**NOTE:**

This template is provided by the Office of the Information Commissioner (OIC) as an example of the content that is typically included in a PIA Report. It is a guide only. You may need to adapt the template to meet your agency’s needs or build on the template to include additional information due to the size and complexity of the project.

If you are unsure whether to complete a Privacy Impact Assessment (PIA), you can complete the screening questions in OIC’s [Threshold Privacy Assessment](https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process/undertaking-a-privacy-impact-assessment). If you answer yes to any of the questions, the project will benefit from a PIA.

This template is based on the Information Privacy Principles (IPPs) and as such, is suitable for use by agencies other than health agencies. If your agency is a health agency, please use the template which is based on the National Privacy Principles.

Instructions and tips for completing the report are provided in blue italicised text. Please delete this text as you complete each section.

Feedback on suggested improvements to this template or your experience using the template is most welcome. Please send feedback to [enquiries@oic.qld.gov.au](mailto:enquiries@oic.qld.gov.au) or contact OIC’s Enquiries Service on (07) 3234 7373.

<Project name>

**Privacy Impact Assessment Report**

<Day> <Month> <Year>

## **Document information**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date PIA completed: |  | | | |
| Status: | New PIA | Update. Date of previous version: | | |
| Prepared by: |  | | | |
| Position: |  | | | |
| Email: |  | | Telephone: |  |

## **Endorsement and approval**

Project manager:

I **recommend** the project proceeds as proposed in this document.

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Name: |  | | |
| 1. Position: |  | | |
| 1. Signature |  | 1. Date: |  |

The following officer/s have **endorsed** this document:

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Name: |  | | |
| 1. Position: |  | | |
| 1. Signature |  | 1. Date: |  |

*Add further names as required*

Project Executive/Steering Committee/senior management:

I **agree** to the project proceeding as proposed in this document.

|  |  |  |  |
| --- | --- | --- | --- |
| Name: |  | | |
| Position: |  | | |
| Signature |  | 1. Date: |  |
| 1. Comments: | | | |

## **Introduction**

## **Purpose**

This Privacy Impact Assessment (PIA) Report:

* identifies possible impacts on the privacy of individuals' personal information; and
* recommends options for mitigating or minimising any negative impacts.

## **Applicable legislation**

This PIA analyses the privacy impacts of collecting, storing, using and disclosing personal information for the purposes of <the project> against the privacy principles set out in the *Information Privacy Act 2009* (Qld) (IP Act).

*If your agency’s enabling legislation or other legislation explicitly requires, permits or limits the collection, use or disclosure of personal information involved in this project, you should also cite the legislation and relevant sections within that act.*

## **Project description**

*Explain the project and what it intends to achieve by addressing the following key points:*

* *what the project will deliver*
* *why the project is needed*
* *the benefits to the agency or the community; and*
* *whether the project is part of a program of related projects.*

*The term ‘project’ is used broadly in this context. It is intended to cover the full range of activities and initiatives that may have privacy implications, such as new systems, processes or practices for handling personal information, new legislation or policies, or an information sharing initiative.*

## **Scope of the PIA**

*If applicable, explain what part or stage of the project the PIA covers and, if necessary, what it does not cover.*

## **Review**

*In the case of a large or complex project, the PIA may need to be reviewed a number of times throughout the project’s lifecycle to ensure that its findings continue to be relevant. If applicable, outline any dates or milestones that will be used as a checkpoint to review whether anything significant has changed since this PIA was completed.*

## **Personal information flows**

This section explains how personal information will flow through the agency’s systems and processes as a result of the output or deliverable to be produced by the project. It describes:

* what personal information will be collected and how it will be used and disclosed
* who will have access to it; and
* how it will be stored and protected.

