Office of the Victorian Information Commissioner

Privacy Impact Assessment

Template

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. • Updated wording of Questions 1 – 5, 17, 22 and 28.	Policy, OVIC

Privacy Impact Assessment Template

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

Undertaking a PIA is not just a compliance exercise – it is about improving organisational practice and demonstrating respect for individuals' privacy. The questions in this template go beyond the requirements under the Information Privacy Principles (**IPPs**) 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 Accompanying guide, which contains further information on how to complete this template.

Name of Program			
Name of Organisation			
Date		PIA Version Number	
PIA Drafter		Email	
Program Manager		Email	
Is your organisation a law enforcement agency as defined in section 3 of the *Privacy and Data Protection Act 2014*?			
Has the Privacy Officer of your organisation been consulted in the drafting of this PIA?			
Privacy Officer		Email	

Part 1

Description of the program and parties

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

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 expected benefits of the program and why it is necessary for your organisation's functions; and
- other parties (e.g. contracted service providers) and their roles, including the types of information they will be collecting and how they will use or disclose that information.

For more information, refer to section 1 in Part 1 of the accompanying guide (pages 10 – 11).

Scope of this privacy impact assessment

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

This section should include:

- the elements of the program that this PIA process 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* (**PDP Act**) related to this program;
- other PIA processes that have been undertaken that are relevant to this program; and
- where multiple parties are involved in a program, which party is covered in the PIA process.

For more information, refer to section 2 in Part 1 of the accompanying guide (pages 12 – 13).

Legal authority

[Delete the text below and add your description of your legal authority.]

This section should include:

- your organisation's legal authority to collect, use and disclose personal information for this program (under enabling legislation, the PDP Act or other legislation); and
- other legislation to consider when designing or implementing the program.

For more information, refer to section 3 in Part 1 of the accompanying guide (page 13).

Stakeholder consultation

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

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.

For more information, refer to section 4 in Part 1 of the accompanying guide (page 14).

Information flow diagram

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

Please insert below, or attach as an appendix, a diagram or table that shows the flow of information involved in this program, indicating the systems used and different 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.

For more information, refer to section 5 in Part 1 of the accompanying guide (pages 14 – 15).

Part 2

Privacy analysis table

The following table assesses the privacy implications of your program. For guidance on responding to the questions, refer to the relevant section of the Privacy Impact Assessment Accompanying guide indicated in the last column.

Some questions in the table include prompts to assist you to identify privacy risks. However, you should think about potential privacy risks even when not explicitly prompted in the table and note any identified privacy risks in Part 3 of this template. You may also refer to the PIA guide for examples of potential privacy risks that may arise as you complete the privacy analysis.

Depending on your answer to a particular question, subsequent related questions may not be relevant or applicable. Where this is the case, please note this in your response.

Identifying information elements

#	Question	Response	PIA guide
1	**Does the program involve personal information?** *List each piece of personal information that is involved in the program.*		*6.2 – 6.5* *Pages 16 – 17*
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 your program.*		*6.6* *Page 17*

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.*		*6.7 – 6.9* *Pages 17 – 18,* *7.4* *Page 20*
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).*		*6.10* *Page 18*
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.*		*6.13 – 6.18* *Page 19*

Collection of personal information

6	**Is all the personal information collected necessary for the program?** *Explain why all the information collected is necessary for your program.*		*7.2 – 7.3* *Page 20*
	Privacy risk: If some personal information is not necessary for the program, consider whether there is a risk of overcollection.		
7	**Do you need to collect information that identifies an individual for the purposes of the program, or can individuals remain anonymous?**		*7.5* *Page 21*

8	**If individuals can remain anonymous, will you be collecting indirect identifiers, such as demographic information?**		*6.3 – 6.4* *Page 17*

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*		*7.7 – 7.8* *Page 21*
	Privacy risk: Consider whether your method of collection is fair and not unreasonably intrusive.		
10	**Is the personal information collected directly from the individual?**		*7.9* *Page 21*
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.*		*7.13 – 7.16* *Page 22*
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.*		*7.10 – 7.11* *Pages 21 – 22*

	Privacy risk: If you are collecting personal information indirectly, 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.*		*7.15* *Page 22*

Unique identifiers

14	**Will the program assign a unique identifier or collect a unique identifier assigned by another organisation to adopt as your 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.*		*7.18 – 7.19* *Page 23*
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.*		*7.20 – 7.21* *Page 23*

Quality of personal information

16	**What steps will you take to ensure the personal information collected is accurate, complete, and up to date?**		*9.16 – 9.18* *Pages 27 – 28*

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 your organisation implements to protect personal information. Please indicate how these measures will be governed. Include links or attachments where appropriate*		*8.2 – 8.9* *Pages 23 – 25*
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.)*		*8.2 – 8.9* *Pages 23 – 25*
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.*		*8.2 – 8.9* *Pages 23 – 25*
	Have you completed a separate security risk assessment? *If so, please refer to or attach a copy of the assessment to this PIA. If not, OVIC suggests you complete a security risk assessment.*		*8.10 – 8.11* *Page 25*

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.*		*9.2* *Page 25*
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.*		*9.3 – 9.4* *Page 26*
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.*		*9.4* *Page 26*

