office of the privacy commissioner
new south wales

Guidance

Guide to Privacy Impact Assessments in NSW

Contents

1. Overview	3
2. The NSW privacy legislation	3
3. What is a PIA?	4
4. Why undertake a PIA?	4
5. When to do a PIA?	5
6. Core elements of an effective PIA	5
7. The PIA process	6
8. End Notes	17
9. References	18

1 Overview

Privacy Impact Assessments (PIA) assist public and private sector organisations identify and minimise the privacy risks of changes to services or policies and new projects. Also, a PIA can assist compliance with privacy obligations, address wider privacy issues and execute a 'privacy by design' approach.[1]

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.

The Guide:

- explains the benefits of undertaking a PIA;
- sets out the basic steps of a PIA process and relevant considerations;
- draws upon practice in Australia, New Zealand, the United Kingdom, the United States, Canada and the European Union.[2]

This Guide is not intended to offer legal advice or restrict the NSW Privacy Commissioner's statutory powers. Advice can be sought from the Privacy Commissioner's Office (see contact details at the back).

Dr Elizabeth Coombs
A/NSW Privacy Commissioner

December 2016

2 The NSW privacy legislation

NSW privacy legislation includes:

- the *Privacy and Personal Information Protection Act 1998* (PPIP Act); and
- 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. '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; or
- the health service provided to an individual; or
- personal information collected in providing a health service or in connection with the donation of an individual's body parts, organs or body substances; or
- genetic information about an individual; or
- healthcare identifiers.

Both the PPIP Act and HRIP Act are principles based and these principles focus on the collecting, holding, using or disclosing of personal and health information. In the Guide, they are referred to as the privacy principles. Organisations need to consider if these principles will be affected when introducing new projects or changing existing services or policies.

Organisations also need to check if other applicable legislation has privacy provisions to be considered.

3 What is a PIA?

NSW privacy legislation does not define a PIA and it is a concept that continues to evolve.[3] In the Guide, the following definition is used:

> *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 deployment of the project.* [4]

A PIA applies to any project that could intrude on a privacy principle or any reasonable expectations of privacy. A PIA examines:

- positive and adverse privacy impacts including community reaction;
- compliance with privacy and other relevant legislation;
- controls that mitigate any identified risks.

A PIA can also consider if additional controls will enhance privacy.

4 Why undertake a PIA?

PIA is an important 'privacy by design' process that assists compliance with privacy obligations and delivers benefits to organisations.

Internally, such benefits include:

- providing information to inform decision-making on:
  - › compliance with privacy laws;
  - › the fit with community values around privacy, personal and health information;
  - › potential privacy problems and possible solutions.
- promoting awareness of privacy issues and building privacy risk management capacity
- providing an early warning system of adverse privacy impacts and opportunity to address these[5];
- contributing to the broader organisational risk management capacity ;

For external audiences, a PIA:

- demonstrates an organisation has privacy as a core corporate value and designed the project with privacy and privacy safeguards in mind;
- builds community understanding of the project through public consultation and assists in establishing good will, trust and confidence.

There are risks associated with not conducting a PIA including:

- failure to comply with legal requirements;
- loss of credibility and reputational damage if the project fails to meet expectations about how privacy and personal or health information will be protected; and
- late identification of privacy risks resulting in unnecessary costs or inadequate solutions.[6]

5 When to do a PIA?

The greater the project's complexity and privacy scope, the more likely it is that a PIA is required to identify and manage its privacy impacts. A threshold assessment (see section 7.1), can determine if a PIA is necessary and can guide decisions around the scale and scope of a PIA if it is required.

An effective PIA is an integral part of the project planning process, not an afterthought.[7] It is timed so it can genuinely contribute to the project design or decision making around the project's feasibility.[8] It is best undertaken as a part of project decision making and supported by organisational risk management processes.

6 Core elements of an effective PIA

An effective PIA is[9]:

- ***Integral to an organisation's governance:*** the PIA is most effective when it is a standard organisational commitment to assessing privacy risks and there are clear roles and responsibilities of senior executives, managers and employees for a PIA, including who initiates, undertakes and signs off on the final PIA report.

