# Part 2 Appendix A: Template – Privacy Impact Assessment Report

**NOTE:**

This template is provided as an example of the key types of information that can be considered during the PIA process. Adjust it as necessary to fit your organisation’s needs.

[Project name]

Privacy Impact Assessment Report

<Day> <Month> <Year>

## Privacy Impact Assessment Report – Contents

1. Project summary: Describe the project and its context 3

2. Scope of the PIA 4

3. Personal information 5

4. Privacy assessment 6

5. Risk assessment 12

6. Recommendations to minimise impact on privacy 13

7. Action plan 14

## **1. Project summary** (Describe the project and its context)

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

* Describe the project as a whole
* Where does the PIA sit within the project?
* What is the purpose of doing a PIA?
* What is the organisation trying to achieve with this project?
* Is the project a one-off initiative or part of ongoing business development?
* How does the organisation currently manage privacy? Show where the change that the project involves will fit with your current systems.

## **2. Scope of the PIA**

### 2.1 Scope

Describe what the PIA covers and what it doesn’t cover. For example:

* What parts of the organisation, project, systems, or IT infrastructure are included?
* What are the information-management processes that the PIA will consider (such as use, storage, access, retention and disposal)?
* What are the limitations of the PIA? For example, it might not cover the use of personal information by a third party if there is no direct control or agreement in place to manage the relationship.

### 2.2 The process

Describe how the PIA was done. For example:

* What types of information were used?
* Who was involved?
* Was anyone outside the organisation consulted?

### 2.3 Explain the scope and process

Describe the rationale for the scope of the PIA and for the process that was followed.

## **3. Personal information**

Identify and describe the type of personal information involved and what is happening with it.

“Personal information” is any information that is capable of identifying a living human being. It doesn’t have to be particularly sensitive or negative information.

However, the level of sensitivity and the level of impact on individuals will affect whether your information handling is likely to breach the law, or whether there are other privacy risks that need to be mitigated.

Identify the personal information involved and document the flow of this information through your systems and processes. An information flow diagram is often the clearest way to do this.

Describe both the **current** and **future** information flows so that the differences are visible at a glance.

Show, for example:

* what personal information is collected and used, and how it flows through the system
* how the project will change the information flow
* all changes to personal information involved in the project – for instance:
* Is new personal information being collected? Where is it coming from?
* Will information that the organisation already holds be used for a new purpose? Why and how?
* What is the nature of the information collected and the source?
* What measures are in place to ensure the information is accurate and up to date?
* Will the organisation tell the individuals what’s happening to their information? How will it tell them?
* How is the information managed, handled or protected?
* Who will have access to the information (whether inside or outside the organisation)?
* How long will the information be retained and how will it be disposed of?

## **4. Privacy assessment**

The principles in the Privacy Act provide the legal framework that your organisation has to consider. This section lets the decision-makers see at a glance whether the policy or proposal will comply with the law.

Each row in the following table summarises the key requirements of each of the privacy principles and outlines some key questions or considerations you should address. A risk assessment table can help you identify the privacy risks relevant to your initiative.

The accompanying Risk and Mitigation Table (see Appendix B) provides a more detailed explanation of how the project fits with the privacy principles. Either cut and paste from the Risk and Mitigation Table into this section of the PIA Report (and then omit those details from the “Risk assessment” section of this report, to save repetition), or provide a brief overview here and then expand on it in the “Risk assessment” section.

It is still useful to consider the privacy principles even if your agency is one of the few that doesn’t have to comply with the Privacy Act (for instance, if you’re a news agency collecting, using or publishing information for news purposes; or you’re a court or tribunal exercising judicial functions). Your activity may be legally compliant, but understanding how the Privacy Act deals with a matter can better inform you as to the likely privacy impacts of your proposal, and how privacy concerns can best be accommodated.