Transfer and sharing of personal information

24	**Will any personal information be shared outside of your 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, and how disclosures will be recorded.*		*9.6 – 9.7* *Page 26*
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.*		*9.8 – 9.9* *Page 26*

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.*		*9.10 – 9.11* *Page 27*

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.*		*9.13 – 9.14* *Page 27*
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.*		*6.14 – 6.18* *Page 19*
	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	**How will you ensure the ongoing accuracy, completeness, and currency of the personal information used in this program?** *Describe the steps that will be taken, or the measures that are in place, to ensure the ongoing integrity of the information.*		*9.16 – 9.18* *Page 27 – 28*

Management of personal information

30	**Is there a document available to the public that sets out your 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.*		*10.2, 10.5* *Page 28*

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.*		*10.3* *Page 28*
32	**Is there a way for a person to find out the types of personal information your organisation holds about them? Can you tell them the purposes for which it is held, and how your organisation collects, holds, uses and discloses that information?** *Describe the steps and provide links where relevant.*		*10.4 – 10.5* *Page 28*

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.*		*10.6 – 10.7* *Page 29*

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.*		*11.2 – 11.3* *Pages 29 – 30*

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.*		*11.4* *Page 30*
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.*		*11.6 – 11.7* *Page 30*

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.*		*11.9 – 11.10* *Pages 30 – 31*

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.*		*12.2 – 12.4* *Page 31*

39	**Does your organisation have a data breach response plan in place?** *If so, describe at a high level the steps that your organisation will take in the event of a data breach.*		*12.5 – 12.6* *Pages 31 –32*
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.*		*12.7* *Page 32*
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.*		*12.8* *Page 32*
42	**Does the program comply with your organisation's other information handling or information management policies?**		*12.9* *Page 32*
43	**Will this PIA be published?**		*Page 7*
44	**Are there any other broader privacy considerations associated with this program?**		*12.10* *Page 32*

Part 3

Risk assessment table

This section of the template lists any privacy risks that may have been identified during the privacy analysis in Part 2. The following table is a standard risk assessment template.
OVIC recommends that you use your organisation's own risk assessment framework where possible. You may delete the table below and insert your own risk assessment table.

For guidance on completing the risk assessment table, refer to sections 13 – 16 in Part 3 of the Accompanying guide (pages 33 – 35).

#	*Description of the risk*	*Impact rating*	*Likelihood rating*	*Risk rating*	*Accept risk (Y/N)*	*Risk management strategy*	*Residual impact rating*	*Residual likelihood rating*	*Residual risk rating*	*Risk owner*
1	*'The risk of... event ... caused by ... how ... resulting in ... impact(s) ...'*	*Rate the impact of the risk to your organisation .*	*Deter- mine the likelihood of the risk occurring.*	*Assign an overall risk rating.*	*Identify whether your organi - sation will accept the risk or not.*	*Detail the measures taken (or to be taken) to mitigate and manage the risk. Where relevant, include the timeframe for implementing the strategy and identify who is responsible for it.*	*Rate the impact of the risk to your organisati on after security measures have been applied.*	*Rate the likelihood of the risk occurring after security measures have been applied.*	*Assign an overall risk rating after security measures have been applied.*	*Assign a risk owner who will be responsible for monitoring and reviewing the risk.*
#										

#	*Insert additional rows as required*										

Summary of risks

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

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

- Significant findings in relation to privacy risks, including any risks that cannot be mitigated. What is the likely public reaction to these risks? Are these risks outweighed by the public benefit that will be delivered by the program?
- Privacy enhancing features of the program.

For more information, refer to section 17 in Part 1 of the Accompanying guide (page 36).

Part 4

The final section of this template covers any next steps that you may need to complete after undertaking the PIA process, endorsement of the PIA template or report, and document information. For more information refer to sections 18 – 22 in Part 4 of the Accompanying guide (pages 33 – 38).

Action required

Where relevant, list the action items that need to be completed, who is responsible for that action, and any timeframes within which the action needs to be completed. These actions may be items that are identified during the privacy risk assessment, or over the course of undertaking the PIA process more broadly.

#	*Action*	Action Owner	*Timeframe*	*Date Action completed*

Endorsement

List any endorsements required for this PIA template or report. This may include the program manager or individual(s) with oversight over the program and privacy risks (if any), your organisation's Privacy Officer, and executive business owner.

Name	*Position*	*Signature*	*Date*

Document information

Document title	
Document owner	*Identify the branch, unit, team or individual within your organisation that has ownership over this document.*
Document distribution	*List any individuals or parties to whom this PIA template or report has been distributed. If your PIA template or report has been published, you may also include details of publication here (e.g. date of publication, website where published).*
Related documents	*List any other relevant documents that relate to this program, for example:* • *other relevant PIAs that have been undertaken (e.g. if this PIA only covers one aspect of the program)* • *security risk assessment* • *contract review* • *procurement requirements*

PIA review

Note when the PIA template or report will be reviewed to ensure that it is still accurate. If required, the PIA template or report should be updated to account for any changes to the program.

Date review should be completed by	

Document version

Version number	*Date*	*Document status*	*Author*
		e.g. 'draft' or 'final'	

Further Information

Contact Information

t: 1300 00 6842
e: enquiries@ovic.vic.gov.au
w: ovic.vic.gov.au

Disclaimer

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