Guideline: Privacy Impact Assessment

Purpose

To provide advice on when to undertake a Privacy Impact Assessment (PIA) and the content of a PIA.

Definitions

Personal Information has the meaning given it in the *Privacy Act* 1998 (Cth).

Privacy Act 1988 (Cth) is the Commonwealth Act that applies to the ANU and other Commonwealth agencies.

Guideline

When developing or reviewing a new or revised project or system, you must consider the need for a privacy impact assessment (PIA).

A PIA is an important component of the University's protection of privacy and is to be implemented as part of the University's privacy by design requirement under the Privacy Act.

A PIA identifies how a new or revised project or system can have an impact on an individual's privacy, and makes recommendations for managing, minimising or eliminating those privacy impacts.

The PIA process should be included as part of the project and system planning processes, and recorded in the project plan and risk reporting. It should be revisited and updated when changes to a project or system are considered.

Determining whether a PIA is required

The first step is determining whether a PIA is required.

A PIA is beneficial for any project or system that involves new or changed ways of handling personal information. If the project or system will not handle any personal information or the project or system does not propose any changes to existing information handling practices (and where the privacy impacts of these practices have been assessed previously and found to be appropriate), no PIA is required.

A PIA is likely to be required if:

- personal information is collected in a new way;
- personal information is collected in a way that might be perceived as being intrusive;
- personal information will be disclosed to another agency, a contractor, the private sector or to the public; or
- there is a change in the way personal information is stored or secured.

Undertaking a PIA

The Project Manager or Business Owner of the new or revised project or system is responsible for the completion of the PIA.

The steps after identification that a PIA is required are:

1. Plan: Consider: how detailed the PIA will be, who will conduct it, what is the timeframe, what is the budget, who will be consulted and how will the recommendations be implemented and monitored.

2. Describe the project or system. To be included in the PIA report. The project description should be brief, but sufficiently detailed to allow all to understand the project. It should be written in plain English, avoiding overly technical language or jargon.

3. Identify and consult with stakeholders. To be included in the report. Consultation should be on privacy risks and concerns, to understand known risks better, and develop strategies to mitigate all risks.

4. Map personal information flows. To be included in the PIA report. Describe and map the personal information flows in the project or system. The map should detail what information will be collected, used and disclosed, how it will be held and protected, and who will have access to it. It is not a statement of the stages of the project.

5. Privacy impact analysis and compliance check. To be included in the PIA report. Analyse how the project or system might impact upon privacy, both positively and negatively. Assessment should be made against relevant Australian Privacy Principles (APP's)

6. Privacy management — addressing risks. Consider options for removing, minimising or mitigating any privacy risks identified through the privacy impact analysis. Can be combined in the PIA report with the above item.

7. Recommendations. Make recommendations that identify avoidable impacts or risks and how they can be removed or reduced. The recommendation should include timeframes for implementation.

8. Prepare the PIA report. A report template is Attachment 2. Prepare a PIA report that sets out all the information gathered.

9. Respond and review. The document should be a living document regularly reviewed, perhaps as part of an annual system review process.

PIA report

After the assessment is completed it should be documented in a PIA report. A PIA report template is attached (Attachment 2).

The need for a PIA report is to be reviewed by the Privacy Officer and where it meets the threshold the draft will be reviewed by the Data Governance Committee.

The Office of the Australian Information Commission has guidance at https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.

Attachment 1. Office of the Australian Information Commissioner

10 steps to undertaking a privacy impact assessment (PIA)

When developing or reviewing a project, consider the need for a privacy impact assessment (PIA). A PIA identifies how a project can have an impact on individuals' privacy, and makes recommendations for managing, minimising or eliminating privacy impacts. The Office of the Australian Information Commissioner (OAIC) recommends that organisations and agencies conduct PIAs as part of their risk management and planning processes.

Each project is different, but a PIA should generally include the following ten steps.

1. Threshold assessment

Ask if any personal information will be collected, stored, used or disclosed in the project. If the answer is yes, a PIA is usually necessary. Keep a record of this threshold assessment.

2. Plan

Plan the PIA. Consider: how detailed the PIA will be, who will conduct it, what is the timeframe, what is the budget, who will be consulted and how will the recommendations be implemented and monitored.

3. Describe the project

Prepare a project description to provide context for the PIA project. The project description should be brief, but sufficiently detailed to allow external stakeholders to understand the project. It should be written in plain English, avoiding overly technical language or jargon.

4. Identify and consult with stakeholders

Identify the project stakeholders. Consulting them can help to identify new privacy risks and concerns, understand known risks better, and develop strategies to mitigate all risks.

5. Map personal information flows

Describe and map the personal information flows in the project. The map should detail what information will be collected, used and disclosed, how it will be held and protected, and who will have access to it.

6. Privacy impact analysis and compliance check

Analyse how the project might impact upon privacy, both positively and negatively. Ask questions such as: Do individuals have to give up control of their personal information? How valuable would the information be to unauthorised users?

7. Privacy management — addressing risks

Consider options for removing, minimising or mitigating any privacy risks identified through the privacy impact analysis.

8. Recommendations

Make recommendations that identify avoidable impacts or risks and how they can be removed or reduced. Recommendations should include a timeframe for implementation.

9. Prepare the report

Prepare a report that sets out all the information gathered in steps 1 to 8. The report should be a practical document that can easily be interpreted and applied. The OAIC encourages the publication of PIA reports.

10. Respond and review

Monitor the implementation of the PIA report. A PIA should be an ongoing process that does not end with preparation of a report. It is important that action is taken to respond to the recommendations in the report, and to review and update the PIA.

Please refer to the OAIC's *Guide to undertaking a privacy impact assessment* available on the OAIC website: **www.oaic.gov.au**

Attachment 2. Template for PIA

Project or System name	
Prepared by Date	
Executive summary	Optional
PIA methodology	*Approach taken to undertaking the PIA, including any stakeholder consultation.*
Project description	*Includes description and map of information flows.*
Information Flows	*Insert model of information flows*
Analysis	*Project manager/System Executive* *Privacy Officer/Data Governance Committee* *Date*
Conclusion	*Includes recommendations*
Approval	
Appendices	*Where required*

Document information

Title	Privacy Impact Assessment Guideline
Document Type	Guideline
Document Number	ANUP_019407
Version	3
Purpose	The Guidelines on Privacy Impact Assessment provide an essential tool to assist projects and services ensure they comply with the Privacy Act 1988 and they assist with the implementation of good privacy practise.
Audience	Staff-Academic, Students, Alumni, Staff
Category	Administrative
Topic	Information Management
Subtopic	Privacy
Effective Date	1 Jan 2019
Review Date	23 May 2023
Responsible Officer	University Librarian and Director, Scholarly Information Services
Approved By	Chief Operating Officer (COO@anu.edu.au)
Contact Area	Library, Archives and University Records (director.sis@anu.edu.au)
Authority	Privacy Act 1988 Archives Act 1983
Printed On	22 Mar 2023