in the PIA template.

9.16 IPP 3 – making sure that the personal information your organisation collects, uses, and discloses is accurate, complete and up to date – applies throughout the entire information lifecycle, not just at the collection stage. When using or disclosing personal information as part of your program, you must therefore ensure that it is accurate, complete, and current. This is particularly important as the personal information your organisation holds about individuals can directly affect and influence their lives – for example, inaccurate personal information may adversely affect an individual's ability to access welfare or services.

9.17 Some measures that your organisation can take to maintain the integrity of the personal information being used or disclosed for the program may include periodic reviews of the information to confirm that it is still accurate, complete and up to date, or implementing a retention schedule. Your PIA template or report should clearly outline any steps or measures your organisation will take to ensure the ongoing integrity of the personal information.

9.18 More information about IPP 3 can be found in OVIC's *Guidelines to the Information Privacy Principles*.[26]

Examples of potential privacy risks when using and disclosing personal information

- Individuals may be upset or surprised if their personal information is used or disclosed for purposes that were not communicated to them at the time of collection.
- Personal information used or disclosed for the program becomes out of date or inaccurate.
- Personal information is shared with or transferred to third parties outside Victoria that are not subject to the same privacy standards.

10. Management of personal information

10.1 This section of the guide relates to questions 30 – 32 of the privacy analysis table in the PIA template.

10.2 Under IPP 5 – Openness, organisations are required to have a document that sets out their policies on the management of personal information. This is often referred to as a privacy policy. This document must be made available to anyone who asks for it (IPP 5.1). Linking to or including your organisation's privacy policy in the PIA can provide additional information and context to the reader.

10.3 If your program involves a new collection, use or disclosure of personal information, you should update your organisation's privacy policy to reflect this new practice. Where applicable or appropriate, it may be a good idea to notify relevant individuals of the changes to your organisation's privacy policy, to promote transparency and trust in your organisation's information handling practices.

For more information about privacy policies, refer to OVIC's *Drafting a privacy policy* information sheet[27] and *Guidelines to the Information Privacy Principles.*[28]

10.4 Upon request, your organisation must also take reasonable steps to let an individual know generally what types of personal information it holds and for what purposes, and how it collects, holds, uses and discloses that information (IPP 5.2).

10.5 Apart from complying with IPP 5, being transparent about the types of personal information your organisation holds is important for facilitating individuals' rights to access and correct their personal information – people need to know what information about them is generally held by an organisation so that they can ask for access to, or correct, that information.

[26] Available at https://ovic.vic.gov.au/resource/guidelines-to-the-information-privacy-principles/

[27] Available at https://ovic.vic.gov.au/resource/drafting-a-privacy-policy/

[28] Available at https://ovic.vic.gov.au/resource/guidelines-to-the-information-privacy-principles/

Access and correction of personal information

10.6 IPP 6 – Access and Correction gives individuals the right to request access to their personal information and correct it where it is inaccurate. Where a VPS organisation has obligations under the *Freedom of Information Act 1982* (Vic) (**FOI Act**), a request for access or correction to that organisation should be made under the FOI Act. However, organisations may also provide access outside the FOI Act. IPP 6 will generally apply where an organisation is not bound by the FOI Act, but *is* bound under state contract to the PDP Act and the IPPs.

10.7 If your program involves CSPs, it is important to clearly identify in the PIA which party (your organisation or the CSP) will hold what information, and how individuals can access their personal information (that is, whether through the FOI Act, IPP 6, or some other avenue).

> **Examples of potential privacy risks when managing personal information**
>
> - The organisation's privacy policy is long and difficult to understand, or is not easily accessible.
> - Individuals cannot easily access or correct their personal information, leading to a risk of poor quality or inaccurate data.
> - Personal information is held by CSPs that are not bound by the FOI Act, nor to the IPPs under State contract, leading to a risk that individuals cannot access or correct their personal information.

11. Disposal of personal information

Recordkeeping obligations

11.1 This section of the guide relates to questions 34 and 35 of the privacy analysis table in the PIA template.

11.2 When identifying how long personal information will be retained for the purposes of your program, you may need to consider a range of different recordkeeping obligations or policies, such as:

- your organisation's enabling legislation;
- your organisation's internal recordkeeping policies or processes;
- the *Public Records Act 1973* (Vic) and any relevant retention and disposal schedules or authorities issued by the Keeper of Public Records (for example Retention and Disposal Authorities);[29]
- IPP 4.2, which states that organisations need to take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose; and
- other legislation that may impose recordkeeping requirements on your organisation or program.