  Responsibility for a PIA is best placed with a senior officer who ensures the PIA is conducted by an independent but knowledgeable person and who ensures there are no conflicts of interests. PIAs need to be included in reports to the Audit and Risk Committee and Executive or Board. On occasions it may be appropriate to have the PIA externally reviewed. A register of PIAs has been used to identify systemic privacy issues that have arisen across multiple project proposals.[10]

- ***Fit for Purpose:*** the PIA needs to be sized according to the potential privacy risks. If a preliminary assessment identified low privacy risks, a short PIA may be adequate. If high risk privacy issues were identified, such as a risk to sensitive information or risks to a large number of individuals, a more extensive PIA is appropriate. Inputs need to correspond to the content of the project being assessed.

- ***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 attestations, and operational Human Resource policies and practices such as the training to accompany project implementation.[11]

- ***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 or matter being assessed. If there are substantial changes to how personal information will be handled for example, it may be necessary to undertake another 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.

7 The PIA process

Leading practice is summarised below. [12, 13]

7.1 Determine if a PIA is necessary (threshold analysis)

A threshold assessment identifies those projects with privacy implications and helps determine the likely scope and scale of the PIA.[14] This is best undertaken by an officer with familiarity with privacy requirements. Project or technical experts may not have the necessary knowledge or may have competing objectives and so are not well placed to make this preliminary assessment.

Some projects are of such a scale or nature that it is self-evident that a PIA is required, for instance, projects such as data-warehousing the personal information of people in NSW, or use of surveillance devices which have widespread impact on the privacy of members of the public or projects which amass otherwise confidential information into accessible databases.[15]

For smaller projects determining whether a PIA is necessary will depend on the merits of each project. 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 and/or does the project impact on the privacy of anyone?'.

A PIA may not be necessary if the project does not propose any changes to existing information handling practices, if the privacy implications of these practices have been assessed previously and controls are current and working well.[16] The reasons for not undertaking a PIA need to be recorded in the project documentation.

The record of the threshold assessment 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 personal and/or health information;
  - access to and amendment of the personal and/or health information;
- any known or likely views of any stakeholders about the impact of the project on privacy;
- whether a PIA is recommended or not; and
- details of the person or team responsible for the threshold assessment.

Don't Assume - De-identified information

A PIA may be necessary in circumstances involving the use of de-identified information, information that is linked to personal or health information and where new technologies are being proposed to handle information. Although it may be thought that the information has been de-identified caution is warranted as re-identification of information considered de-identified is possible and this can reduce public confidence in how your organisation respects individual privacy and be already of privacy law.

The threshold assessment will help determine also the scale and scope of the PIA. If the threshold analysis indicates that the risks are not significant, then the scale and scope of a PIA could be limited but if the risks are significant, then a PIA should be more detailed.

Factors that influence the level of detail needed in the PIA include:

- Consideration of the type of privacy and if it is 'informational privacy', the information's:
  - nature (personal and/or health information)
  - quantity
  - treatment – are new methods of requiring, using or disclosing personal information planned, or proposals for aggregation into databases, outsourced, linked or used for data-matching;
  - potential impacts - on key aspects of an individual's life (such as livelihood, housing, reputation, health), or possible adverse outcomes (such as fines, reduction or cancellation of entitlements);
- Project factors
  - the size and complexity of the project bearing in mind that size or budget is not always a reliable indicator as even a small-scale project may have significant privacy implications;[17]
  - any cross- agency or cross-sector information sharing, within NSW, within Australia or outside of Australia;
- Technological issues
  - will new or innovative technology be used to collect or store personal information?;
  - existence or not of IT security accreditations or attestations;
- Context
  - likely community and/or media interest in the project.

These factors can also inform decisions about who should conduct the PIA, its terms of reference, the level of stakeholder consultation required, the budget and timeframe for completion of the PIA. Generally, the greater the privacy scope of the project, the more detailed the PIA will need to be.

7.2 Assign roles and responsibilities, set terms of reference, resources, and time frame

Who should undertake a PIA?

Generally, the project sponsor or project manager will be responsible for ensuring a PIA is carried out, however, it can be that the organisation's Chief Audit or Risk Management Officer (or similar position holder) may be responsible.

