# Privacy Impact Assessments

## A guide for the Victorian Public Sector

Edition 2 – April 2009

privacy victoria

Office of the
Victorian Privacy
Commissioner

*COVER PHOTO: www.istockphoto.com*

# Table of Contents

# Introduction

Privacy Impact Assessments, known as PIAs, are one of the fundamental components in the protection of individual privacy. They assess the privacy impact of any new or amended project or process and identify ways in which any negative impacts can be mitigated and any positive impacts enhanced. As such, they should be an important part of the risk management and planning processes of all organisations. The importance of PIAs was reflected in the Australian Law Reform Commission's report on Australian Privacy Law and Practice *For Your Information* released August 2008 which recommended that Commonwealth agencies be required to carry out PIAs where directed to by the Privacy Commissioner.

This revised guide and its accompanying documents is primarily aimed at the Victorian public sector: those organisations and individuals subject to the *Information Privacy Act 2000 (Vic)* and the *Charter of Human Rights and Responsibilities Act 2006 (Vic)*. However, it may assist anyone undertaking a PIA.

The guide is not intended to cover the *Health Records Act 2001 (Vic)*. If your organisation handles health information, you will need to comply with the Health Privacy Principles (HPPs) in that Act as well. Advice on compliance with the HPPs should be sought, in the first instance, from the Office of the Health Services Commissioner, which regulates the handling of health information in Victoria.

This office first published a Guide to *Privacy Impact Assessments* in 2004. While this second edition has built on that work, much has changed in the intervening years.

The *Charter of Human Rights and Responsibilities* now means that privacy considerations need to be broader than compliance with the *Information Privacy Act*, as the right to privacy in the Charter covers not just information privacy, but bodily, territorial, locational and communications privacy. As well, PIAs are now more common in Australia and around the world, so there is much greater breadth and depth of experience to draw upon, in order to make the guide more practical and effective.

This new edition will hopefully achieve this. It includes more practical tools for use in actually commissioning or conducting a PIA: in particular, a template PIA Report and *Accompanying Guide* comprehensively identify privacy risks and mitigation or enhancement strategies, including guidance on identifying and complying with *Charter* obligations. There is more emphasis on public consultation and measuring community expectations– an important part of any thorough PIA .

Some of the tools may appear disconcertingly long. Don't be discouraged by this. In order to be comprehensive and thorough, every possible privacy impact has been included. However, not all impacts will apply to every project or process. The tools are intended to be modified to suit your particular project. The template PIA Report is available as a Word document on our website, to allow for it to be used in this way.

This second edition was revised by Anna Johnston of Salinger Privacy. Anna is the former New South Wales Deputy Commissioner. Since establishing the consulting firm Salinger Privacy she has conducted many PIAs and privacy audits. This revised Guide and accompanying documents reflect her experience. I would also like to thank a number of privacy officers from the Victorian public sector who volunteered their time as a focus group to assist Anna in identifying the needs of the sector and review drafts: Christina Agiannitopoulos (Department of Human Services), Kathy Bramwell (RMIT), Melanie Casley (Department of Justice), Leanne Crowe (Department of Transport), Andrew Fitzgerald (Victoria Police), George Karaisaridis (WorkSafe Victoria), Sandra Pickett (Kingston City Council), Bryan Sketchley (Department of Education and Early Childhood Development), and Jeff Warren (Department of Human Services).

I hope that all organisations will find the guide and accompanying tools useful and make PIAs an integral part of any projects that involve the handling of personal information. And our staff are always available to advise those undertaking or considering a PIA.

Helen Versey
Victorian Privacy Commissioner
April 2009

# What is a PIA?

## Definition

Privacy Impact Assessment (PIA) has been defined as "an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated".[1]

A PIA considers the future consequences of a current or proposed action, and looks to prevent or minimise any negative impacts on privacy.

In designing or managing any project or system, there may be several competing public interests to be considered, including the protection of privacy. Decision-makers need tools to assist them to get the balance right. A PIA is one such tool.

Where legal rights and obligations are affected, the reassurance offered by a PIA can be important as a risk management tool and as a way of building trust.

## Risk management

"Impact" itself is a neutral term. Privacy impacts can be positive (privacy-enhancing) or negative (privacy-invasive). A PIA should examine both, but primarily the focus will be on the negative impacts.

