information and privacy commission
new south wales

A guide to Privacy Impact Assessments

Updated May 2020

Contents

A guide to Privacy Impact Assessments

A Privacy Impact Assessment (PIA) can help you to identify and minimise privacy risks when you are starting a new project or making changes to existing initiatives. A PIA is one way to implement 'privacy by design' in your organisation's practices, and it can help you to build and demonstrate compliance with privacy laws.

This Privacy Impact Assessment Guide has been issued by the NSW Privacy Commissioner under:

- section 36(2) of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) to promote the adoption of, and compliance with, the Information Protection Principles (IPPs) and protection of personal information and the privacy of individuals; and
- section 58 of the *Health Records and Information Privacy Act 2002* (HRIP Act) to promote the adoption of, and compliance with, the Health Privacy Principles (HPPs) and the protection of heath information and the privacy of individuals.

This guide explains the benefits of undertaking a PIA and sets out the basic steps of a PIA process. With new forms technology increasingly being used, this guide also considers the particular privacy issues that PIAs for digital projects may need to cover.

Samantha Gavel

Privacy Commissioner
Information and Privacy Commission NSW

May 2020

1. What is a PIA?

While NSW privacy legislation does not define a PIA, the following definition is useful in highlighting the important role a PIA can play in addressing privacy issues throughout a project's lifecycle:

> *A PIA is a methodology for assessing the impacts on privacy of a project, technology, product, service, policy, programme or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts. A PIA is more than a tool: it is a process which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should continue until and even after the deployment of the project.*[1]

A PIA should involve an assessment of:

- positive and adverse privacy impacts including community reaction
- compliance with privacy laws and other relevant legislation
- measures to reduce any identified risks to privacy.

2. Why undertake a PIA?

A PIA is an important 'privacy by design' process, ensuring that privacy considerations are built into projects from their conception through to implementation.

The benefits of the PIA process include:

- enabling early identification of adverse privacy impacts and an opportunity to address these
- promoting awareness of privacy issues and building privacy risk management capacity in an organisation
- complying with privacy laws
- demonstrating that privacy is a core corporate value and that a project is designed with privacy and privacy safeguards in mind
- building good will, trust and confidence of the community and stakeholders that your projects/ initiatives are privacy compliant.

The risks of not conducting a PIA include:

- failure to comply with privacy laws
- loss of credibility and reputational damage if the project fails to meet community expectations about how privacy and personal or health information will be protected
- late identification of privacy risks, resulting in unnecessary costs or inadequate solutions.

3. NSW privacy legislation

When considering a PIA, you will need to refer to NSW privacy legislation, which includes:

- the *Privacy and Personal Information Protection Act 1998* (PPIP Act)
- the *Health Records and Information Privacy Act 2002* (HRIP Act).

The PPIP Act protects personal information and applies to NSW public sector agencies including local councils and universities.

[1] Wright D, Finn R and Rodrigues R "A Comparative Analysis of Privacy Impact Assessment in Six Countries" (2013) 9(1) *Journal of Contemporary European Research*, 160-180.

'Personal information' is information or opinion (which can be part of a database) about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion. Personal information can include fingerprints, retina prints, body samples or genetic characteristics.

The HRIP Act protects health information. It applies to NSW public sector agencies, private health service providers irrespective of size, and private organisations that hold health information which are above a certain size.

'Health information' includes:

- information or opinion about the physical or mental health or disability of an individual
- the health service provided to an individual
- personal information collected in providing a health service or in connection with the donation of an individual's body parts, organs or body substances
- genetic information about an individual
- healthcare identifiers.

Both the PPIP Act and HRIP Act are principles-based and focus on the collecting, holding, using or disclosing of personal and health information. You will need to consider if these principles will be affected by new projects or changes to existing services or policies.

You may also need to check if there are privacy provisions to consider in other applicable legislation. For example, the *Data Sharing (Government Sector) Act 2015* contains provisions that apply to the sharing of data between public sector agencies.