[29] For more information about recordkeeping obligations under the *Public Records Act 1973*, go to https://prov.vic.gov.au/ or contact the Public Record Office Victoria.

11.3 If there is other legislation that imposes requirements to retain information for a certain amount of time, that legislation will override the PDP Act. The requirement to retain personal information for recordkeeping or archival purposes, for example, overrides the requirement under IPP 4.2 to destroy personal information, as retaining personal information for recordkeeping purposes *is* a purpose for which your organisation will need to retain it. If your program or organisation is bound by other legislation to keep personal information for a certain amount of time, make sure that this is clearly reflected in your PIA template or report.

11.4 It is also important to consider security when disposing or destroying personal information. For example, using a communal recycling bin may not be the most appropriate or secure way to dispose of personal information. When completing question 35, explain how your organisation's method for destroying or disposing of personal information for this program is secure.

> **Top tip**
>
> If you are unsure about how long personal information should be retained, you may find it useful to consult with relevant staff in your organisation who have knowledge of or responsibility for recordkeeping matters.

De-identifying personal information

11.5 This section of the guide relates to question 36 of the privacy analysis table in the PIA template.

11.6 If your organisation no longer needs personal information for your program, IPP 4.2 also provides the option of de-identifying the information.

11.7 If your organisation decides to de-identify personal information, it is important to manage the risk of re-identification of that information – consider who will have access to the de-identified information, where it will be stored, and what will be done with it. If applicable, note this in the PIA template or report. The template or report should also outline the steps or measures that will be taken (where relevant) to manage the risk of re-identification.

For more information about the risks associated with de-identifying unit record level data, refer to OVIC's *Protecting unit-record level personal information*[30] and *De-identification and privacy – Considerations for the Victorian public sector*.[31]

Personal information held by third parties

11.8 This section of the guide relates to question 37 of the privacy analysis table in the PIA template.

11.9 If your program involves personal information being transferred to or collected by other parties (for example, cloud service providers or collection of information via third party platforms), it is important to consider what will happen to the personal information that may be held by those parties once its use has expired or the program ends.

[30] Available at https://ovic.vic.gov.au/wp-content/uploads/2018/07/Protecting-unit-record-level-personal-information.pdf
[31] Available at https://ovic.vic.gov.au/resource/de-identification-and-privacy-considerations-for-the-victorian-public-sector/

11.10 Where possible, your PIA template or report should detail for how long any third parties or CSPs will keep the information, how they will destroy or de-identify that information, and where applicable, attach any relevant documents outlining this arrangement.

> **Examples of potential privacy risks relating to the retention and disposal of personal information**
>
> - Personal information is retained indefinitely 'just in case', leading to a risk of a privacy breach or unauthorised use or disclosure.
> - There is a risk that personal information will become out of date or inaccurate if it is held for longer than necessary.
> - Personal information is not securely destroyed, leading to a risk of misuse or unauthorised disclosure.

12. Other considerations

12.1 This section of the guide relates to questions 38 – 44 of the privacy analysis table in the PIA template.

Complaints

12.2 An important element of good privacy governance is having a clear complaints process within your organisation. Identifying how and to whom individuals can make a privacy complaint before the program is implemented could save time and confusion in the future should one be made. This is particularly important if your organisation does not have a designated Privacy Officer.

12.3 In the first instance, privacy complaints should be handled internally by your organisation, ideally by or with the involvement of your organisation's Privacy Officer. If a privacy complaint cannot be resolved, individuals may escalate the complaint to OVIC. For more information about privacy complaints to OVIC, refer to the OVIC website[32] and OVIC's *Guide for respondents*.[33]

12.4 You should ensure that the individuals whose information is being collected, used or disclosed for your program are aware of these internal and external complaint avenues or processes, and when completing question 38 of the privacy analysis table, explain how individuals will be given this information.