Privacy "risk" means the risk that a project will not comply with privacy laws, will not meet community expectations, or will have unmitigated or unnecessary negative impacts.

A PIA can give confidence to those taking action–and those who will be affected by it–that the impact on privacy has been considered, and any risks arising have been appropriately addressed.

In other words, a PIA is a tool which should offer both a diagnosis of a project's well-being in terms of its privacy impacts, and a prescription of ideas to help treat any problems diagnosed.

Privacy risk can be avoided or mitigated by:

- ensuring a project complies with the law;
- ensuring a project meets community expectations;
- making a project less privacy-invasive; and
- making a project more privacy-enhancing.

As with any process of risk management, you may not be able to eliminate or mitigate every risk, but ultimately you have to judge whether the public benefit to be derived from the project will outweigh the risk posed to privacy.

**A PIA is a tool which should offer both a diagnosis of a project's well-being in terms of its privacy impacts, and a prescription of ideas to help treat any problems diagnosed.**

[1] Blair Stewart, "Privacy Impact Assessments", (1996) 3 *Privacy Law + Policy Reporter* 61, 62.

# Is a PIA needed for our project?

This guide uses the word "project" to encompass any type of proposed undertaking–it could be a project, process, system, legislation, program, service, database, application, initiative, policy or procedure.

The project need not be new; it might be a proposal to subtly change an existing system or legislation, which might lead to new ways of handling personal information, or new data-sharing.

Nor does the project need to be large; the size or budget for a project is not a useful indicator of its likely impact on privacy.

The project does not even need to involve recorded "personal information" as defined under the *Information Privacy Act*; a program that may include the need for bodily searches can still impact on privacy even if no personal information is recorded, and therefore the right to privacy in the Charter of Human Rights and Responsibilities needs to be considered.

A simple Threshold Privacy Assessment should therefore be routinely conducted for every project in your organisation.

## Threshold Privacy Assessment

A Threshold Privacy Assessment is a brief, initial consideration of a project, to determine whether its potential privacy impacts necessitate a PIA. Appendix A sets out a series of 17 simple yes/no questions to be asked of any project. This Threshold Privacy Assessment is designed to be completed by a relevant project officer; no privacy knowledge is required.

If the answer to one or more of the 17 questions is "yes", then a PIA should be seriously considered.

Once you have completed your Threshold Privacy Assessment, a signed and dated copy should be provided to your organisation's Privacy Officer, as well as kept on your own project file. You can then discuss with your Privacy Officer whether or not a PIA is needed, what form it might take, and what level of involvement each party should have.

## Communicating the need for a Threshold Privacy Assessment

Ensuring that every project in an organisation at least undergoes a Threshold Privacy Assessment poses a challenge for the Privacy Officer.

Privacy assessment can be incorporated as a step in your organisation's risk management procedures for large and "new" projects. Smaller projects, or those involving modifications rather than entirely new proposals, might be more difficult to find or influence.

For the Privacy Officer the task will involve reaching the right people in the organisation, who can influence how projects are conducted in their area. These might include not only IT project managers, but managers across a number of areas of responsibility - human resources, legal and policy, programs or operations, even facilities management. Obtaining support from senior management is also important; up-front commitment from an organisation's executive to the conduct of PIAs whenever they are needed is the first step in ensuring buy-in to the eventual PIA's recommendations.

There are many ways you can communicate the need for Threshold Privacy Assessments across your organisation. Some options include:

- risk management and audit committees;
- induction training for new staff;
- internal workshops for project managers and IT staff;
- training or presentations during Privacy Awareness Week;
- policies or notices on the intranet; and
- staff noticeboards or newsletters.

You may need to highlight the benefits for each project and the organisation of conducting a PIA. Some of those benefits are outlined below.

# Why should a PIA be done?

The primary object of a PIA is to allow any negative privacy impact to be weighed properly against whatever benefits the project offers in the public interest.

## Value to organisations

Building-in good systems and processes from the start is less expensive or time-consuming than trying to retrofit later.

A Privacy Impact Assessment is often described as an "early warning system" for your organisation. It allows you to detect potential privacy problems, take precautions and build tailored safeguards before, not after, you make heavy investments in time and perhaps in technologies. PIAs help identify inherent privacy risks that may be costly to address later in the project.

The PIA affirms that privacy issues have been addressed and that reasonable steps have been taken to provide an adequate level of privacy protection at the time of assessment. The PIA also provides a mechanism for reviewing the privacy impact of projects as changes occur.