The nature and size of the project will influence decisions about who undertakes the PIA. A range of knowledge, skills and experience may be required to conduct a PIA but the nature of the project is the primary consideration. Expertise could be required in information privacy and data protection, information security, technology and systems, risk management, law, ethics, compliance analysis, operational procedure and other industry-specific knowledge. A multidisciplinary team approach using 'in-house' experts and outside expertise as necessary can be most effective.

A PIA conducted by external assessors may be preferable in some instances. External input from experts not involved in the project can help identify privacy impacts not previously recognised and help develop community trust in the PIA findings and the project's intent.[18]

The team conducting the PIA needs to be familiar with the requirements of the PPIP Act and HRIP Act and the organisation's obligations regarding how personal information is to be collected, stored, used and disclosed. They also need to be familiar with any other legislation or regulations that might apply and the broader dimensions of privacy.[19]

A good PIA has independence and objectivity and takes into account all relevant information.[20]

The assigned responsible officer should draft the PIA terms of reference specifying:

- whether public consultations are to be held;
- to whom the PIA report is to be submitted; and
- the nominal budget and time frame for the PIA.

Prepare a PIA plan

The PIA plan should spell out who is responsible for the PIA, what is to be done to complete the PIA, the expertise and inputs required, who will do what, the PIA schedule, important milestones, including decision-making points that determine the project's design and which influence phases of the PIA, and, especially, how consultations will be carried out. This includes specifying who will be consulted and how they will be consulted (for example, interview, survey, workshops, focus groups, public hearings or submissions).

The PIA Plan needs to describe the proposed project as it provides context and is an essential component of the PIA report. It can also be used in consulting with stakeholders. It needs to:

- 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; and
- how the project might impact the consumer's privacy.

This information can typically be sourced from the project's management documentation, such as the Project Brief or Business Case or information prepared for the threshold assessment. The project description should be kept brief but sufficiently detailed to allow external stakeholders to understand the project, and written in plain English avoiding overly technical language or jargon. The project description might need to be updated as the project progresses.

Determine the budget for the PIA

This will need to consider whether in-house expertise or external expertise (or a mix) is to be used. There is no formula but discussion with the Chief Audit Officer (or similar) may assist in gaining an understanding of the cost of previous risk assessment exercises. In most cases, in-house expertise will not need to be costed but external expertise will. Adequate coverage of expenses such as travel, consultations and incidentals is required. Include a contingency factor and identify the source of funds. Depending on organisational delegations, the budget may require the approval of senior management. Approved procurement processes need to be followed for contracting external resources.

Stakeholder involvement

Consultation with the people and organisations with an interest in the project, or who will be affected by the project, is essential. 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; and
- avoids criticism about a lack of consultation in relation to the project.

First identify the stakeholders who have a privacy interest in the project proposal, including:

- internal stakeholders - such as the Minister, the Executive, the Audit and Risk Committee, members of the project team, information technology, privacy, legal, procurement and records management staff as well as the front-line or customer-facing staff who will have to use the new system or process that will be delivered by the project; and
- external stakeholders – such as suppliers, customers, government agencies, non-government organisations, advocacy organisations, regulatory authorities, service providers, industry experts, academics and the public.

The stakeholder list should identify the individuals and organisations within each of these categories. It may be necessary to add to the stakeholder list as the PIA progresses.

Involving internal stakeholders in the PIA process is critical as these are the people who know the project and operational environment. They will be able to explain and answer questions about likely information flows, governance structures and technical architecture of the project. They may be able to provide insight into legislation under which the organisation operates that authorises certain information to be collected, used or disclosed, and information retention and disposal requirements. Importantly, they may also be able to suggest potential solutions to address the identified privacy issues or provide advice on the practicality of options to address risks identified.

The range and number of stakeholders to be consulted is a function of the size and complexity of the project, likely privacy risks and the numbers of citizen-consumers who could be impacted. It may not be necessary to consult with all identified stakeholders. For a small project with limited privacy impacts, it may be sufficient to consult only with internal stakeholders. In contrast, a high profile project having significant privacy impacts may require broad and public consultation. Even if a broad public consultation is not warranted, some form of targeted consultation might be advisable, such as with relevant public sector agencies or regulatory bodies, or advocacy groups representing relevant sectors of the community.

