**[Insert organisations branding/logo]**

**[Insert organisations name]**

**Privacy Impact Assessment**

**[Insert program name]**

# Introduction

Organisations are encouraged to insert their own branding and logo, and customise the template to the needs of the organisation.

A privacy impact assessment (**PIA**) is a process for analysing a program’s impact on individuals’ information privacy. Undertaking a PIA can help identify the personal information involved, identify potential privacy risks, develop risk mitigation strategies, and enhance privacy practices. If the program involves the handling of personal information, it is best practice to conduct a PIA.

Undertaking a PIA is not a compliance exercise – it is about improving organisational practice and demonstrating respect for individuals’ privacy. The questions in this template go beyond the requirements of the Information Privacy Principles (**IPPs**) contained in Schedule 1 of the *Privacy and Data Protection Act* *2014*. This is to encourage organisations to think about privacy and information management broadly, not just in the legal sense.

This PIA template has been prepared by the Office of the Victorian Information Commissioner (**OVIC**). It should be read alongside OVIC’s Privacy Impact Assessment Guide (**PIA Guide**), which contains further information on how to complete the PIA template.

This template is divided in to four parts:

* Part 1 – Program background and details
* Part 2 – Privacy analysis
* Part 3 – Privacy risk assessment
* Part 4 – Action items, endorsement, and document information.

Part 1 – Program background and details

|  |  |  |  |
| --- | --- | --- | --- |
| Program |  | | |
| Organisation |  | | |
| PIA Drafter |  | Email |  |
| Program Manager |  | Email |  |
| Privacy Officer |  | Email |  |
| Date Completed |  | | |

Description of the program and parties

### Delete this text and the text below and add a description of the program and parties. Refer to Section 1 in Part 1 of the PIA Guide for further information.

This section should include:

* a detailed description of the program and its context;
* the purpose and objectives of the program;
* how the program will work;
* the benefits or expected benefits of the program;
* why it is necessary for the organisation’s functions; and
* other parties (for example, contracted service providers) and their roles, including the types of information they will be collecting and how they will use or disclose that information.

## Scope of this privacy impact assessment

### Delete this text and the text below and add a description of the PIA scope. Refer to Section 2 in Part 1 of the PIA Guide for further information.

This section should include:

* the elements of the program that this PIA will and will not cover;
* any public interest determinations, temporary public interest determinations, information usage arrangements or certifications in place under the *Privacy and Data Protection Act 2014* related to the program;
* other PIA processes that have been undertaken that are relevant to the program; and
* where multiple parties are involved in the program, which party is covered in the PIA process.

## Legal authority

### Delete this text and the text below and describe the organisations legal authority. Refer to Section 3 in Part 1 of the PIA Guide for further information.

This section should include:

* the organisation’s legal authority to collect, use and disclose personal information for the program (under enabling legislation, the *Privacy and Data Protection Act 2014* or other legislation); and
* other legislation to consider when designing or implementing the program.

## Stakeholder consultation

### Delete this text and the text below and add a description of any stakeholder consultation process. Refer to Section 4 in Part 1 of the PIA Guide for further information.

This section should include:

* an outline of any internal and external stakeholder consultation that has been undertaken in relation to the program; and
* where relevant, a summary of the outcomes of any consultation.

## Information flow diagram

### Delete this text and the text below and insert an information flow diagram. Refer to Section 5 in Part 1 of the PIA Guide for further information.

Insert here or attach as an appendix a diagram or table that shows the flow of information involved in the program. This should indicate the systems used, the parties involved (if applicable), and the methods of transfer. Where possible, indicate the types of information that flow, between the various stages or parts of the program, and between different parties.

# Part 2 – Privacy analysis

The part identifies the privacy elements and risks the program. The PIA Guide provides guidance on responding to the questions. The right column indicates the relevant section of the PIA Guide. Some questions may not be relevant or applicable. The response should be noted as N/A where this occurs.