The object of a PIA is not to "sell" an idea that may have negative privacy impacts. The primary object of a PIA is to allow any negative privacy impact to be weighed properly against whatever benefits the project offers in the public interest. The *Information Privacy Act* aims at a balance, in particular circumstances, between the public interest in the free flow of information and the public interest in privacy. That said, a by-product of a good PIA may well be that it helps reassure people that a trade-off of privacy is worth it, or that promised safeguards can work.

A PIA can benefit an organisation because it:

- helps to ensure compliance with the Information Privacy Principles (IPPs) in the *Information Privacy Act*;
- helps to ensure compatibility with the Charter of Human Rights and Responsibilities;
- assists in anticipating and responding to the public's possible privacy concerns;
- exposes any internal communication gaps or hidden assumptions about the project;
- promotes awareness and understanding of privacy issues inside the organisation;
- helps reduce cost later in management time, legal expenses and potential media or public concern by considering privacy issues early;
- enhances informed decision-making at the right level; and
- enhances the legitimacy of a project, especially where some compromise or trade-off is necessary.

The fact of having done a PIA itself may also assist in demonstrating compliance in the context of a subsequent complaint, privacy audit or compliance investigation. Imagine that your organisation suffers a security breach and personal data goes missing or turns up in the wrong hands with harmful consequences. If individuals complain under the *Information Privacy Act*, an organisation will be in a better position if it can show it considered in advance its data security risks and analysed the potential for unauthorised disclosure or misuse. Although the protections may have failed in the particular instance, the PIA will be evidence of advance consideration of data security and other privacy issues.

Once you have been through the PIA process, you will be able to assess the privacy risks associated with your project. You can then determine whether the risks are avoidable, what options you have and what cost effective steps can reduce them to an appropriate level. The final decisions about where the balance lies will be for the appropriately senior decision-makers. But the first steps are to diagnose for them what the risks, benefits, costs and safeguards are–this is primarily what a good PIA will do.

Implementing the PIA process in your organisation will also demonstrate to employees and contractors that data protection is taken seriously and that it needs to be thought about into the future.

## Essential risk management

The Victorian Government *Risk Management Framework* requires all department and agency heads to attest in their annual reports that they have risk management processes in place, consistent with the Australian/New Zealand *Standard AS/NZS 4360: 2004*, and that a responsible body or audit committee verifies that view.

Robust project management methodologies include planning and business case phases, incorporating consideration of the regulatory environment. PIAs should form part of the risk evaluation and management tasks for any substantial undertaking.

PIAs should therefore be seen as part of the essential toolkit for organisations to identify, assess and manage risks arising from new projects, in relation to compliance with the *Information Privacy Act*, the Charter of Human Rights and Responsibilities, and community expectations about how privacy will be protected.

## Compliance with the law

Privacy law is known as “fuzzy law”, with organisations expected to comply with broad-based privacy principles, which use tests such as “what is reasonably necessary?”.

For example, IPP 4 (data security) doesn’t say “protect data by using X brand software”; it says “take reasonable steps to protect the personal information (your organisation) holds from misuse and loss and from unauthorised access, modification or disclosure”. IPP 1 (collection) doesn’t say “you can collect information about a person’s gender but not their age”; it says you “must not collect personal information unless the information is necessary for one or more of (your organisation’s) functions or activities”.

It is difficult for an organisation to demonstrate its compliance with the IPPs unless it has conducted some assessment of the situation, examining and ruling out all other alternatives to the proposed course of action. Only then can an organisation say with confidence “yes, this collection of personal information is reasonably necessary”.

A PIA can therefore provide assurance that the 10 IPPs have been taken into account at all stages of the development of a project.

## The Charter of Human Rights and Responsibilities

A PIA can also help ensure compatibility with the Charter of Human Rights and Responsibilities, which includes a right to privacy that is broader than just the information privacy covered in the 10 IPPs. Section 13 of the *Charter of Human Rights and Responsibilities Act* expressly grants each person the right not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with, or reputation unlawfully attacked.

The Charter does not provide any new avenue of redress for individuals who believe their privacy has been breached. But it does impose an obligation on all public authorities to act in a way that is compatible with the human rights protected by the Charter. Importantly, it requires that all statutory provisions, whether enacted before or after the Charter, be interpreted so far as is possible in a way compatible with human rights. It gives the Supreme Court the power to declare that a statutory provision cannot be interpreted consistently with a human right and to require the relevant Minister to respond to the declaration. The Charter also requires statements of compatibility to accompany all Bills introduced into Parliament.