4. Core elements of an effective PIA

An effective PIA is:

- ***Integral to an organisation's governance:*** a PIA is most effective when it is a standard organisational commitment to assessing privacy risks and there are clear roles and responsibilities for senior executives, managers and employees, including who initiates, undertakes and signs off on the final PIA report.
- ***Fit for Purpose:*** the PIA needs to be sized according to the potential privacy risks. If a preliminary assessment identifies low privacy risks, a short PIA may be adequate. If high risk privacy issues are identified, such as a risk to sensitive information or risks to a large number of individuals, a more extensive PIA is appropriate.
- **Comprehensive*:*** PIAs cover all privacy issues, not just compliance for the handling of personal or health information, but also the views of key stakeholders, supporting documentation such as Privacy Management Plans, relevant IT security protocols, and operational Human Resource policies and practices such as the training to accompany project implementation.
- ***Available:*** the PIA report demonstrates accountability. It is in the public interest for it to be available to a wider audience. A summary is an option if the report contains sensitive information.
- ***Enables compliance:*** legal and policy compliance checks are core elements of a PIA. It must address all relevant obligations under privacy and other legislation including requirements for movement of personal or health information out of the jurisdiction.
- ***Ongoing:*** allows updating or revision according to any changes in the project. If there are substantial changes to how personal information will be handled for example, it may be necessary to undertake a further PIA.
- ***Constructive:*** a good PIA adds to the privacy culture of an organisation by demonstrating the value of managing privacy risks and contributing to organisational success[2].

[2] De Hert P, Kloza, D and Wright, D (2013) Recommendations for a privacy impact assessment framework for the European Union, European Commission-Directorate General Justice, Brussels, Belgium.

5. The PIA process

Determine if a PIA is necessary

A threshold assessment identifies those projects with privacy implications and helps determine the likely scope and scale of the PIA. This assessment is best undertaken by someone with familiarity with privacy requirements.

The first question to ask when assessing whether a PIA is needed is, "Will any personal or health information be collected, stored, used or disclosed in the project?" However, even if no personal information is being handled, you might still decide to conduct a PIA if you wish to show how you are avoiding the use of personal information.

You should document the outcome of your threshold assessment. This record could include:

- a brief project description
- whether the project involves personal and/or health information
- a brief description of the personal and/or health information such as name, address, date of birth, health information, bank details
- why this information is needed
- the relevant authority
- storage and security of the information
- access to and amendment of the information
- any known or likely views of any stakeholders about the impact of the project on privacy
- whether a PIA is recommended or not
- details of the person or team responsible for the threshold assessment.

Technology and privacy impacts

When projects involve innovative technology, including artificial intelligence (AI), this can give rise to unique and complex privacy issues. While there are no strict legal requirements in NSW around undertaking a PIA, other jurisdictions provide useful examples of the types of technology and processing for which you should consider a PIA.

Under the European Union *General Data Protection Regulation* (GDPR), data protection impact assessments (which share features of a PIA) are required for any new projects that are likely to involve a "high risk" to people's personal information. Data protection impact assessments are mandatory where processing involves:

- large-scale use of sensitive data
- systematic and extensive profiling
- public monitoring[3].

In the United Kingdom, the Information Commissioner's Office has listed other processing operations for which a data protection impact assessment is also mandatory. These include:

- innovative technology, including AI
- denial of service based on automated decision-making
- large scale profiling of individuals
- any processing of biometric data
- any processing of genetic data, other than by an individual GP or health professional for the provision of health care directly to the data subject
- "invisible processing": processing of personal data that has not been obtained directly from the data subject
- tracking of an individual's geolocation or behaviour, including but not limited to the online environment
- targeting of children or other vulnerable individuals

[3] Article 35 of the General Data Protection Regulation (2018).

- risk of physical harm: where the processing is of such a nature that a personal data breach could jeopardise the health or safety of individuals[4].