The assessment includes prompts to assist identifying the program’s elements and risks. There may exist elements or risks beyond each prompt, and each question should be given a broad interpretation. Identified privacy risks should be listed in Part 3. The PIA Guide contains examples of privacy risks that may arise.

## Identify the information elements

|  |  |  |  |
| --- | --- | --- | --- |
|  | *Question* | *Response* | *Guide* |
| *1* | **Does the program involve personal information?**  *List each piece of personal information that is involved in the program.* |  | *PART 2*  *Section 6* |
| *2* | **Does the program involve other information that has the potential to identify individuals?**  *This may include information that does not appear to be personal information at first glance, but which could identify individuals based on the context of the project or how the program uses the information.*  *Describe this other information and explain how it could potentially identify individuals within the context of the program.* |  | *PART 2*  *Section 6* |
| *3* | **Does the program involve sensitive information (as defined under Schedule 1 of the PDP Act)?**  *Describe the type(s) of sensitive information that is involved in the program (if any), and how the collection or use of the sensitive information is authorised either by the PDP Act or other legislation.* |  | *PART 2*  *Section 6*  *Section 7* |
| *4* | **Does the program involve health information?**  *If the answer is yes, please refer to the Health Records Act 2001 or consult with the Health Complaints Commissioner in relation to health information (and where applicable, the Office of the Australian Information Commissioner).* |  | *PART 2*  *Section 6* |
| *5* | **Does the program involve information that has previously been de-identified?**  *Describe the type(s) of de-identified information that is involved in the program (if any), and the potential for re-identification.* |  | *PART 2*  *Section 6* |

**Collection of personal information**

|  |  |  |  |
| --- | --- | --- | --- |
| *6* | **Is all the personal information collected necessary for the program?**  *Explain why all the information collected is necessary for the program.* |  | *PART 2*  *Section 7* |
| ***Privacy risk: If some personal information is not necessary for the program, consider whether there is a risk of overcollection.*** | | | |
| *7* | **Does the organisation need to collect information that identifies an individual for the purposes of the program, or can individuals remain anonymous?** |  | *PART 2*  *Section 7* |
| *8* | **If individuals can remain anonymous, will the organisation be collecting indirect identifiers, such as demographic information?** |  | *PART 2*  *Section 6* |

**Method and notice of collection**

|  |  |  |  |
| --- | --- | --- | --- |
| *9* | **How will the personal information be collected?**  *Describe the means by which the information will be collected. If personal information is collected via a third party platform, explain whether the platform will also be collecting that information* |  | *PART 2*  *Section 7* |
| ***Privacy risk: Consider whether the method of collection is fair and not unreasonably intrusive.*** | | | |
| *10* | **Is the personal information collected directly from the individual?** |  | *PART 2*  *Section 7* |
| *11* | **Will the individual be notified about the collection of their personal information?**  *Describe the steps taken to provide notice to the individual OR explain why notice will not be provided to the individual. Include a link or attach collection notices where appropriate.* |  | *PART 2*  *Section 7* |
| *12* | **Will any personal information about the individual be collected indirectly from another source?**  *Describe how and from which other sources the personal information will be collected.* |  | *PART 2*  *Section 7* |
| ***Privacy risk: If personal information is indirectly collected, consider whether there is a risk of the information being inaccurate, out of date or incomplete. Consider the impact on individuals if they are not made aware that their information is being collected from another source.*** | | | |
| *13* | **Will the individual be notified that their personal information has been collected from another source?**  *Describe the steps taken to provide notice to the individual OR explain why notice will not be provided to the individual. Include a link or attach collection notices where appropriate.* |  | *PART 2*  *Section 7* |

**Unique identifiers**

|  |  |  |  |
| --- | --- | --- | --- |
| *14* | **Will the program assign a unique identifier or collect a unique identifier assigned by another organisation to adopt as the organisation’s own?**  *Describe the unique identifier, the purpose for assigning or collecting it, and how this is authorised by either the PDP Act or other legislation.* |  | *PART 2*  *Section 7* |
| *15* | **Does the program require an individual to provide a unique identifier?**  *Explain why or how the provision of a unique identifier is necessary for the program.* |  | *PART 2*  *Section 7* |