The dimensions of privacy that need to be considered are:

- bodily privacy (to protect the integrity of the physical person);
- territorial privacy (to protect personal space, objects and behaviour);
- communications privacy (to protect against eavesdropping);
- locational privacy (to protect against surveillance); and
- information privacy (to protect personal information).

## Value to the public

Respect for privacy upholds the dignity of the individual, and promotes trust. The Australian Privacy Commissioner has noted the benefits of conducting a PIA:

> *Conducting a PIA provides agencies with the opportunity to consider the values the community places on privacy–trust, respect, individual autonomy and accountability–and to reflect those values in the project by meeting the community's privacy protection expectations.*[2]

A proper PIA can give the general public confidence that their privacy has been adequately considered and addressed. Demonstrating that your organisation has identified and managed privacy issues in a particular project builds and sustains trust with the public and other agencies. If you demonstrate that you take privacy seriously, you are demonstrating respect for people. People who are confident that they and their privacy are respected are more likely to provide the information and co-operation that will make your projects successful. The PIA should be seen as a source of information and action to allay fears about loss of privacy or about protection of personal information. It can also assist in anticipating public reaction to the privacy implications of a given proposal.

One of the primary objects of the *Information Privacy Act* is to increase transparency in the handling of personal information by the public sector. Releasing a PIA Report gives the public an opportunity to express concerns and have them addressed before a project has been implemented.

---

[2] Office of the Privacy Commissioner (Australia), *Privacy Impact Assessment Guide*, August 2006, p.6.

# When should a PIA be done?

Having decided to do a PIA, consider its timing.

The point of a PIA is to influence decision-making on a project. The timing of the PIA must therefore be early enough so that the findings and recommendations can influence the final design of, and thinking about, the project.

Ideally, a PIA should be initiated at the early stages of project development and planning. Your early consideration of privacy issues through the PIA will be a factor in the allocation of resources needed for a project and should prevent unnecessary effort being expended on options incompatible with the IPPs or Charter of Human Rights and Responsibilities.

Often, a PIA will be useful more than once in the project's life. The PIA should be dynamic, updated as changes are contemplated to projects. It should be revisited at various times throughout the project development. The PIA will then form an integral part of project management and decision-making processes. In this sense, PIAs are a practical tool for making data protection part of an organisation's culture, so that in time it becomes a more automatic and reflex action.

If in doubt, err on the side of starting the PIA as soon as possible. If there are fundamental flaws, you need to know about them sooner rather than later. If necessary, conduct a preliminary PIA, which should be clear about saying "this is early days, here's a set of assumptions we're working from, but things may change". Of course this means you will need to revise the PIA later on, and perhaps even do another one.

**EXAMPLE: IT projects**

Sometimes the privacy risks cannot be identified until it is known what proprietary software is going to be used, and that won't be decided until the project is put out to tender. You shouldn't wait until then to do the PIA, because ideally the PIA results should feed into your tender specifications. That may mean that the preliminary PIA has to work from certain assumptions, perhaps based on your knowledge of how the leading software products would operate. You would then conduct a final PIA once the software has been chosen.

Another factor which suggests starting your PIA early is how long it will take. Whether you plan to conduct your PIA in-house or use an external consultant, be realistic about the time needed to set the terms of reference for the PIA, get the right people involved, gather all the necessary information, organise internal and external consultations, conduct the analysis and prepare a PIA Report. A comprehensive PIA on a significant or complex project may take between 20 and 60 business days, perhaps spread over a few months.

**Ideally, a PIA should be initiated at the early stages of project development and planning.**

# Who should do the PIA?

## Choosing the right people

The skills required to undertake a PIA will vary depending on the project being evaluated but, in general, analytical and writing skills will be required. Other skills that may be useful, depending on the project, include facilitating stakeholder consultation, the ability to test IT systems, and knowledge relevant to your sector.

A PIA can be performed by:

- an individual from within the organisation;
- a team or section from within the organisation;
- a joint team or working group if more than one organisation is involved in a project;[3] or
- an external consultant.