| # | Description of the  privacy principle  *(These can be deleted from your final report if they’re not relevant to your project – but you should at least consider each principle)* | Summary of personal information involved, use and process to manage | Assessment of compliance | Link to risk assessment (if required) |
| --- | --- | --- | --- | --- |
| 1 | Principle 1 - Purpose of the collection of personal information Only collect personal information if you really need it | *Identify each element of personal information and satisfy yourself that it is necessary for the project. What is the purpose of collecting the personal information involved here? How will that enable the organisation to do what it needs to do? Are you only collecting what you actually need? For example, do you really need “date of birth”, or will “age” or “over 18” be enough?* | *Note for each principle whether the project complies or risks being non-compliant* |  |
| 2 | Principle 2 – Source of personal information Get it directly from the people concerned wherever possible | *How is the information collected, and who from? If personal information is collected from some source other than the individual, is this appropriate and justifiable?* |  |  |
| 3 | Principle 3 – Collection of information from subject Tell them what information you are collecting, what you’re going to do with it, whether it’s voluntary, and the consequences if they don’t provide it. | *How will you tell people everything in this checklist? Or will it be so obvious to them that you don’t need to spell it out? If you’re not going to be open with them about what you’re doing, which of the exceptions allows you to keep it from them?*  Many of these aspects should be covered in any privacy statements or policy that relate to information collection. |  |  |
| 4 | Principle 4 – Manner of collection of personal information Be fair and not overly intrusive in how you collect the information | *This should describe how the information is collected, and should assess whether the method of collection is fair and appropriate in the circumstances* |  |  |
| 5 | Principle 5 – Storage and security of personal information Take care of it once you’ve got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse. | *There may be a number of methods to help you safeguard the personal information you hold, such as policies and codes of conduct that govern how employees treat personal information, through to physical or technical controls that protect the information. It is useful to refer directly to any documents or information that are available to support this.*  *Safeguards may include: physical security; IT security; staff training; policies that staff have to observe; confidentiality clauses in contracts with external providers etc.*  *Consider whether there are vulnerabilities in each part of the information pathway – identify any weak links* |  |  |
| 6 | Principle 6 – Access to personal information People can see their personal information if they want to | *This section should describe what steps the organisation takes to enable an individual to access their information and how the organisation will deal with requests for access.*  *Can the system be designed to make it easy to give people their information?* |  |  |
| 7 | Principle 7 – Correction of personal information  They can correct it if it’s wrong, or have a statement of correction attached | *This section should consider how the organisation will deal with a request for personal information to be corrected or for a statement of correction to be attached*  *Are there limitations? (for instance character limits in data fields; or lack of ability to add a flag indicating there is relevant information held on a physical file)* |  |  |
| 8 | Principle 8 – Accuracy etc. of personal information to be checked before use Make sure personal information is correct, relevant and up to date before you use it | *Reasonable steps will vary depending on the information involved. Relevant factors include: what process is there to check that information is correct? Has the information been supplied by the individual directly? Has it been checked with the individual directly? Is it automated, or do you have the ability to apply human judgment? How damaging will it be to the individual if information is wrong or misleading? (The more damaging it will be, the more extensive should the steps be for checking accuracy)* |  |  |
| 9 | Principle 9 – Not to keep personal information for longer than necessary Get rid of it once you’re done with it | *How long are you proposing to keep the information for? Are there any obligations to hold the information for a specific period of time, such as under regulation or legislation? If no such obligations exist, what would be considered to be a reasonable length of time to hold the information? How will you dispose of it? Where information is shared with a third party, consider how long they will hold the information for and what steps are in place to ensure that they dispose of personal information when the business requirement is completed.* |  |  |
| 10 | Principle 10 – Limits on use of personal information Use it for the purpose you collected it for, unless one of the exceptions applies | *Be clear about the purpose for having and using the information.*  *Is this what the individual will expect?*  *Are you using it for a different purpose from the one for which you collected it? If so, is there an exception justifying this use?* |  |  |
| 11 | Principle 11 – Limits on disclosure of personal information Only disclose it if you’ve got a good reason, unless one of the exceptions applies | *Be clear about the purpose for having and disclosing the information. Identify everyone who will receive it. Is disclosure one of the purposes for which you collected the information? If so, was the individual told that at the time? (This links to principle 3.) If you’re disclosing for a different purpose, is there an exception justifying the disclosure? Or another law that applies allowing you to disclose?* |  |  |
| 12 | Principle 12 – Unique identifiers Only assign unique identifiers where permitted | *Set out what the unique identifier is and why a unique identifier is necessary.* |  |  |
|  | Other privacy interests | *Use this section If the project involves activities such as bodily intrusions, intrusions into personal space, or storage of DNA, bodily samples or biometric templates* | *The Privacy Act deals with personal information, but other legislation or case law deals with other areas of privacy protection – consider any relevant laws here* |  |

### Summary / Conclusions

## **5. Risk assessment**

This section describes the privacy risks you’ve identified through the PIA process and how you propose to mitigate and manage those risks. It can be useful to link this back to the privacy principles to show why these risks and the proposed actions are relevant.

Note: A PIA doesn’t set out to identify and eliminate every possible privacy risk: its role is to identify genuine risks that are not unreasonably small or remote.

### Categorise your proposed actions

In some cases, it may be helpful to categorise these actions into areas such as:

* governance
* people
* process
* technology

Categorising the proposed controls in this way helps to define where within the organisation they will be managed.

Add a narrative summary of your risk assessment and options for mitigating those risks here.

Alternatively, attach a separate risk assessment document, such as one modelled on the template in Appendix C. If you don’t want to attach the whole document, you can cut and paste the relevant information into this section.

Document the risks in line with any existing risk management processes your organisation has – it will be more efficient than trying to run a separate process.

## **6. Recommendations to minimise impact on privacy**

Summarise the recommendations to minimise the impact on privacy based on your risk assessment

|  |  |  |
| --- | --- | --- |
| **Ref** | **Recommendation** | **Agreed Y/N** |
| R-001 |  |  |
|  |  |  |

## **7. Action plan**

This section of the report should describe what actions are being taken (whether short or long term) and how they’ll be monitored. There may also be links to other processes in the organisation. For example, a proposed action might relate to security controls (such as restricting access to a system). This will then link in with security processes in the organisation.

Reporting on the outcome of the mitigation may be necessary. If the PIA is being performed as part of a project, then the project is likely to require some reporting on their implementation as part of governance arrangements. Once the project is completed, any on-going privacy monitoring should be incorporated into normal business operations.

In the case of a particularly long or complex programme of work, the PIA may need to be reviewed a number of times to ensure that it continues to be relevant. This section should describe how this will be achieved.

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref** | **Agreed action** | **Who is responsible** | **Completion Date** |
| A-001 |  |  |  |
|  |  |  |  |