**Quality of personal information**

|  |  |  |  |
| --- | --- | --- | --- |
| *16* | **What steps will the organisation take to ensure the personal information collected is accurate, complete, and up to date?** |  | *PART 2*  *Section 9* |
| ***Privacy risk: If there are inadequate or no steps taken, consider whether there is a risk that the information will be inaccurate, incomplete or out of date.*** | | | |

**Security of personal information**

|  |  |  |  |
| --- | --- | --- | --- |
| *17* | **Are there security measures in place (existing or intended) to protect the personal information collected and used for this program?**  *List the policies, procedures, or controls that the organisation implements to protect personal information. Please indicate how these measures will be governed. Include links or attachments where appropriate* |  | *PART 2*  *Section 8* |
| *18* | **Where and how will personal information be stored?**  *Describe the format in which the personal information will be stored (e.g. electronic, hard copy etc.) and where it will be stored (e.g. internally, external provider, cloud, third party platform etc.)* |  | *PART 2*  *Section 8* |
| *19* | **Who will have access to the personal information?**  *Describe the positions that will have access how access is gained or controlled, and whether it is logged.* |  | *PART 2*  *Section 8* |
| *20* | **Has a separate security risk assessment been completed?**  *If so, please refer to or attach a copy of the assessment to this PIA. If not, OVIC suggests a security risk assessment is completed.* |  | *PART 2*  *Section 8* |
| ***Privacy risk: If there are inadequate or no security measures in place, consider whether there is a risk that the information will not be properly protected, leading to loss, misuse, or unauthorised access, modification or disclosure.*** | | | | |

**Primary and additional uses and disclosures of personal information**

|  |  |  |  |
| --- | --- | --- | --- |
| *21* | **Is the personal information (including any sensitive information) involved in this program used or disclosed for the main or primary purpose for which it was collected?**  *Describe what personal information will be used or disclosed, and for what purposes.* |  | *PART 2*  *Section 9* |
| *22* | **Does the program use or disclose personal information (including sensitive information) for a new or additional purpose other than the original purpose of collection?**  *Describe the new/additional purpose for the use or disclosure of the information and explain how it is authorised, by either the PDP Act or other legislation. If relying on IPP 2.1(a), explain how the secondary use or disclosure is related to the primary purpose of collection.* |  | *PART 2*  *Section 9* |
| ***Privacy risk: If relying on IPP 2.1(a) to use personal information for a secondary purpose, consider whether individuals would reasonably expect their information to be used for that secondary purpose. If relying on IPP 2.1(b) to use personal information for a secondary purpose, ensure the individual’s consent is meaningful.*** | | | |
| *23* | **Will the individual be notified of the additional use(s) of their personal information?**  *Explain how the individual will be given notice of the secondary use(s) of their information, or why notice of the secondary use will not be provided.* |  | *PART 2*  *Section 9* |

**Transfer and sharing of personal information**

|  |  |  |  |
| --- | --- | --- | --- |
| *24* | **Will any personal information be shared outside of the organisation?**  *Describe:*   * *what information will be shared;* * *with whom the information will be shared;* * *the frequency of the disclosure;* * *how the information will be shared; and* * *how the disclosure is authorised by either the PDP Act or other legislation.*   *Identify whether any information sharing agreements are or will be in place.* |  | *PART 2*  *Section 9* |
| *25* | **Will any personal information be transferred outside Victoria?**  *Describe what information will be transferred, to whom the information will be transferred, in which jurisdiction the information will be stored, and how the information will be transferred. Explain how the transfer is authorised by either the PDP Act or other legislation.* |  | *PART 2*  *Section 9* |