The "Privacy Impact Assessor", whether an individual or a group, needs to be familiar with the Information Privacy Principles and the broader dimensions of privacy, and be able to help others understand them. Finding the right people with the right skills will make the PIA process easier and quicker.

Using the organisation's own resources and personnel to conduct the PIA gives the organisation a sense of ownership of the PIA. It uses and builds experience and internal expertise to identify privacy issues and to handle later what the PIA process identifies or anticipates.

External consultants with particular skills may be brought in to conduct the PIA, or to assist with certain aspects. In either case it will still be important for the organisation to have overall responsibility for the PIA.

The nature and size of the project may determine whether an internal individual or team conducts the PIA, with or without external specialist advice. By-products of doing a PIA internally are the way it grows and reinforces the organisation's knowledge base about privacy and data protection, and (depending on the seniority of the lead Assessor) the way it signals to the organisation's staff the significance that senior management attaches to getting privacy right.

Where the PIA is undertaken by staff rather than a specialist external consultant, you may wish to consider incorporating external opinion on the result before finalising the PIA. Outsiders often ask useful questions that insiders have not considered because of their familiarity or assumptions. Some independent external involvement may also be useful in building public confidence in the PIA later.

[3] Another approach for joint projects is for each participating organisation to conduct their own PIA. The benefit of this approach is that each Assessor will have greater expertise in his/her own area. The downside is that this approach can lead to duplication of effort. If you do take this approach, ensure there is clear responsibility assigned to one organisation to bring together the different PIAs for comparison and final decision-making.

# Who else should be involved?

The categories of who you might involve in your PIA process will include:

- internal stakeholders–such as project managers, IT and records management personnel;
- internal or external specialist advisers–such as your privacy officer, legal team, privacy consultants and the Office of the Victorian Privacy Commissioner (Privacy Victoria); and
- external stakeholders–such as partner organisations, suppliers, clients, non-government organisations representing your clients and/or the advocates for the public interest.

## Internal stakeholders

The involvement of project or program managers will be essential for the PIA process. These are the people who know the project and the operational environment best. Project managers will need to supply the Assessor with project and contextual documentation such as the business case and business requirements, and be prepared to explain and answer questions about likely data flows, accountability and governance structures, and stakeholder relations.

### INFORMATION TECHNOLOGY

For most projects, IT staff will need to be involved, and be prepared to explain and answer questions about data security relating to the project or the organisation at large. This might include technical architecture, network security, online applications, and backup procedures. IT staff will be particularly useful when developing end to end data flow diagrams.

### PROCUREMENT

If the project will involve the procurement of technology or other goods or services, involve your procurement officers, to ensure that privacy considerations are included in the drafting of tender documents as well as the evaluation of tender responses.

### RECORDS AND FACILITIES MANAGEMENT

Also consider involving your records managers, who can advise on how information is stored and disposed of. Facilities managers can also provide advice on how physical security is managed for the organisation.

### HUMAN RESOURCES

Human Resources managers should also be involved if the project will involve employee records.

### LEGAL

To properly assess the legislative backdrop that applies to your project, and ensure you can proceed lawfully, include your legal team in the conduct of your PIA. Your legal team should examine any particular provisions applying to your organisation which deal with secrecy, confidentiality, or other restrictions on the collection, storage, use or disclosure of personal information.

## Privacy Victoria

You should also consider consultation with Privacy Victoria early in the project's development and design. Privacy Victoria has an advisory role, but cannot conduct a PIA for you. Our staff can assist with advice on whether a PIA is needed and whether an external consultant is warranted. More importantly, we can sometimes provide a brief overview of potential problems under the *Information Privacy Act*, or even identify easy solutions to mitigate your privacy risks.

Whether you choose to consult with Privacy Victoria will depend on the likely significance of the privacy risks involved with your project. Features suggesting the project should involve consultation with Privacy Victoria include:

- if there is a large amount of personal information at issue;
- if the personal information at issue includes sensitive information;
- if there will be sharing of personal information between organisations;
- if any personal information will be handled by a contracted service provider;
- if any personal information will be transferred outside Victoria; or
- if there is likely to be public concern about actual or perceived impact on privacy.

## External stakeholders and public consultation

If your project will involve more than one organisation, including contracted service providers or other third party services, your PIA should consider the privacy risks arising from those organisations too. Consultation with any partner organisations or suppliers will therefore be necessary.