Plan the PIA: assign responsibilities and describe the project

The nature and size of your project will determine who undertakes the PIA. You may require expertise in a range of areas, including information privacy and data protection, technology and systems, risk management, law and ethics.

A PIA conducted by external assessors may be preferable in some instances. External input from experts can help identify privacy impacts you may not have recognised and help develop community trust in the PIA findings and the project's intent.

If your project involves the use of a new form of technology or data processing, the product or system developer may have undertaken their own PIA, which you could use to inform your analysis.

You should set out who is responsible for the PIA, the expertise and inputs required, important milestones, key decision-making points and how consultations will be carried out. You should also outline:

- the context or setting in which the project is being undertaken including relevant social, economic and technological considerations
- why the project is being undertaken
- the project's overall aims and objectives and how these fit with the agency's broader objectives
- any links with existing programs or projects
- the target market of the project
- what personal and health information will be collected and how it will be stored, used and disclosed and how security and quality are to be addressed.

Particularly for digital projects, you should clearly describe the nature and scope of any processing of personal or health information, as well as whether the project will use any new technology or novel types of information processing.

Stakeholder consultation

Early engagement with the people and organisations with an interest in the project, or who will be affected by the project, is essential. Consultation can continue throughout the project lifecycle, so that the necessary people are consulted at the appropriate time or as the project changes. Stakeholder consultation:

- can identify privacy risks and concerns not previously identified and possible strategies to mitigate these risks
- offers stakeholders the opportunity to discuss risks and concerns with the agency and to gain a better understanding of, and provide comment on, any proposed mitigation strategies
- can gain the confidence of stakeholders and the public that privacy is being taken seriously and managed effectively.

The range and number of stakeholders to be consulted will depend on the size and complexity of the project, the likely privacy risks and the number of people who could be impacted. When deciding what degree of consultation is necessary for a project, consider whether there is:

- likely to be public concern about actual or perceived impacts on privacy
- a large number of people or a particularly vulnerable group whose privacy is affected
- any personal information holding which is vulnerable to misuse or abuse

[4] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/?_sm_au_=iVVH06WPMJV3VcFFNKCfNKt3tRVRF

- any existing project consultation process into which the privacy aspects can be incorporated
- existing levels of trust in a new practice or technology.

You may also wish to consult with the Privacy Commissioner or the IPC on the privacy implications of new projects or initiatives. The IPC has published a fact sheet on The Role of the Privacy Commissioner: Consulting the IPC on Initiatives and Projects.

Map information flows

The flow of personal and health information in a project needs to be mapped, detailing what information will be collected, used and disclosed, as well as how it will be stored and protected.

Your mapping should describe:

- who will collect what information, and from whom
- how the information will be collected, and for what purpose
- how the information will be used or processed
- how the information will be stored and kept secure
- the processes for ensuring information quality
- whether the information will be disclosed to another agency or organisation, to whom and for what purpose
- if the information is to be disclosed to and used by secondary users, how well will those secondary users protect that information and whether they will pass it on to others
- whether personal information will be transferred to another organisation in another jurisdiction either in Australia or overseas
- whether individuals will be able to access and correct their personal information
- how long the information will be retained and when and how the information will be disposed of.

If you are undertaking data linkage or matching, your mapping should also consider:

- planned or potential data-matching or linking to other information held in different databases (by you or other entities)
- how any data-matching or linking will be done
- any decisions affecting the individual that might be made on the basis of data matching or linking.

Mapping information flows will be particularly important where AI or other innovative processing systems are used, given that data can be moved around in multiple ways, making it difficult to maintain records and to control access. Understanding and documenting how personal information is being processed will help you to comply with your privacy obligations, allow you to efficiently handle requests from individuals for access to their information and improve your organisation's data governance.

The Office of the Australian Information Commissioner has produced detailed guidance on useful considerations when mapping information flows, available in its Guide to undertaking privacy impact assessments.