Data breach response plans

12.5 In addition to complaints processes, your organisation should also have a data breach response plan in place, in the event that a data breach occurs. A data breach response plan can help your organisation respond to data breaches quickly and efficiently, and potentially significantly reduce the harms (for example financial or reputational damage) to your organisation and affected individuals. If your organisation has a data breach response plan, you may wish to attach it to your PIA template or report, or at least provide a high level overview at question 39 of the steps that your organisation will take when dealing with a data breach.

[32] See https://ovic.vic.gov.au/privacy/for-agencies/responding-to-privacy-complaints/
[33] Available at https://ovic.vic.gov.au/resource/8322-2/

12.6 More information about responding to data breaches can be found on the OVIC website[34] and OVIC's *Responding to privacy breaches: Guidelines*.[35]

Staff training

12.7 Staff training is important as it can help minimise the risk of a data breach and ensure staff have the ability to handle personal information appropriately for the program. Training should be tailored to the specific program in question; however, ongoing training to remind staff of their privacy obligations is also good practice.

Program evaluation

12.8 Another aspect to consider is whether your program will be evaluated. While this is not directly related to any privacy obligations under the PDP Act, evaluating your program has many benefits:

- it can help you track the program against its objectives and ensure that it is meeting them;
- it is a good opportunity to revisit the program's collection and information handling practices, and identify any issues that may have arisen since its implementation; and
- it can allow you to assess the measures and controls in place to mitigate any privacy breaches, to ensure that they are still effective.

12.9 When first designing and developing your program, as well as during any program evaluations, it is a good idea to check your organisation's other existing policies and ensure your program's initial and ongoing compliance with them. If there are any that are applicable to your program or that relate to privacy matters, it may be useful to list them in your PIA template or report.

Other elements of privacy

12.10 As you design, develop, and implement your program, it is also important to keep in mind the other elements of privacy that it might impact upon, such as bodily, locational, and territorial privacy. While the privacy obligations under the PDP Act only cover information privacy, the ways in which your program impacts upon these other elements can have an effect on public expectations, and influence stakeholder and public support and acceptance of the program.

> **Top tip**
>
> When undertaking the PIA process, consider the effects of your program on these other elements of privacy and whether they align with public expectations and your enabling or other legislation, such as the Victorian Charter of Human Rights and Responsibilities. Where you identify potential threats to privacy, consider how you might amend elements of your program to make it more privacy-enhancing.

[34] See https://ovic.vic.gov.au/privacy/for-agencies/responding-to-data-breaches/
[35] Available at https://ovic.vic.gov.au/resource/responding-to-privacy-breaches-guideline/

Part 3

Part 3 of the PIA template assesses the privacy risks identified during the analysis conducted in Part 2. A privacy risk is a potential adverse event that a particular practice or activity associated with the collection, handling and management of personal information will fail to meet individuals' reasonable expectations of privacy.[36] They can arise in many different circumstances, and may be a risk to individuals' privacy, your organisation, or both.

Analysing a privacy risk involves considering the cause(s) and consequence(s) of the risk, and the likelihood of it occurring. The consequences arising from a privacy risk may have an impact on your organisation, as well as the individuals whose personal information is concerned. When assessing risks, it is therefore essential to consider the risk from the perspective of both your organisation and individuals who may be affected by it.

The table included in the PIA template is a basic risk template. Where possible, OVIC recommends using your organisation's existing risk management framework, which may include a risk assessment template specific to your organisation's unique operating environment. If your organisation does not have a standard risk assessment framework, you can use the template in Part 3.

This section of the PIA guide provides guidance on completing the privacy risk assessment table contained in Part 3 of the PIA template. The table and the following guidance is based on the VPDSF *Assurance Collection*.[37]

13. Description of the risk

13.1 The risk description is a concise statement that should cover key elements such as:

- the 'risk event' – what is the privacy risk?;
- the cause of the risk – this may be an external cause outside of your organisation's control, or internal, caused by actions or failures of people, processes, or systems within your organisation. A risk event may also have multiple causes;
- the impact of the privacy risk – if the risk occurred, what would happen to your organisation and the individuals whose personal information is the subject of the risk?