More broadly, "external stakeholders" will refer to your clients, or the public at large. Public consultation as part of the PIA process not only allows for independent scrutiny, but also generates confidence amongst the public that their privacy has been considered.

The PIA itself may not be the proper vehicle for public consultation for every project. Transparency may come at a later stage than the PIA itself, but the contents of the PIA will very often assist the subsequent consultation. (See further below on whether to publish your PIA Report.)

However a PIA should assess not only a project's strict compliance with privacy and related laws, but also public concerns about the wider implications of the project. The need to examine issues beyond compliance with privacy laws is partly because in many respects, the IPPs defer to other legislation that authorises or requires certain data to be collected, used or disclosed.

As a result, the critical question is not necessarily whether or not the project will comply with the letter of the relevant privacy laws, but whether or not it will meet the spirit or intent of the privacy principles, and community expectations about privacy and about your project.

**Public consultation can also sometimes generate new options or ideas for dealing with a policy problem, or may even suggest that the policy problem is not so great as first supposed.**

Matters that may influence your decision to undertake a public consultation as part of conducting the PIA might include:

- whether there is likely to be public concern about actual or perceived impact on privacy;
- whether there are a large number of people whose privacy is affected, or a particularly vulnerable group;
- whether your initial thinking indicates that new formal authority will need to be obtained for the collection and handling of personal information that the project envisages;
- whether there is already a formal consultation process into which the privacy aspects can be incorporated; and
- the need to build trust in a new practice or a new technology.

Public consultation can also sometimes generate new options or ideas for dealing with a policy problem, or may even suggest that the policy problem is not so great as first supposed. For example, your clients may place far less value than you expect on a project's objectives of "convenience" or "improved customer service", if a privacy trade-off is part of the equation.[4]

The UK Information Commissioner has identified a number of benefits attributable to conducting public consultation:

- "gathering of information about the privacy impacts of a project from all relevant perspectives;
- assisting the exchange of information among the participants;
- emergence of mutual appreciation by the various groups of one another's perspectives;
- identification of issues;
- creative construction of possible solutions;
- gaining of feedback about the acceptability of the possible solutions to the affected parties;
- avoidance of problems being discovered at a late stage of the project, when all possible solutions are expensive;
- avoidance of credible complaints being made at a late stage by affected parties that they were unaware of the project, or particular features, or of its impacts; and
- assurance that all relevant parties have the opportunity to contribute to the PIA, are seen to have that opportunity, and perceive themselves to have had that opportunity".[5]

If widespread public consultation is not an option, consider more targeted consultation with your stakeholders, by approaching groups which represent your client base or the wider public interest, or which have expertise in privacy, human rights and civil liberties.

---

[4] See the focus group research from the UK, outlined in Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006, at part 4:25

[5] Information Commissioner's Office (United Kingdom), *Privacy Impact Assessment Handbook*, December 2007, p.39.

# How is a PIA done?

A PIA involves describing a project, assessing its likely impacts on privacy, and making recommendations to minimise privacy risks. The output of the PIA process is a PIA Report.

A PIA for the Victorian public sector should assess compliance with the *Information Privacy Act* ("personal information"), as well as the *Health Records Act* ("health information") and the right to privacy in the Charter of Human Rights and Responsibilities.

## Structuring the PIA Report

Your PIA Report might have a Table of Contents that looks something like this:

- Description of the project;
- Description of the data flows;
- Analysis against the IPPs;
- Analysis against the other dimensions to privacy;
- Analysis of the privacy control environment; and
- Findings and recommendations

A Template PIA Report that any organisation may adopt and use, according to your circumstances is available. Not all of the template will be relevant to your project, but the template includes instructions throughout to assist you to determine how best to conduct your PIA.

Even if you decide to engage an external consultant to conduct the PIA, the Template PIA Report could be useful when drafting the terms of reference for the consultant.

## Scope of the assessment

Regardless of whether the PIA is to be conducted by an internal team or external consultant, you should develop some terms of reference (e.g. in your Request for Quotation [RFQ]). Ensure your terms of reference are not overly narrow. A PIA should allow for assessment of a project's potential future uses, foreseeable project expansions, or likely changes in structure, scope or governance. Knowledge of what is intended to happen with the project in the future, or what is reasonably likely to happen, should influence the project's up-front design.

A PIA for the Victorian public sector should assess compliance with the *Information Privacy Act* ("personal information"), as well as the *Health Records Act* ("health information") and the right to privacy in the Charter of Human Rights and Responsibilities.