**Other considerations relating to use and disclosure**

|  |  |  |  |
| --- | --- | --- | --- |
| *26* | **Does the program use or disclose a unique identifier assigned by another organisation?**  *Describe the unique identifier and how it will be used or disclosed, and whether this is authorised by either the PDP Act or other legislation.* |  | *Para No.*  *PART 2*  *Section 9* |
| *27* | **Will any data matching occur as part of this program? This includes matching datasets within the program, or matching to other datasets external to the program.**  *If so, explain the purpose for the data matching, what personal information will be matched and what other datasets it will be matched with, and what the combined dataset will be used for.* |  | *PART 2*  *Section 9* |
| *28* | **Will any personal information be de- identified as part of the program?**  *Describe the purpose for de-identifying personal information for the program, the method of de-identification, how the de-identified information will be used, and the potential for re-identification.* |  | *PART 2*  *Section 6* |
| ***Privacy risk: If personal information is de-identified, consider whether there is a risk that the information can be re-identified. For example, de-identified information may be re-identifiable when matched to other information, or because of the way the de-identified information is used in the context of this program.*** | | | |
| *29* | **What will be done to ensure the ongoing accuracy, completeness, and currency of the personal information?**  *Describe the steps that will be taken, or the measures that are in place, to ensure the ongoing integrity of the information.* |  | *PART 2*  *Section 9* |

**Management of personal information**

|  |  |  |  |
| --- | --- | --- | --- |
| *30* | **Is there a document available to the public that sets out the organisation’s policies for the management of personal information, such as a privacy policy?**  *Identify the document(s) and provide a link where available or include as an attachment to this PIA.* |  | *PART 2*  *Section 10* |
| *31* | **Will the document be updated to reflect the new collection or use of personal information for the purposes of this program?**  *If not, explain why.* |  | *PART 2*  *Section 10* |
| *32* | **Is there a way for a person to find out the types of personal information the organisation holds about them? Can an individual find out the purposes for which it is held, and how the organisation collects, holds, uses and discloses that information?**  *Describe the steps and provide links where relevant.* |  | *PART 2*  *Section 10* |

**Access and correction of personal information**

|  |  |  |  |
| --- | --- | --- | --- |
| *33* | **How can individuals request access to, or correct their personal information?**  *Identify the avenues available for individuals to request access to or correction of their personal information, and who is responsible for handling such requests.* |  | *PART 2*  *Section 10* |
| ***Privacy risk: If engaging third parties such as contracted service providers, consider whether there are arrangements in place to allow access and correction of personal information held by third parties. If not, there may be a risk that individuals cannot access or correct their personal information.*** | | | |

**Retention and disposal of personal information**

|  |  |  |  |
| --- | --- | --- | --- |
| *34* | **How long will the personal information be kept for?**  *Describe any relevant retention and disposal schedules or policies, including those issued by the Keeper of Public Records or those in other legislation.* |  | *PART 2*  *Section 11* |
| *35* | **How will personal information be destroyed once it is no longer required?**  *Describe the method of destruction and explain how that method is secure.* |  | *PART 2*  *Section 11* |
| *36* | **As an alternative to destroying personal information, will any personal information be de-identified once it is no longer required?**  *Describe the method of de-identification that will be used and the purposes to which the de-identified information will be put.* |  | *PART 2*  *Section 11* |
| ***Privacy risk: If de-identifying personal information once it is no longer required, consider whether there is a risk that the information can be re-identified.*** | | | |
| *37* | **If applicable, what will happen to personal information held by third parties (such as contracted service providers, cloud storage, third party platforms etc.)?**  *Describe any arrangements (for example, any contractual provisions) in relation to third parties’ obligations to retain and dispose of personal information.* |  | *PART 2*  *Section 11* |
| ***Privacy risk: If there are no arrangements in place relating to third parties’ retention and disposal of personal information, consider whether there is a risk that personal information will be held indefinitely.*** | | | |