When deciding what degree of consultation is necessary for a project, consider whether there is:

- likely to be public concern about actual or perceived impact 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;
- any existing project consultation process into which the privacy aspects can be incorporated;
- existing levels of trust in a new practice or technology.

Commercial-in-confidence or security considerations can sometimes affect how much information about the project can be released to third parties. In these circumstances, it may be necessary to make the release of information subject to confidentiality agreements or to release a summary of information.

7.3 Undertake the assessment

Map the information flows and identify privacy impacts

The project's privacy aspects and personal or health information usage needs to be `detailed. In particular the requirements for personal and health information and the flows of this information need to be mapped. The analysis should be sufficiently detailed to provide a sense of what information will be collected, used and disclosed, how it will be held and protected, and who will have access to it.

The map needs to describe the information flows and, specifically:

- who will collect what information from whom and for what purpose;
- how will the information be used or processed, and whether the collection of any personal or health information is excessive;
- how will the information be stored and kept secure;
- the processes for ensuring information quality;
- whether the information will be disclosed to another agency or organisation, and to whom and for what purpose;
- if the information is to be disclosed to and used by secondary users (for example, another organisation, the organisation's service providers, system or application developers), how well will those secondary users protect that information or whether they will pass it on to others;
- whether personal information will be transferred to another organisation in another jurisdiction either in Australia or outside Australia;
- whether individuals will be able to access and correct their personal information; and

- how long will the information be retained and when and how will the information be disposed.

This analysis should be as detailed as possible to help identify potential privacy risks.

The following details the questions to be considered in mapping information flows. [21]

7.4 Questions to be considered

Collection

Identify and describe:

- the personal information to be collected, including any sensitive information;
- how the collection relates to the organisation's functions or activities;
- why the personal information, including the particular items and kinds of information, is necessary for the project;
- whether the information can be collected in a de-identified or anonymous way;
- whether individuals can choose not to provide some or all of the personal information; or
- if the method of collection may be unreasonably intrusive for some individuals (for example, seeking personal information from individuals in a public area where others may overhear)

Detail the collection process, including:

- the reasons why the personal information is collected;
- any legislation or other authority on which the organisation relies to collect the information;
- how the information will be collected (for example, hard copy or electronic forms, online transactions, CCTV);
- whether unsolicited personal information may be used in the project;
- where the information will be collected from (for example, directly from the individual, from other individuals or entities, or from publicly available sources);
- how an individual's circumstances will be taken into account when the personal information is collected (for example, if they may require support to understand why the information is collected);
- collection alternatives that have been considered and rejected (for example, using de-identified information);
- how often the personal information is to be collected (once only or ongoing);
- any limits on the nature of the information to be collected (for example, information over a certain age);
- any potentially sensitive or intrusive collection (for example, photographs, fingerprinting, drug testing, collection of genetic information, biometrics or facial recognition);
- any covert methods of collection (such as surveillance) and why they are necessary and appropriate; or
- the information (notice) about collection to be given to individuals and how and when it will be communicated to them.

Use

Identify and describe how the organisation intends to use the information such as:

- all the planned uses of the personal information, including infrequent uses;
- whether the uses are consistent with the purpose for collection;
- proposed uses of the information for purposes other than the purpose of collection;
- whether there are choices for individuals about how their personal information is handled, and if so, whether you will inform them; or
- measures in place to prevent uses for secondary purposes or to ensure that any secondary uses are permitted by the IPPs or HPPs.

If information may be used for a secondary purpose, identify and describe:

- whether consent is required for the secondary use;
- if the use is related or directly related to the purpose of collection;

- whether an individual can refuse consent for secondary uses and still be involved in the project;
- any consequences for individuals who refuse consent; or
- how individuals will be involved in decisions if new, unplanned purposes for using personal information occur during the project.