13.2 An example of a risk description is:

> **The risk of** unauthorised / unlawful collection of personal information
>
> **Caused by** individuals not being aware of the collection of personal information by organisation
>
> Resulting in limited:
>
> - legal/regulatory non-compliance (breach of IPP 1 (collection))
> - harm to individual's safety or liberty
> - dissatisfaction from public/VPS, reputational damage, loss of public confidence and trust.

[36] New Zealand Privacy Commissioner, *Part 2: How to do a Privacy Impact Assessment*, p. 12, available at https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment/.
[37] Available at https://ovic.vic.gov.au/resource/assurance-collection/

14. Risk ratings and acceptance

14.1 When assigning ratings under the impact, likelihood and risk columns, you should refer to your organisation's own risk criteria, where possible. You may also refer to the VMIA's *Risk Management Framework Practice Guide* and additional resources published on the VMIA's website.[38]

14.2 The ratings relate to:

- **Impact:** this rating reflects the effect to your organisation if the event occurred. You should also consider the impact of the privacy risk to individuals.
- **Likelihood:** this rating reflects the probability of the privacy risk occurring. When assigning a likelihood rating, consider the cause of the risk and any existing security measures in place within your organisation, as these elements may directly influence the rating.
- **Risk:** once you have identified the impact and likelihood of the privacy risk, assign an overall current risk rating. Where possible you should use the risk rating criteria or matrix within your own organisation's risk management framework.

14.3 The risk acceptance column identifies whether your organisation accepts the privacy risk or not. When determining whether to accept a particular privacy risk, you should consider your organisation's risk appetite (i.e. the amount and type of risk your organisation is willing to accept or avoid to achieve its objectives), as well as the impact to individuals if you decide to accept the risk.

14.4 If the privacy risk is accepted, then you may decide not to treat the risk any further. However, even if the privacy risk is accepted, you may still wish to adopt measures to further lower the risk where possible.

14.5 If the identified privacy risk is not accepted, you will need to identify a risk mitigation strategy (or strategies) to treat the risk.

15. Risk mitigation strategy

15.1 The risk mitigation strategy refers to the measures you will take to mitigate and manage each identified privacy risk. Some mitigation strategies may already be in place within your organisation, or they may be measures that your organisation intends to implement.

15.2 The measures you decide to adopt to treat the identified privacy risks may address different elements of the risk, such as its impact(s), likelihood, or even the personal information itself (for example, minimising the personal information collected). There may also be a range of measures implemented to address one risk.

15.3 Some questions to consider when identifying measures to mitigate a privacy risk include:

- Whether they overlap – that is, if one measure fails, is there another one in place that mitigates or manages that particular risk?
- Do the measures themselves introduce new privacy risks? A mitigation strategy may in fact be more privacy invasive than the risk it was designed to treat.

[38] Available at https://www.vmia.vic.gov.au/risk/risk-tools/risk-management-tools

- Do the measures have other consequences to your organisation? If the measure impacts on risk elsewhere within your organisation, you might consider consulting with those relevant areas when deciding whether or not to adopt the measure.
- Do the measures affect stakeholders, such as individuals? Some measures may be more acceptable to stakeholders than others.

15.4 For more information about identifying, evaluating and implementing measures, refer to the VPDSF *Assurance Collection*.[39]

16. Residual risk ratings and risk ownership

16.1 Once you have identified the appropriate measure(s) to mitigate and manage the identified privacy risk, it is important to reassess the impact, likelihood and residual risk ratings. The residual risk ratings assign a projected rating after a risk mitigation strategy has been applied.

16.2 Your organisation may decide to accept a privacy risk based on its residual rating. However, if your organisation is not willing to accept the privacy risk based on its residual rating, you may need to apply further measures to lower the risk. If your organisation applies additional measures, you will need to revisit the residual risk ratings and update them accordingly. The risk assessment process is therefore iterative, and may require you to reassess risk mitigation strategies and residual risk ratings until the risk is treated to an acceptable level.

16.3 If the privacy risk cannot be mitigated or managed to an acceptable level, your organisation may decide to amend aspects of the program to avoid that privacy risk altogether.

16.4 Finally, it is important to allocate an owner to each identified risk. It is the risk owner's responsibility to ensure that the risk is managed on an ongoing basis and reviewed with appropriate frequency, and that any additional actions and measures required are undertaken within a designated timeframe where appropriate.