*Describe what personal information is involved and document how this information will flow through the proposed new system or process. For example:*

* *What is the nature of the information being collected and who is it collected from?*
* *How will the information be collected?*
* *How will it be stored and what safeguards will be put in place to protect it?*
* *Who will have access to the information?*
* *What will the personal information be used for and by whom?*
* *Will the personal information be routinely disclosed and if so, to whom will it be given and for what purpose?*
* *How can individuals seek access or amendment to their personal information?*
* *How long will the information need to be retained?*

*Keep in mind that personal information includes any information or opinion about a living individual who is or can reasonably be identified[[1]](#footnote-1).*

*There is no ‘one size fits all’ approach to documenting the flow of information. The following table is one example of how you could describe the information flows. You may prefer to use a diagram or business process map. The approach will depend on the complexity of the project’s information flows.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Business process/activity**  *(For example, an individual applies for permit or licence)* | **Components of personal information**  *(For example, name, date of birth, address)* | **Collection**   * *From?* * *By who?* * *How?* * *Lawful authority (if any)?* | **Storage**   * *How?* * *Where?* * *By who?* * *For how long?* | **Use**   * *By who?* * *Why?* * *When?* * *How?* * *Lawful authority (if any)?* | **Disclosure**   * *By who?* * *To?* * *Why?* * *When?* * *How?* * *Lawful authority (if any)?* |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## **Risk analysis**

## **Privacy risks**

*The following table summarises the key requirements of each privacy principle and outlines key questions to help you to identify potential privacy risks. This list is not exhaustive, but gives an indication of the types of questions you could consider.*