Data linkage or matching, which involves aggregating or bringing together personal information that has been collected for different purposes, has additional privacy risks. If your project will involve data linkage or matching, identify and describe:

- any intention or potential for personal information to be data-matched, linked or cross-referenced to other information held in different databases (by you or other entities);
- how data-matching, linking or cross-referencing may be done;
- any decisions affecting the individual that might be made on the basis of data matching, linking or cross-referencing;

Disclosure

Identify and describe:

- to whom, how and why the personal information will be disclosed;
- whether the disclosed information will have the same privacy protections after it is disclosed;
- whether the information is to be published, or disclosed to a register, including a public register;
- whether an individual will be told about the disclosure and what choices they have (such as publishing or suppressing their information);
- whether the disclosure is authorised or required by law, and if so, which law;
- the people or organisations to which you usually or sometimes disclose personal information, and any further uses or disclosures that are made by those people or organisations; or
- whether the personal information will be disclosed to overseas recipients.

Information quality

Identify and describe:

- the consequences for individuals if the personal information is not accurate or up to-date, including the kinds of decisions made using the information and the risks of using inaccurate information;
- the processes that ensure only relevant, up-to-date and complete information will be used or disclosed, including by any contracted service providers; or
- how personal information updates will be given to others who have previously been given personal information about an individual.

Security

Assess the project against the organisation's IT, telecommunications and physical and organisational security safeguards.

Identify and describe:

- security safeguards that will protect the personal information from loss, unauthorised access, use, modification, disclosure or other misuse (including for contracted service providers);
- audit trails and other oversight mechanisms that will be in place;
- protections in place to ensure data linkage accuracy and that individuals will not be adversely affected by incorrect data matching;
- how information will be transferred between sites;
- how personal information will be protected if it will be managed by someone else;
- who will have access;
- who will authorise access;
- action that will be taken if there is a data breach.

Retention and disposal

Identify and describe:

- when personal information will be de-identified or destroyed;
- how this will be done securely;
- whether an information retention policy and destruction schedule is in place; or
- how compliance with this policy and any relevant legislation about record destruction will be assessed.

Access, accuracy and correction

Identify and describe:

- how individuals can access their personal information, including any costs to the individual;
- how the individual can have their personal information corrected, or annotations made, if necessary; or
- how decisions will be made about requests from individuals for access to or correction of their information.

Some jurisdictions suggest the use of tables or diagrams to map information flows.[22] The PIA can usefully consider the impacts on other types of privacy as well.[23]

7.5 Consult with stakeholders

The views of the stakeholders need to be considered in identifying and assessing privacy risks and in formulating options and recommending solutions to mitigate identified risks.

Consultation with stakeholders follows understanding the projects' privacy aspects and the use of personal and health information. Consultation can occur throughout the PIA process so that the necessary people are consulted at the appropriate time or as the project changes.

For consultation to be effective stakeholders need to be sufficiently informed about the project, be provided with the opportunity and time to provide their perspectives and to raise any concerns. Stakeholders need information to make an informed contribution to the identification of risks and proposed solutions.

There are a variety of ways to consult with stakeholders from written submissions to holding workshops to allow stakeholders to interact with one another and generate shared outcomes or identify key differences.

7.6 Check for compliance against relevant legislation

Once the personal information flows have been mapped, you can compare the project's personal, sensitive or health information handling practices against the privacy obligations set out in:

- the PPIP Act and HRIP Act and regulations;
- Privacy Codes of Practice and Public Interest Directions applicable;
- Commonwealth privacy legislation, if applicable;
- other legislation that applies to your agency relating to the collection, storage and security, access to and amendment of, use, disclosure and disposal of personal and health information;
- Organisational privacy policies, plans and other documentation.

Even if the project appears to be compliant with privacy legislation, there may still be other privacy risks that need to be addressed, such as community expectations.[24] Best practice is for organisations to publicly respond to submissions received.

7.7 Identify risks and possible remedial actions

Once the information flows have been mapped, you need to identify and critically analyse how the project impacts upon privacy (both positively and negatively) and develop actions that address adverse impacts to achieve compliance with privacy legislation and possibly meet community standards. These risks may be to individual privacy, to an entity's compliance and reputation, or both.

Taking into account the information obtained from the previous steps, analysis is required to:

- identify all possible privacy risks and who is likely to be affected by those risks, including individuals, groups and numbers of people who could be affected; and
- assess identified risks for their likelihood, frequency and consequence.

The risk assessment should include consideration of the content of the information and the context in which the information is collected. Even minimal personal information handled inappropriately may impact on someone's privacy in ways an organisation did not intend.[25] Also, some types of personal information are more sensitive than others, such as personal address, genetic, health or criminal conviction information.