Depending on the project, you may also need to consider your obligations under laws such as the *Freedom of Information Act 1982 (Vic)*, *Surveillance Devices Act 1999 (Vic)*, the *Public Records Act 1973 (Vic)*, the *Telecommunications (Interception) Act 1979 (Cth)*, and secrecy provisions or other restrictions in your own legislation. Indeed your own legislation may place greater restrictions on your project than the *Information Privacy Act* does.

## Measuring community expectations

Ensuring your project complies with the law may not be enough. The New Zealand Privacy Commissioner has noted that:

> *Proposals may be subject to public criticism even where the requirements of the Act have been met. If people perceive their privacy is seriously at risk, they are unlikely to be satisfied by (an organisation) which justifies its actions merely by pointing out that technically it has not breached the law.*[6]

To protect your project you will therefore need a solid understanding of public perceptions and community expectations.

The best way to measure community expectations about your project and its impacts on their privacy is by conducting public consultation or research as part of the process of conducting your PIA. However consultation and/or research is not always feasible, for reasons of cost, time, or sensitivity.

If widespread consultation is not an option, consider more targeted consultation, by approaching groups which represent your client base or the wider public interest, or which have expertise in privacy, human rights and civil liberties.

You may also be able to make assumptions about community expectations by examining what has worked and what hasn't in similar projects in your organisation in the past; or what occurred in peer organisations which have implemented similar projects.

Another option is to look to existing research sources about community attitudes towards privacy; there may be research or policy conclusions that apply to your project. The following sources are particularly rich in insights, but you may be able to find more:

- Privacy Victoria, *Privacy in Diverse Victoria: Research report into attitudes towards privacy in diverse communities*, October 2002;
- "Community Attitudes Towards Privacy" surveys, prepared in 2001, 2004 and 2007 for the Office of the Federal Privacy Commissioner; available from www.privacy.gov.au;
- Australian Law Reform Commission, Report 108, *For Your Information: Australian Privacy Law and Practice*, 2008; in particular see part 67 on children's and young people's attitudes towards privacy; and
- focus group research from the UK, outlined in Privacy Victoria, *Guidelines to the Information Privacy Principles*, September 2006, at part 4:25.

## Description of the project

Your PIA Report should work as a stand-alone document, which explains to the lay reader what the project involves, what it is intended to achieve, and how it will work, as well as its privacy impacts.

The PIA Report should therefore begin with a description of the project's objectives, drivers, scope, environment, and operational details. The Template PIA Report explains a little more about what should be included under each of these headings.

---

[6] Office of the Privacy Commissioner (New Zealand), *Privacy Impact Assessment Handbook*, June 2007, p.24.

## Mapping the personal information data flows

The IPPs focus on the life cycle of personal information, from collection through to disposal. Working through the life cycle of the information will help you determine at which points decisions are made and where privacy becomes particularly vulnerable.

The PIA Report should therefore describe the project in terms of:

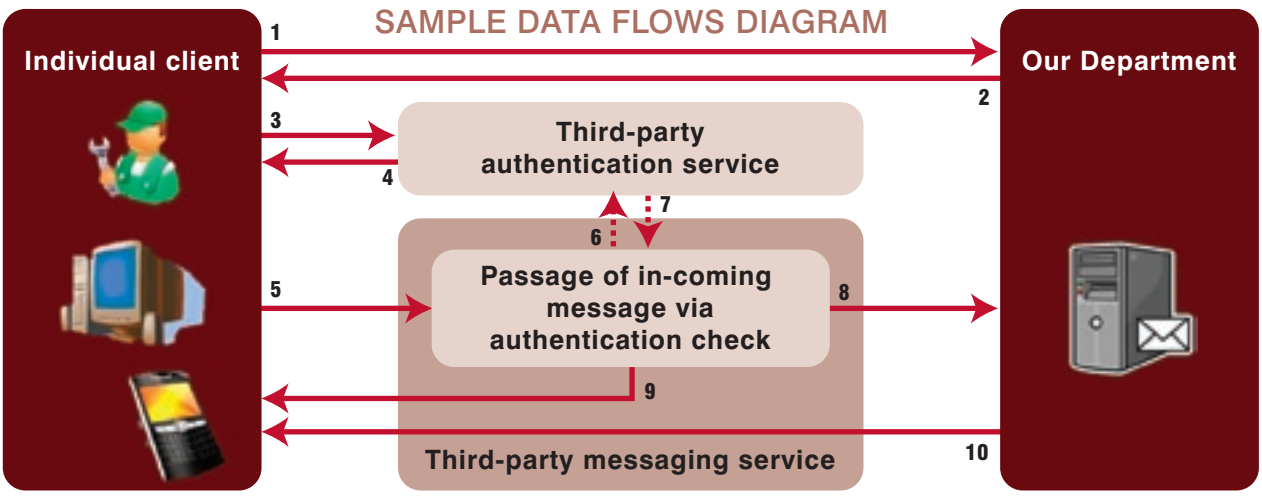
- collection (the type of personal information collected, the original source of the information, and the circumstances for collection);
- use (the processing of the information, and its intended uses);
- disclosure (who the information will be distributed to, for what purposes or in what circumstances);
- data quality (how the quality of personal information will be assured);
- data security (the safeguards that will operate against misuse, loss, unauthorised access, modification or disclosure, including at disposal); and
- access and correction (how individuals will be able to access and, if necessary, correct their personal information).