**Other considerations**

|  |  |  |  |
| --- | --- | --- | --- |
| *38* | **Who can individuals complain to if they have concerns about the handling of their personal information?**  *Identify the avenues (internal and external) for making a privacy complaint, including who is responsible for complaint handling.* |  | *PART 2*  *Section 12* |
| *39* | **Does the organisation have a data breach response plan in place?**  *If so, describe at a high level the steps that the organisation will take in the event of a data breach.* |  | *Para No.*  *PART 2*  *Section 12* |
| *40* | **Will any training be provided to staff to ensure the appropriate collection and handling of the personal information collected for this program?**  *Describe the type of training staff will receive.* |  | *PART 2*  *Section 12* |
| *41* | **Will the program be evaluated against its objectives?**  *Describe who will evaluate the program, at what point in the program evaluation will occur, and how often.* |  | *PART 2*  *Section 12* |
| *42* | **Does the program comply with the organisation’s other information handling or information management policies?** |  | *PART 2*  *Section 12* |
| *43* | **Will this PIA be published?** |  |  |
| *44* | **Are there any other broader privacy considerations associated with this program?** |  | *PART 2*  *Section 12* |
| *45* | **Has the organisation’s privacy officer been consulted?**  *The organisation’s privacy officer should be consulted.* |  |  |

**Part 3 – Privacy risk assessment**

This part lists any privacy risks that have been identified as part of the analysis in Part 2. Refer to **Part 3** of the PIA Guide for guidance on completing the risk assessment table.

|  |  |  |
| --- | --- | --- |
| **Were any privacy risks identified in the privacy analysis completed in Part 2 of this PIA?** | Yes  Enter each privacy risk in the risk assessment table below. | No  Proceed to Part 4 of this PIA. |

**Note:** This is a standard risk assessment table. It is recommended that the organisation’s own risk assessment framework and table is inserted here. Only use the provided table if the organisation does not have its own risk assessment framework.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | *Description of risk* | *Consequence rating* | *Likelihood rating* | *Overall risk rating* | *Accept* | *Risk management strategy* | *Residual consequence rating* | *Residual likelihood rating* | *Residual risk rating* | *Owner* |
| *1* | ‘The risk of... event … caused by … how … resulting in … impact(s) …’ | What is the impact of the risk? | What is the likelihood of the risk occurring? | What is the overall risk rating on? | Is the risk accepted or not? | Detail the measures taken (or to be taken) to mitigate and manage the risk. Where relevant, include the timeframe for implementing the strategy and identify who is responsible for it. | What is the impact of the risk after security measures have been applied? | What is the likelihood of the risk occurring after security measures have been applied? | What is the overall risk rating after security measures have been applied? | Who is responsible for monitoring and reviewing the risk? |

\*\*Add more rows by clicking in the bottom right cell and pressing ‘tab’

# Part 4 – Action items, endorsement, document information

This part details any action items identified, endorsement of the PIA, and document information. Refer to **Part 4** of the PIA Guide for more information.

## Action items

Action items identified in Parts 2 or 3 are listed here, along with the owner of the action and any timeframe within which the action needs to be completed.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | *Action* | *Owner* | *Timeframe* | *Completed* |
| *1* |  |  |  |  |
| *2* |  |  |  |  |

## \*\*Add more rows by clicking in the bottom right cell and pressing ‘tab’

## Endorsement

The required endorsements for this PIA are listed below. This may include the program manager, a privacy officer, executive business owner, or any other responsible person.

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

## \*\*Add more rows by clicking in the bottom right cell and pressing ‘tab’

## Document information

|  |  |
| --- | --- |
| *Document title* |  |
| *Document location* |  |
| *Document owner* |  |
| *Document distribution* |  |
| *Related documents* |  |
| *Next review* |  |
| *Document version* |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Template Version Control – D20/6441** | | | |
| **Version** | **Published** | **Detail** | **Author** |
| 1.0 | 1 / 5 / 2019 | Template published. | Policy Team, OVIC |
| 1.1 | 2 / 7 / 2019 | * Updated language of template to frame it as a process. * Updated language of template questions 1 – 5, 17, 22 and 28. | Policy Team, OVIC |
| 1.2 | 15 / 4 / 2021 | * Updated language of template and minor formatting and layout amendments. | Policy Team, OVIC |