Guidelines developed by the Office of the Australian Information Commissioner[26] suggest some key questions to consider at this stage.

They include:

- do individuals have to give up control of their personal information?
- will the project change the way individuals interact with the agency, such as through more frequent identity checks, costs, or different impacts on different individuals or groups?
- will decisions that have consequences for individuals be made as a result of the way personal information is handled in the project (such as decisions about services or benefits)?
- is there a complaint handling mechanism? If yes, is it visible, comprehensive and effective?
- how will privacy breaches be handled?
- are there audit and oversight mechanisms in place (including emergency procedures) in case the system fails?
- does the project recognise the risk of function creep? Is there an interest in using the personal information collected for the project for other purposes in the future?
- 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?
- is any intrusion fully justified and in proportion to the project's anticipated benefits? Is it the only way of achieving the aims of the project, and done in the least intrusive manner? Is it subject to legislative or judicial authority? What auditing and oversight measures are in place?
- how consistent is the project with community values about privacy? Has there been any community response to similar projects, or research into community attitudes about privacy and this project?
- Does the project collect more information than is needed? Use intrusive means of collection, or disclosing sensitive details more widely than necessary?

Ultimately, the risk assessment determines whether the project has acceptable or unacceptable privacy impacts.

The next step is to consider what action can be taken to resolve the privacy risks identified to ensure compliance with the PPIP Act and HRIP Act. This involves considering what options might enhance privacy protection or remove or minimise any negative privacy impacts identified through the PIA. [27]

The focus is on finding options that will address the privacy impact and still achieve the project's goals. Options may include:

- management and operational controls (for example, agency policies or procedures, staff training and accountability measures);
- technical controls (for example, access control mechanisms, authentication mechanisms, encryption methods and design changes); and
- physical controls (for example, lockable filing cabinets and limiting access to certain floors or areas).

The report needs to consider the dimensions of the remedial action and where there are multiple options to address a privacy risk, and evaluate the likely costs, risks and benefits of each option to identify which option is the most appropriate.

7.8 Formulate and consult on draft recommendations

The above analysis leads to a set of recommendations that include an action plan and timeline.

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

- changes to the project that would achieve a more appropriate balance between the

project's goals and protection of personal and health information and the privacy of citizens;

- 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.

Actively raise and discuss proposed recommendations with affected stakeholders before they are finalised to facilitate understanding of the issues and identify likely responses. Improvements may be identified and assist securing their commitment to the recommended actions.

7.9 Prepare and publish the report

The draft PIA report needs to outline the consultation process conducted, and be subject to consultation with relevant stakeholders, including the Office of the NSW Privacy Commissioner.

The PIA report needs to set out all the information gathered throughout the PIA, its findings and recommendations. The report demonstrates accountability and is an important public record.[28]

Key elements include:

- introduction and background information including the context of the project;
- project description;
- PIA methodology;
- a description of the information flows;
- results of the consultation with stakeholders;
- 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;
- recommendations to mitigate or avoid privacy risks; and
- 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, and if any approach is to be made to the Privacy Commissioner.

The format of the report is best tailored to suit the complexity of the project. It needs to be provided to the relevant delegate, governance body or project manager for approval before decision making processes commence.

It is best practice that agencies publish their PIA reports to demonstrate transparency and that the project has undergone critical privacy analysis, potentially reducing community concerns about privacy.

There may be circumstances when the full release of a PIA report may be inappropriate; for example, if the 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. Where these difficulties exist, consider releasing a summarised or edited version.

If possible, give stakeholders an opportunity to comment on the draft report and its recommendations and suggest improvements before it is finalised.[29]

The following is a template to guide the content to be included in the report. Depending on the PIA, not all components may be necessary and some not covered which should be included.

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 professional expertise) • key steps that were 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 projects • timeframes in which the project will be delivered • 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: • who was consulted • the method of consultation • the focus of the consultation • whether any further consultation will be necessary • what feedback was provided.
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 and risks to privacy protection more broadly • 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. Explanations are best placed in the section above. Recommendations can be in the Executive Summary or incorporated through the report.