|  |  |  |
| --- | --- | --- |
| **Privacy principles** | **Proposed information handling practices** | **Identified risks** |
| **Collection (IPPs 1 to 3)**   * Collect only that personal information necessary for or required to fulfil a purpose that is directly related to a function or activity of your agency. * Obtain it lawfully and fairly and in a way that is not unreasonably intrusive into an individual’s personal affairs. * Inform the individual of what you are going to do with their information, of any applicable law and of any third parties the information will be given to. * Take reasonable steps to ensure the information is complete and up to date. | *For example:*   * *What business process or function is enabled by collecting this information?* * *How is the collection of each piece of personal information necessary or directly related to this purpose?* * *Are there any laws that require or authorise the agency to collect this information? If so, include details of the legislation and the relevant section and a description of the information to be collected. Include only those laws that create an explicit authority or obligation for your agency to collect personal information, rather than legislation that broadly details the nature and extent of the agency’s responsibilities and powers.* * *Will personal information be collected directly from the individual it is about? If not, why is it being collected from a third party?* * *What reasonable steps will be taken to make individuals generally aware of the purpose for which their personal information will be used, any law that authorises or requires the collection, and the entities to whom their personal information will be routinely disclosed? Will this collection notice be given at this time of collection? If not, why it is not practicable to do so?* * *Is the collection notice easy to understand and can it be easily accessed by the individual?* * *Will individuals be required to verify their identity? If so, do their identification documents need to be recorded or just sighted?* * *Is any of the information being collected optional? If so, how will individuals know which information is mandatory and which information is optional?* * *Is the personal information being collected for more than one purpose (e.g. demographic information that is collected that will be used to improve customer engagement)? If so, how will an individual know what information will be used for which purpose?* * *Is the individual likely to be upset by the way in which their personal information will be collected or by how much information will be collected? If so, is the collection an unreasonable intrusion into the individual’s personal affairs?* * *What reasonable steps will be taken to ensure that the personal information collected is checked to ensure that it is relevant, complete and up to date?* | *Common risks may include:*   * *Personal information is collected without a clear purpose, which could increase the risk of scope creep or unauthorised use.* * *Information collected is either unnecessary or excessive.* * *Individuals are not aware of how their personal information will be used, or to whom it will be routinely disclosed, which can lead to a lack of trust.* * *Collection notices are not consistently provided, for example, across all communication channels.* * *Information is collected unfairly because the individual provides information that they would not have, had they known they had a choice not to provide it.* * *Collection methods may be unjustifiably intrusive.* * *Personal information collected from a third party may be of poor quality, as the affected person does not have the opportunity to check the data for accuracy.* |
| **Storage and security (IPP 4)**   * Make sure personal information is protected by appropriate security safeguards to prevent it being lost, accessed improperly, misused, modified or disclosed. * If giving the information to a third party, take reasonable steps to prevent its unauthorised use or disclosure. | *For example:*   * *What controls will be in place to protect the personal information from loss, unauthorised access, use, modification, disclosure or other misuse – while in transit and at rest? Has the project considered operational (e.g. policies or training), technical (e.g. access controls or encryption) and physical controls (e.g. doors or locks)? Are these safeguards adequate to provide the level of protection that can reasonably be expected to be provided? Can you reference any standards or documents that support the chosen controls?* * *How will access be controlled? Who will authorise access? What process will be used to grant access? How will access be changed or revoked when the user leaves or their role changes? Will access be audited regularly?* * *What measures will be in place to prevent and detect misuse or unauthorised access? For example – will audit logs enable actions to be linked to individuals and will these logs be reviewed on an ongoing basis?* * *What training and awareness is necessary to ensure that staff are aware of their privacy obligations, as well as the agency’s security policies and practices?* * *Can the personal information be accessed remotely? Can users access or save the personal information to their personal device? If yes, what controls will be in place?* * *Is there a testing or training environment? If yes, is real or dummy data used?* * *What is the process for identifying when personal information held by the agency is no longer required for undertaking the functions of the agency?* | *Common risks may include:*   * *Access is not limited to the ‘need-to-know’ requirement.* * *System users with administrative privileges is not limited to staff requiring those privileges.* * *Access is not revoked promptly when no longer required.* * *The system does not log who has accessed a file, making it difficult to detect or investigate unauthorised access or misuse.* * *Staff are unaware of their privacy and security obligations.* * *Information is saved onto privately-owned storage devices, increasing the risk of loss, unauthorised access, use, modification or disclosure or other misuse.* * *Personal information is kept for longer than required under approved retention and disposal schedule/s.* |
| **Openness, access and amendment (IPPs 5 to 7)**   * Inform the public about what types of personal information you hold and how it is used and how to request access to or amendment of documents containing their personal information. | *For example:*   * *Will requests from individuals for access to, or amendment of, documents containing their personal information be handled as a formal application under the IP Act or can the request be handled administratively?* * *Will the project allow information to be altered if it is inaccurate, incomplete, out of date or misleading? If information cannot be altered, what mechanism will be in place for a notation to be attached?* * *If the information is held by a contracted service provider, how can your agency get it back when you need it?* * *Will your agency’s list of personal information holdings need to be updated in light of this project? If so, have you contacted your agency’s privacy contact officer to discuss the proposed changes?* | *Common risks may include:*   * *Individuals are not able to easily access or amend their personal information.* * *Access may be hampered if the data is held by a contracted service provider.* * *An individual’s lack of access to their personal information increases the risk of inaccurate or out-dated information.* |