Identify privacy risks and possible remedial actions

Once you have mapped information flows, you will need to identify and assess the potential privacy impacts of your project. As a first step, it is important to check your project's processes in relation to handling personal and health information against the privacy obligations set out in:

- the PPIP Act and HRIP Act and regulations
- any applicable Privacy Codes of Practice and Public Interest Directions
- where applicable, Commonwealth privacy legislation
- other legislation that applies to your agency relating to the collection and use of personal and health information.

Even if the project appears to be compliant with privacy legislation, there may still be other privacy risks that need to be addressed. Some of the key questions to consider include:

- Will individuals lose control over their personal information?
- How valuable would the information be to unauthorised users? For example, is it information that others would pay money for or try to access by hacking?
- How will privacy breaches be handled?
- Is there a visible, comprehensive and effective complaint handling mechanism?
- How consistent is the project with community values about privacy?
- What auditing and oversight mechanisms are in place, especially if a system fails?
- Does the project collect more information than it needs to?[5]

You will also need to consider specific risks to individuals, such as the potential re-identification of pseudonymised data, identity theft or fraud, reputational damage, loss of confidentiality or financial loss. Based on the nature of your project and your handling of personal information, you should consider the likelihood and severity of the risks you identify.

The next step is to consider what action can be taken to resolve these privacy risks. Some options could be that you:

- decide not to collect certain types of data
- reduce the retention periods for some personal information
- anonymise or pseudonymise data where possible
- take additional security measures (both technical, such as access control mechanisms and encryption, as well as physical, such as lockable storage and limited access to certain areas)
- put clear data sharing arrangements into place
- offer individuals the chance to opt out where appropriate
- train staff to ensure risks are anticipated and managed
- prepare internal guidance and processes to avoid risks.

This is not an exhaustive list: the measures you can take to mitigate privacy risks will depend on your project. Where there are multiple options to address a privacy risk, you will need to evaluate the likely costs, risks and benefits of each option to identify which is the most appropriate.

Formulate and consult on draft recommendations

The above analysis will result in a set of recommendations that include an action plan and timeline.

These recommendations should identify how privacy protection measures can be enhanced and how negative privacy impacts or risks can be avoided or reduced. The recommendations could address:

- changes to the project that would achieve a more appropriate balance between the project's goals and the protection of personal and/or health information
- privacy management strategies that will reduce or mitigate privacy risks
- the need for further stakeholder consultation
- whether the privacy impacts are so significant that the project needs considerable re-design or even its feasibility examined
- creation of privacy documentation or amendment of existing agency privacy management plans
- issues beyond project specific matters to overall privacy risk management for the organisation.

You should discuss the proposed recommendations with affected stakeholders before they are finalised, to ensure their views are incorporated and to secure their commitment to the recommended actions.

[5] https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/

Prepare and publish the report

The PIA report needs to set out all the information gathered throughout the PIA process. Key elements include:

- introduction and background information, including the context of the project
- project description
- who was responsible for the PIA and the approach they took
- a description of the information flows
- results of stakeholder consultation
- outcome of risk assessment and compliance check, including privacy risks that have been identified, options considered to mitigate risk, why particular options or alternatives were rejected or discounted and why a particular course of action has been recommended
- description of privacy risks that cannot be mitigated, the likely response to these risks, and whether they are outweighed by the public benefit delivered by the project
- recommendations.

It is best practice to publish a PIA report. This demonstrates transparency and is an important public record. It also shows that the project has undergone critical privacy analysis.

There may be circumstances when the full release of a PIA report may be inappropriate; for example, if a project is still in its very early stages; the PIA report contains privileged or confidential information; or if release would prejudice security measures to protect personal or health information. In these circumstances, you should still consider releasing a summarised or edited version of the PIA.