7.10 Implement the endorsed recommendations

Following the receipt of the PIA report an organisation should consider and adopt a position on the recommendations.

At a minimum, the organisation needs to identify whether it will adopt, partially adopt, has already implemented or will not adopt any of the recommendations made by the PIA report. The organisation should provide reasons why they have not adopted the PIA recommendations if it chooses to do so. It is helpful to prepare an implementation plan for the approved recommendations, indicating who is responsible and the timeframe for implementation.

The organisation's response and agreed actions should be fed back into wider project management and risk management processes. It is recommended that identified risks be recorded in the project risk register or issues log so they are regularly monitored.

The recommended actions, responsibilities and timeframes should be reflected in the project plan to ensure that the activities necessary to implement the recommendations occur. There should be ongoing monitoring and assessment of identified risks and mitigation strategies, and, regular reports to the project sponsor on the progress of implementation of the PIA recommendations.

Publishing the findings of a PIA, together with the organisation's response to those recommendations, contributes to the transparency of the project's development and intent.[30]

7.11 Audit and review

Third-party review and audits can occur as part of consideration of the PIA report as well as following a decision on the PIA's recommendations.[31]

External review can have considerable benefits; it can give confidence to decision makers and identify failures to fully implement recommendations.

It is recommended that:

- organisations incorporate audits of PIA processes in their internal and external audit plans;
- maintain a register of PIA recommendations for future project planning and PIAs and to help identify systemic privacy issues. [32]

7.12 Update the PIA if there are changes in the project

Many projects undergo changes before completion. If changes create new privacy impacts not previously considered revisit the PIA and update it and put it back into organisational decision making processes. Depending on the magnitude of the changes, the organisation might need to revisit the PIA as if it were a new initiative. This might involve a new consultation with stakeholders. If the changes are only minor, the organisation might decide no change or additional consultation is needed.

7.13 Embed privacy awareness throughout the organisation and ensure accountability's

The organisation head is responsible for ensuring that all employees and contractors are aware of privacy laws and the obligations of the organisation, its employees and contractors it engages. This includes being sensitive to the privacy implications and the possible impacts on privacy of what they or their colleagues do.

Leadership of and support for the PIA process develops a privacy positive culture. An organisation with a supportive governance framework is more likely to make better use of the PIA mechanism.[33]

A PIA policy is a useful part of a wider business privacy strategy. Best practice standards are for organisations to explain their response to PIA recommendations or explain in the Annual Report or other mechanism.

For more information

Contact the Office of the Privacy Commissioner

PO Box R232, Royal Exchange, NSW 1225

Level 3, 47 Bridge Street, Sydney NSW 2000

Telephone: (02) 8258 0066

Email: privacy@ipc.nsw.gov.au

Website: www.ipc.nsw.gov.au/privacy

8 End Notes

[1] I Kroener and D Wright, 'A Strategy for Operationalizing Privacy by Design' (2014) 30(5) *Information Society* 335.

[2] See D Wright, R Finn and R Rodrigues, 'A Comparative Analysis of Privacy Impact Assessment in Six Countries' (2013) 9(1) *Journal of Contemporary European Research* 160; P De Hert, D Kloza and D Wright, *Recommendations for a Privacy Impact Assessment Framework for the European Union* (European Commission- Directorate General, 2013); K Wadhwa and R Rodrigues, 'Evaluating Privacy Impact Assessments: Innovation' (2013) 26(1/2) *The European Journal of Social Sciences* 161.

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

[4] Ibid, 162.

[5] Ibid.

[6] Office of the Australian Information Commissioner, (2014), op cit, 2.

[7] Office of the Australian Information Commissioner, (2014), op. cit., 3.

[8] Ibid. See also P De Hert, D Kloza and D Wright, *Recommendations for a Privacy Impact Assessment Framework for the European Union* (European Commission- Directorate General, 2013) 27.

[9] P De Hert, D Kloza and D Wright, (2012), op cit.

[10] Ibid, 17-20.

[11] Ibid, 17.

[12] For a summary of the research see D Wright, R Finn and R Rodrigues "Making Privacy Impact Assessment More Effective" (2013) 29 *The Information Society*, 307-315.