| **Use and disclosure (IPPs 8 to 11)**   * Use information only for the purpose for which it was collected unless one of the exemptions in the IP Act permits it. * Take reasonable steps to make sure the information is accurate, complete and up to date before you use it. * Only use the parts of the personal information that are necessary to fulfil the purpose. * Do not disclose personal information to anyone other than the individual who is the subject of it, unless one of the exemptions in the IP Act permits it. | *For example:*   * *What reasonable steps will be taken to ensure the information is accurate, complete and up to date before it is used?* * *How will you know when the personal information was last updated?* * *Has the information been supplied by the individual directly? If not, can it be checked with the individual directly?* * *Is it information that is likely to change over time (such as an address) or information that is static (such as a date of birth)?* * *How damaging will it be to the individual if information that is inaccurate, incomplete or out of date is acted upon? (The more damaging it will be, the more rigorous the steps should be to check its accuracy.)* * *Is there any opportunity for individuals to routinely correct or update their personal information or to verify its accuracy?* * *Are there any external entities to which the agency routinely discloses this personal information? How and why is this information being disclosed? What reasonable steps will be taken when collecting the personal information to make the individual who the information is about aware of this disclosure (as required under IPP 2)?* * *What process will be followed when a request is made to use the personal information for a secondary purpose or to disclose the personal information to a third party? How will you ensure that one of the permitted exemptions in the IP Act is satisfied? For example:* * *use or disclosure by or for a law enforcement agency* * *where authorised or required under a law* * *where the individual has expressly or impliedly agreed; or* * *use or disclosure for research or statistical purposes.* * *If you intend seeking agreement from the individual concerned, how will you ensure their agreement is valid, i.e. that it is voluntary, informed, specific and current? What mechanisms will be in place to accommodate an objection to the secondary use or disclosure? Will individuals be permitted to opt out if they change their mind and if so, how? If you are relying on implied agreement, what are the facts and circumstances of the particular situation that will support an assumption of the individual’s agreement?* | *Common risks may include:*   * *Incomplete, inaccurate or out-dated information lead to incorrectly informed decisions, which in turn may have a negative impact on the individual concerned.* * *Function creep – information collected for one purpose is then used for another purpose.* * *Information is disclosed in circumstances not permitted under the IP Act. If found to be in breach of the IP Act, there is capacity for an individual to be awarded up to a maximum of $100,000 in compensatory damages.* * *Individuals are surprised or upset by a secondary use, which can lead to a privacy complaint, a lack of trust or negative publicity.* * *An individual’s refusal of consent, or conditional consent, is not respected.* |
| **Transfer of personal information outside Australia (section 33)**  Do not transfer personal information outside Australia unless:   * the individual agrees to the transfer * there is legal authority for the transfer * it is necessary to prevent or lessen a serious threat to life, health, safety or welfare; or * at least two of the criteria in [section 33(d) of the IP Act](https://www.oic.qld.gov.au/annotated-legislation/ip/chapter-2/part-3/33-transfer-of-personal-information-outside-australia) are satisfied. | *For example:*   * *Will personal information be transferred outside Australia? For example – collected using an online survey tool or stored (including back-ups) with a cloud-based service or that uses servers physically located overseas? Or, could information potentially be accessed from outside Australia, for example, where information is posted on a website or social media site? If so, what provision in section 33 of the IP Act will be relied upon to permit this transfer?* * *If the exemption in section 33(a) will be relied on, how will you ensure their agreement is valid, i.e. that it is voluntary, informed, specific and current? What mechanisms will be in place to accommodate an objection to the secondary use or disclosure? Will individuals be permitted to opt out if they change their mind and if so, how?* * *If the exemption in section 33(d) will be relied on, what evidence can be provided to show that the requirements of this exemption have been satisfied?* | *Common risks may include:*   * *Personal information transferred outside Australia is not afforded the same of privacy protections as are in Queensland’s IP Act.* * *Individual does not wish for their information to be transferred outside Australia.* * *An individual’s refusal of consent, or conditional consent, is not respected.* * *Relying on a ‘collection notice’ to obtain an individual’s agreement to transfer their personal information outside Australia where the individual has no choice in whether to participate.* |
| **Use of contracted service providers (chapter 2, part 4)**   * Take all reasonable steps to bind a contracted service provider to compliance with the privacy principles. | *For example:*   * *Will the project involve contracting an external service provider to provide a service for the purpose of performing a function of the agency? And is this service provided directly to the agency, or to a third party of behalf of the agency? If so, will the provision of services under the contract or arrangement involve the exchange or handling of personal information in any way? If yes:* * *What steps will your agency take to ensure that the service provider is bound to comply with the privacy principles? Note – even if the service provider is subject to the Commonwealth Privacy Act 1988 you must still take all reasonable steps to bind them to Queensland’s IP Act as the obligations in the Commonwealth legislation do not apply to a contracted service provider for any acts or practices it undertakes in relation to a State Government contract.* * *Have you considered additional contractual provisions, such as limiting secondary use, placing conditions on the use of sub-contractors or mandatory reporting of any breaches?*   *It is recommended that you contact your procurement unit and/or legal services unit to ensure the contract includes clauses/provisions to bind the service provider appropriately.* | *Common risks may include:*   * *Existing government Information Technology Contracting (GITC) framework contracts may not adequately address the privacy risks of this particular project.* * *The standardised contracts in the Queensland Information Technology Contracting (QITC) framework may not adequately address the privacy risks of this particular project.* * *If the contractor has not been appropriately bound to comply with the IP Act and HHB Act, the contracting health agency will be liable for any breaches arising from the actions of the service provider.* |
| *Other legislative information handling requirements* | *If your agency’s enabling legislation explicitly permits, requires or limits the collection, use or disclosure of personal information, include detail of these requirements and their impact on the project’s information handling practices.* |  |