16.5 The risk owner assigned to a particular risk may depend on the level of the risk involved. If the privacy risk is high, it may be appropriate to assign a senior officer within your organisation to ensure that the privacy risk receives a level of oversight proportionate with the risk level. In some instances, it may also be appropriate to include the privacy risk in your organisation's enterprise risk register for greater oversight and management. This helps to ensure that the privacy risk is integrated into your organisation's wider risk environment so that it is not managed in isolation, and improves visibility for stakeholders.

[39] Available at https://ovic.vic.gov.au/resource/assurance-collection/

17. Summary of risks

17.1 After conducting a privacy risk assessment, you may identify some privacy risks that cannot be mitigated. Your organisation may decide to amend the program to avoid that risk; however this may not always be possible, particularly where a function is mandated by government. Your organisation may also decide that the public benefit that will be delivered by the program outweighs the risk.

17.2 This section of the PIA template or report should outline any significant findings relating to privacy risks, as well as any privacy enhancing features of your program. If applicable, you should also list the privacy risks that cannot be mitigated, and explain why your organisation has accepted that risk – for example, explain what the public benefits are and how they outweigh the privacy risk. You may also wish to discuss what the likely public reaction to these risks will be, and how your organisation will deal with or mitigate that reaction.

Part 4

18. Action required

18.1 As you go through the process of conducting a PIA, you may identify certain actions that your organisation can implement to enhance the privacy protections of your program. For example, as a result of the process your organisation may decide to undertake stakeholder consultation, or undertake a review of any agreements or arrangements involving CSPs or third parties.

18.2 There may also be actions that arise out of the privacy risk assessment covered in Part 3 of the template. For example, there may be measures or controls that your organisation intends to implement to mitigate a particular privacy risk.

18.3 Identifying an action owner and a timeframe for the action will help to ensure that there is someone within your organisation who is responsible and accountable for completing the action.

19. Endorsement

19.1 This section covers the endorsement for the PIA template or report. It is up to you to decide whose endorsement is required or appropriate. There may be several people in your organisation who need to see or review the PIA template or report. For example, your organisation's Privacy Officer, the information security team, the program/project owner, the individual with oversight of the program and the privacy risks (if any) etc. It is also important to obtain executive support or approval of the PIA, particularly where acceptance of risk is required.

20. PIA review

20.1 It is important to note that a PIA is an iterative process. This means that you can – and should – review and update the PIA template or report as necessary, particularly if issues arise as you implement the program. Setting a date to review the PIA template or report is valuable so that any action items identified above can be monitored. Reviewing the PIA process, as well as the resulting template or report, also provides you an opportunity to review the risk mitigation strategies that you have implemented to ensure they remain effective.

21. Document information

21.1 This table covers information about the document, including the name of the document, which individual or team has ownership over the PIA template or report, who it has been distributed to, and any other related documents that are relevant to the program.

22. Document version

22.1 There will likely be several versions of the PIA template or report as you draft, amend, review and update it. It is a good idea to keep track of all the different versions, along with the version and status of the document and who authored that version or made changes. Good document control

is an important part of information management and may help prevent confusion in the future.

Appendix 1

Short guide to the Information Privacy Principles

The 10 Information Privacy Principles (IPPs) are contained in Schedule 1 to the Privacy and Data Protection Act 2014 (PDP Act). This is a short summary of the IPPs and is intended to provide a high-level guide only. For detailed privacy analysis, please refer to the full text of the IPPs.

23. IPP 1 – Collection

An organisation can only collect personal information if it is necessary to fulfil one or more of its functions. It must collect information only by lawful and fair means, and not in an unreasonably intrusive way. It must provide notice of the collection, outlining matters such as the purpose of collection and how individuals can access the information. This is usually done by providing a Collection Notice, which should be consistent with an organisation's Privacy Policy.

24. IPP 2 – Use and Disclosure

Personal information can only be used and disclosed for the primary purpose for which it was collected, or for a secondary purpose that would be reasonably expected. It can also be used and disclosed in other limited circumstances, such as with the individual's consent, for a law enforcement purpose, or to protect the safety of an individual or the public.

25. IPP 3 – Data Quality

Organisations must keep personal information accurate, complete and up to date. The accuracy of personal information should be verified at the time of collection, and periodically checked as long as it is used and disclosed by the organisation.