[13] International Standards Organisation (2016) ISO/IEC DIS 29134 Information technology -- Security techniques -- Privacy impact assessment – Guidelines, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62289

[14] Office of the Australian Information Commissioner, (2014), op cit, 7.

[15] New Zealand Privacy Commissioner (2007) *Privacy Impact Assessment Handbook*, Office of the Privacy Commissioner, Auckland, New Zealand, 14.

[16] Office of the Australian Information Commissioner (2014), op cit,7.

[17] Ibid, 8.

[18] Office of the Australian Information Commissioner (2014), op cit, 10.

[19] Ibid.

[20] Independence of PIA assessors has been identified in research as a feature of effective PIAs. See P De Hert, D Kloza and D Wright (2012), op cit, 21-22.

[21] Adopted from the Queensland Privacy Commissioner guide, *Guideline – Information Privacy Act 2009: Undertaking a Privacy Impact Assessment*.

[22] See for example, Office of the Information and Privacy Commissioner of Alberta, *Privacy impact assessment requirements*, Edmonton, Alberta. https://www.oipc.ab.ca/media/117453/guide_pia_requirements_2010.pdf, 22-24.

[23] R Finn, D Wright and M Friedewald, "Seven types of privacy," in S Gutwirth, R Leenes, P De Hert, et al (Eds) *European data protection: Coming of age?* (2013, Dordrecht, The Netherlands, Springer) 3–32.

[24] See P De Hert, D Kloza and D Wright, D (2012) op cit.

[25] Office of the Australian Information Commissioner (2014) op cit, 18.

[26] Ibid.

[27] Office of the Information and Privacy Commissioner of Alberta, Privacy impact assessment requirements, Edmonton, Alberta. https://www.oipc.ab.ca/media/117453/guide_pia_requirements_2010.pdf, 30 includes a risk mitigation table to assist in recording risks, mitigation strategies and any references to agency policies.

[28] P De Hert, D Kloza and D Wright (2012) op cit.

[29] This is recommended in research on leading contemporary international practice on PIAs. See for example, P De Hert, D Kloza and D Wright (2012), op cit.

[30] This is also recommended in the research on leading contemporary international practice on PIAs. See for example, P De Hert, D Kloza and D Wright, D (2012), op cit.

[31] Ibid.

[32] This is also recommended in research on leading contemporary international practice on PIAs. See for example, P De Hert, D Kloza and D Wright (2012), op. cit.

[33] Ibid, 21-22.

9. References

1. 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.
2. Information and Privacy Commissioner, Ontario, (2005) *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*, Toronto, Ontario.
3. Information Commissioner's Office (2014) Conducting privacy impact assessments code of practice, London, UK.
4. Information Commissioner's Office (2009) Privacy Impact Assessment Handbook (Version 2), London, UK.
5. Kroener, I and Wright, D A "Strategy for Operationalizing Privacy by Design" (2014) 30 (5) *Information Society*, 335-365.
6. New Zealand Privacy Commissioner (2007) *Privacy Impact Assessment Handbook*, Office of the Privacy Commissioner, Auckland, New Zealand.
7. Office of the Australian Information Commissioner (2014) *Guide to undertaking privacy impact assessments*, Australian Government, Canberra, Act
8. Office of the Information and Privacy Commissioner of Alberta, *Privacy impact assessment requirements*, Edmonton, Alberta. https://www.oipc.ab.ca/media/117453/guide_pia_requirements_2010.pdf
9. Office of the Information Commissioner, *Guideline: Information Privacy Act 2009, Undertaking a Privacy Impact 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.
10. Office of the Victorian Privacy Commissioner (2009) *Privacy Impact Assessments A Guide for the Victorian Public Sector*, Melbourne, Victoria.
11. Wadhwa, K and Rodrigues, R "Evaluating privacy impact assessments" (2013) 26 (1/2) *Innovation: The European Journal of Social Sciences*, 161-180.
12. Wright, D "Making privacy impact more effective" (2013) 29 (5) *Information Society*, 307-315.
13. Wright, D and Wadhwa, K (2012) *A Step-by-Step Guide to Privacy Impact Assessment*, presentation paper for the second Privacy Impact Assessment Framework (PIAF) workshop, Poland.
14. 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.