

Consultation Draft

Privacy Threshold Assessment

A privacy threshold assessment is a preliminary assessment to help an IPP entity determine whether it should undertake a PIA. The outcome of a privacy threshold assessment will, therefore, be a recommendation about whether to conduct a PIA. It is not a “mini” PIA to determine the level of risk and identify mitigation strategies.

You can use this template to help you decide whether a Privacy Impact Assessment (PIA) is required to be conducted under the *Privacy and Responsible Information Sharing Act 2024* (WA) (PRIS Act) for a particular function or activity or whether there is another reason for conducting a PIA.

If your proposed activity relates to an information sharing agreement under Part 3 of the PRIS Act, please see [Chief Data Officer Guideline: Assessments for data sharing under the PRIS Act](#). You can use this template to determine whether the activity is likely to have a significant impact on the privacy of individuals.

Use of this template is **not** mandatory.

IMPORTANT: This template should be read with the OIC’s guidance ‘Do I need to do a Privacy Impact Assessment?’

Instructions

Part 1: Provide an overview of the function or activity. Complete and proceed to Part 1.

Part 2: Identify whether personal information will be handled as part of the function or activity and, if yes, the type/s of personal information involved. If the function or activity involves the handling of personal information, proceed to Part 2.

Part 3: Identify whether the function or activity is *‘likely to have a significant impact on the privacy of individuals’*. For each factor described in Part 2, indicate whether it is relevant to the function or activity and provide notes in the space provided to support your selection. Responses to the questions in Part 2 should inform the recommendation of whether a PIA is required, taking into account any other relevant factors.

Part 4: Identify when a PIA is required under the PRIS Act or whether there is another reason for conducting a PIA. Complete and proceed to the recommendation.

Part 5: Set out your recommendation about whether a PIA is required.

Remember, this template has not been designed as a checklist to replace your judgement, nor should it override your knowledge of the function or activity. It is a tool to help you think through the impacts of the proposed function or activity and decide whether to conduct a PIA.

Part 1: Details of function or activity

IPP entity	
Name of function or activity	
Date	
Threshold assessment completed by	
Brief description of the function or activity	

Part 2: Personal information

Is personal information handled?

Under the PRIS Act the definition of personal information has a broad meaning. For more information please see: [What is personal information?](#)

- ☐ Yes Complete the description of the types of personal information below AND continue to Part 2.
- ☐ No It is not necessary to complete a PIA. Record your recommendation in Part 3

Describe the personal information to be handled as part of the function or activity

Describe all the types of personal information that will be handled as part of the function or activity.

Part 3: Determining the potential for a significant impact

Whether a function or activity will have a significant impact on the privacy of individuals will depend on the circumstances. Sometimes a single factor may be enough to indicate a PIA should be performed and other times multiple factors together indicate a likelihood of significant privacy impact.

Will the function or activity involve:	Yes	No
Handling personal information on a large scale? Consider the number of individuals who will be, or could be, impacted by the function or activity. Other factors indicating personal information will be handled at a large scale include the volume and variety of personal information involved, the duration of the function or activity (including whether the amount of personal information to be handled is likely to increase over time) and the geographical coverage of the function or activity. Notes:	☐	☐
Handling sensitive personal information? Sensitive personal information includes information relating to an individual's racial or ethnic origin, gender identity, sexual orientation, political opinions and associations, religious beliefs, trade union membership, or criminal record. It includes health, genetic or genomic and biometric information. You should answer yes where the function or activity might enable sensitive information to be inferred or derived from other personal information handled. Notes:	☐	☐
Handling personal information of children or vulnerable individuals? Consider whether the function or activity involves the personal information of individuals who may be more susceptible to harm or who are likely to be disproportionately impacted by the handling (or mishandling) of their personal information. This may include children and individuals whose age, disability, ethnicity, religious or political convictions, impairments or education may affect their ability to understand, exercise or protect their own privacy rights. Notes:	☐	☐

Will the function or activity involve:	Yes	No
Handling personal information without the individual's knowledge? Consider whether the function or activity involves collecting, using or disclosing the personal information of individuals without their knowledge. This could include secondary use or disclosure of personal information. Notes:	☐	☐
Tracking of individuals? Tracking may include tracking an individual's geolocation, behaviour or preferences. Notes:	☐	☐
Inferring personal information relating to individuals? Consider whether the function or activity involves generating personal information relating to an individual. This may include using personal information to predict an individual's behaviour or preferences. It may also include profiles generated from aggregated information. Notes:	☐	☐
Data linkage or data integration? Consider whether the function or activity involves: <u>Data Linkage:</u> Assigning an identifier to enable related separate records to the same individual, family, place, event or matter, or <u>Data Integration:</u> combining or collating information from two or more data sets Notes:	☐	☐