You should consider and adopt a position on the recommendations in the PIA report. At a minimum, you should identify whether you will adopt, partially adopt or not adopt any of the recommendations made. You should provide reasons why you have not adopted recommendations.

A possible format for a PIA report is included at **Appendix A.**

Review and update

Seeking external review of a PIA by an independent third party can ensure that the PIA has been carried out properly and that the recommendations have been implemented.

Many projects undergo changes before their completion. If the changes are substantial and result in significant new privacy impacts that were not considered in the original PIA, it may be necessary to undertake a new PIA.

Useful resources

- Sample PIA reports: A PIA for the IPC's Information Access Self-assessment tool was completed in 2016. The Office of the Australian Information Commissioner has produced a guide to undertaking PIAs, which includes resources and sample PIA reports. Please note that the IPC does not endorse any of these sample reports.
- For digital projects: the UK Information Commissioner's Office has produced guidance on data protection impact assessments, as required under the GDPR. While the GDPR does not apply to most NSW public sector agencies, this guidance sets out useful privacy considerations when using digital technology.

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

6. References

1. Article 29 Data Protection Working Party (2017) *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, Brussels, Belgium.

   https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

2. De Hert P, Kloza, D and Wright, D (2013) Recommendations for a privacy impact assessment framework for the European Union, European Commission-Directorate General Justice, Brussels, Belgium.

3. Information Commissioner's Office (2018) *Data protection impact assessments*, Wilmslow, UK.

   https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

4. Office of the Australian Information Commissioner (2014) *Guide to undertaking privacy impact assessments*, Canberra, ACT.

   https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/

5. Office of the Information and Privacy Commissioner of Alberta (2010) *Privacy impact assessment requirements*, Edmonton, Alberta.
   https://www.oipc.ab.ca/media/117453/guide_pia_requirements_2010.pdf

6. Office of the Privacy Commissioner Te Mana Matapono Matatapu (2015) *Privacy Impact Assessment Toolkit,* Auckland, New Zealand.

   https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment/

7. Wright D, Finn R and Rodrigues R "A Comparative Analysis of Privacy Impact Assessment in Six Countries" (2013) 9 (1) *Journal of Contemporary European Research*, 160-180.

Appendix A: The PIA Report – Possible Format and Components

Section	Content
Executive summary	Make it easy for readers, describe in brief: • the purpose of the PIA • brief project description and key information flows • a summary of findings • a summary of recommended actions.
PIA methodology	Outline the approach taken, that is: • who was responsible for the PIA • who conducted the PIA (their skills and expertise) • key steps taken to complete the PIA
Project description	This section should describe the key features of the project including: • any relevant background and what it will achieve • why the project is needed • any links with existing projects • who is responsible for the project • timeframes • whether the project will use innovative technology, such as AI • how personal and health information will be handled in the project, from beginning to end, explaining: - what information will be collected - how it will be collected - how it will be stored - who will have access to it - what it will be used for - any third parties to whom it will be routinely or otherwise disclosed Diagrams can help illustrate information flows.
Stakeholder consultation	This section should outline what stakeholder consultation was undertaken, including any feedback.
Analysis of privacy issues	This section should identify and present the analysis of: • the project's impacts (positive and negative) on privacy

- privacy risks that may arise, including whether the project complies with privacy legislation
- any strategies that are already in place to remove or mitigate privacy risks
- options to enhance privacy protections and address negative privacy impacts.

Recommendations	These need to be clear and concise, address actions required, set priorities; specify responsibility for implementation if approved and set target dates. Recommendations can also be included in the Executive Summary or incorporated through the report.

Document information

Identifier/Title:	A guide to Privacy Impact Assessments
Business Unit:	Legal Counsel and Regulatory Advice
Author:	Senior Project Officer
Approver:	Privacy Commissioner
Date of Effect:	May 2020
Next Review Date:	May 2021
EDRMS File Reference:	D20/010012/DJ
Key Words:	Privacy, Privacy Impact Assessment, privacy by design