## **Risk ratings**

*Rating each risk can help you to prioritise your responses according to how likely it is that the privacy risk will materialise and the severity of its consequences. You should refer to your agency’s risk management framework for guidance on the descriptors for risk likelihood and consequences and definitions of the overall ratings. You should also record all privacy risks in the project’s risk register/log.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Identified privacy risk** | **Consequences for the individual or agency** | **Likelihood** | **Risk rating** |
| 1 | *Copy your list of identified risks from section 3.1* | *E.g. Minor, Moderate, Significant* | *E.g. Unlikely, Possible, Likely* | *E.g. Low, Medium, High* |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |

## **Actions to address the identified privacy risks**

*Describe the strategies or actions that will mitigate or minimise the identified risks. Note: While a PIA does not set out to eliminate every possible privacy risk; risk management does not provide an alternative to compliance with the privacy principles. Privacy needs to be incorporated with other project goals such as functionality; not balanced against them.*

*Adapt this table to suit the nature of the project and the needs of your agency, particularly as large or complex project may require a more complex risk analysis. For example, an assessment of any residual risk, or a more detailed analysis of the costs, strengths and weaknesses of all potential actions that could address the risks.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Identified privacy risk** | **Existing controls that contribute to managing the identified risk** | **Recommended actions** | **Comments** |
| 1 | *Copy your list of identified risks from section 3.1* | *What current safeguards help mitigate or minimise the identified risks?* | *What additional measures can be implemented to mitigate or minimise the risk?* | *If there are other strategies that could address the risk, provide comments about why the recommended action is the preferred option.* |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
|  |  |  |  |  |

## **Stakeholder consultation**

*Consultation with key stakeholders is essential to the PIA process. It helps to ensure that key privacy issues are identified, addressed and communicated. Provide details of who you consulted with, how you engaged with them, what you asked them and what information was gathered.*

The following stakeholders were consulted in undertaking this PIA:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Stakeholder** | **Internal/External** | **Scope of consultation** | **Method** | **Results** |
| *Name of stakeholders or group of stakeholders* | *Are the stakeholders internal to the agency or external?* | *What did you ask the stakeholder?* | *How did you engage with the stakeholders? For example, meeting, email, etc.* | *What input did the stakeholder provide?* |
|  |  |  |  |  |
|  |  |  |  |  |

## **PIA outcomes**

*Complete this section after the Project Executive/Steering Committee/Senior Management has reviewed the proposed actions and strategies set out in section 5.*

*Agreed recommendations should also be integrated into a revised project plan to ensure that the activities necessary to implement the recommendations are managed.*

## **Agreed recommended actions**

|  |  |  |
| --- | --- | --- |
| **#** | **Recommendation** | **Agreed Y/N** |
| 1 | *Copy the list of recommended actions from the table in section 4.* | *Document whether the recommendation was approved by the Project Executive/Steering Committee or senior management. If the recommended actions will not be implemented, record the rationale for this decision.* |

## **Action plan**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Actions to be taken** | **Responsibility for action** | **Date for completion** |
| 1 | *List the agreed additional actions.* | *Record who will be responsible for implementing the agreed actions.* | *Record the planned date for completion.* |

## **Contact point for future enquiries**

|  |  |  |  |
| --- | --- | --- | --- |
| Name: |  | | |
| Position: |  | | |
| Business unit: |  | | |
| Email: |  | Telephone: |  |
| File name/reference: |  | | |

1. Whether information is about a ‘reasonably’ identifiable individual requires case-by-case consideration of factors such as the nature and amount of information, who will have access to the information and other information that is available and the practicability of using that information to cross-match or link the information held by the agency to an individual. [↑](#footnote-ref-1)