Will the function or activity involve:	Yes	No
Automated decision-making or artificial intelligence? Automated decision-making (ADM) is where a computer system (including an AI system) is used to automate all or part of a decision-making process. This may include simple pre-programmed rules-based systems where decisions are easy to explain, or more complex systems relying on predictive models where the reasons for the decision are opaque and often hard to explain. Consider whether the function or activity involves using an ADM to automate all or part of a decision-making process. <i>Note: if the activity or function involves ADM you will likely also be required to complete an ADM assessment under IPP 10,</i> Notes:	☐	☐
Using technology in a novel way? Consider whether the activity involves using new technology to handle personal information or using existing technology in a new way. Notes:	☐	☐
Disclosure of personal information to another entity? This might include disclosure of personal information to another IPP entity including a contracted service provider or another third party. Consider the volume and sensitivity of the personal information that will be disclosed (record this in the notes section below). Notes:	☐	☐
Using personal information to make a decision that affects an individual's rights, entitlements, interests or liabilities, or otherwise has a significant effect on an individual's life circumstances, opportunities, behaviour or wellbeing? Consider whether the activity involves making a decision about an individual or group of individuals that could have any serious or lasting impacts. Notes:	☐	☐

Will the function or activity involve:	Yes	No
Handling personal information in a way that could result in personal harm? Consider the potential consequence for individuals whose personal information is handled as part of the function or activity. Harm may include physical or psychological harm, injury to feelings, humiliation, discrimination, financial loss, identity theft or limiting access to a service.	☐	☐
Notes:		
Handling personal information in a way that could result in collective harm? Consider whether handling personal information may have a collective impact on a particular group of individuals, community or the public more broadly. Consider both the immediate impact as well as any potential broader societal or long-term impacts. Collective privacy impacts may be more likely where the function or activity involves issues of public concern.	☐	☐
Notes:		
Any other factors that may have a significant impact on the privacy of individuals? Consider if there are any other relevant factors that have not otherwise been addressed.	☐	☐
Notes:		

Outcome

Taking into account the responses in this part and any other relevant matters, is the function or activity likely to have a significant impact on the privacy of individuals?

- ☐ **Yes** The function or activity is likely to have a significant impact on the privacy of individuals. Continue to Part 2
- ☐ **No** The function or activity is not likely to have a significant impact on the privacy of individuals. Continue to recommendation

Part 4: Deciding when to do a PIA

A PIA must be conducted:

- before an IPP entity first performs a high privacy impact function or activity, or
- when an IPP entity makes a significant change to the way in which personal information is handled as part of a high privacy impact function or activity, or
- before entering into an information sharing agreement if the activity is likely to have a significant impact on privacy, involves data integration or data linkage or any of the proposed recipients is an external entity.

Even where a PIA is not required under the PRIS Act, an IPP entity may also choose to conduct a PIA to understand its privacy risk exposure and identify how it is meeting its obligations under the IPPs. This is particularly important in relation to legacy activities where the privacy risks have not previously been formally assessed.

Which of the following apply?

- ☐ This is the first time the function or activity will be performed.
- ☐ This is an existing function or activity but there is a significant change to the way personal information is being handled.
- ☐ The activity is related to an information sharing agreement under Part 3 of the PRIS Act
- ☐ This function or activity would benefit from a PIA for another reason.
- ☐ Circumstances do not require a PIA - include your reasoning in the notes below.

Notes:

Part 5: Recommendation

Considering the responses in Part 2 and Part 3 of this template and all other relevant context, is a PIA recommended for this function or activity?

- ☐ Yes Document reasons why a PIA is required.
- ☐ No Outline reasons why a PIA is not required. If you have ticked “yes” for any of the responses in Part 2 but have determined that a PIA is not required document the reasons for the decision.

Notes:



Office of the
**Information
Commissioner**
Western Australia

Address: Albert Facey House, 469 Wellington St, Perth WA 6000, Australia

Website: www.oic.wa.gov.au • **Telephone:** +61 8 6551 7888

Freecall (WA country): 1800 621 244 • **Email:** info@oic.wa.gov.au