26. IPP 4 – Data Security

Organisations need to protect the personal information they hold from misuse, loss, unauthorised access, modification or disclosure. An organisation must take reasonable steps to destroy or permanently de-identify personal information when it is no longer needed.

27. IPP 5 – Openness

Organisations must have clearly expressed policies on the way they manage personal information. Individuals can ask to view an organisation's Privacy Policy.

28. IPP 6 – Access and Correction

Individuals have the right to seek access to their own personal information and to make corrections to it if necessary. An organisation may only refuse in limited circumstances that are detailed in the PDP Act. The right to access and correction under IPP 6 will apply to organisations that are not covered by the Freedom of Information Act 1982.

29. IPP 7 – Unique Identifiers

A unique identifier is an identifier (usually a number) that is used for the purpose of identifying an individual. Use of unique identifiers is only allowed where an organisation can demonstrate that the assignment is necessary to carry out its functions efficiently. There are also restrictions on how organisations can adopt unique identifiers assigned to individuals by other organisations.

30. IPP 8 – Anonymity

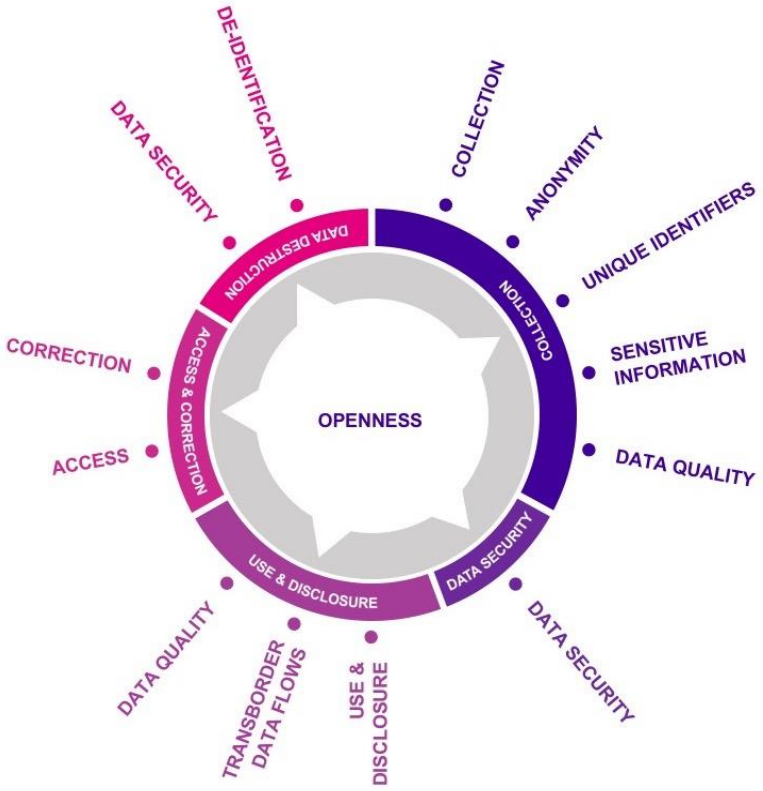
Where lawful and practicable, individuals should have the option of transacting with an organisation without identifying themselves.

31. IPP 9 – Transborder Data Flows

If an individual's personal information travels outside Victoria, the privacy protection should travel with it. Organisations can only transfer personal information outside Victoria in certain circumstances, for example, if the individual consents, or if the recipient of the personal information is subject to a law or binding scheme that is substantially similar to the Victorian IPPs.

32. IPP 10 – Sensitive Information

The PDP Act places special restrictions on the collection of sensitive information. This includes racial or ethnic origin, political opinions or membership of political associations, religious or philosophical beliefs, membership of professional or trade associations or trade unions, sexual preferences or practices, and criminal record. Organisations can only collect sensitive information under certain circumstances.



This graphic represents the IPPs throughout the information lifecycle, highlighting the principles that should be considered at each stage, starting with collection.

Document control

Version	Publish date	Detail	Author
1.0	1 May 2019	Final version published.	Policy, Office of the Victorian Information Commissioner (OVIC)
1.1	2 August 2019	Updated language around PIA to frame it as a process.	Policy, OVIC