The Template PIA Report explains what should be included under each of these headings.

Diagrams depicting the flow of personal information can be particularly valuable in a PIA Report to illustrate how personal information is likely to 'flow' as a result of the project. You might consider one version showing how things work now, and a second version showing how things are intended to work if the project is implemented according to its current design.

Data flow diagrams should show each business unit and organisation involved in the project, including contracted service providers and other jurisdictions, and show how personal information will move between those units. You may need an accompanying table to explain the diagram and provide more detail.

An example is provided below of a project to implement reporting communications between a Department and its clients via email or SMS, with third parties providing the authentication and messaging services. The project features initial client registration (steps 1-2), initial enrolment and identification for the new system (steps 3-4), the passage of a report coming into the Department (steps 5-8), a receipt communication (step 9) and a confirmation communication (step 10).



## Assessing the privacy risks

Risks to privacy can arise in many circumstances. Collecting excessive information, using intrusive means of collection, or disclosing sensitive details more widely than justified, all involve risks both to individuals' privacy and to the organisation's compliance and reputation.

Much analytical work will be required to identify the privacy risks arising from your project, and find ways to mitigate those risks. Assessors should follow the motto "plan for the worst, hope for the best". Think about ways that things could go wrong–how data could be misused for example–and then design systems and processes to minimise the risk of that happening.

If you are doing a PIA well, the Assessor should be posing some tough questions for the project team, such as:

- why is each piece of data needed?
- can we get rid of some of it?
- how can we protect it? and
- what will people's expectations be about how we will use or disclose it?

To identify privacy risks you will need to analyse your project as against each IPP in some detail. To assist in this process, the Template PIA Report's *Accompanying Guide* lists common risks associated with each IPP, and the other dimensions to privacy.

Not every risk listed in the Template PIA Report's *Accompanying Guide* will be relevant to your project. Nor will every risk associated with your project be found there–you may uncover many other privacy issues.

Also consider what has worked and what hasn't in similar projects in your organisation in the past; and in peer organisations which may have implemented similar projects.

## Mitigating the risks

A PIA is not just about identifying privacy risks. It should come up with solutions or strategies to mitigate those risks. When developing your recommendations, keep in mind a few basic strategies:

- ensure the project has a sound justification with a public benefit;
- minimise the personal information you collect to only what is absolutely necessary;
- maximise transparency about what personal information you will be collecting, storing, using and disclosing;
- limit uses and disclosures of the information; and
- protect data security.

Recommendations to mitigate privacy risks can work off one or more levers:

- IT design;
- Legislation;
- policies and procedures;
- transparency (internal and/or external communication);

- staff training; and
- accountability measures.

See the Template PIA Report's *Accompanying Guide* for further ideas on risk mitigation strategies associated with each privacy principle, and the other dimensions to privacy.

## Concluding the Report

Your PIA Report should conclude with a summary or overview of the most significant findings, in relation to both privacy risks and privacy-enhancing features.

Also include an overview of the critical recommendations, to highlight which privacy risks can be mitigated by following your recommendations.

Conclude with an overview of which privacy risks cannot be mitigated, the likely public reaction to such risks, and whether the risks are outweighed by the public benefit in the project proceeding nonetheless.

# What should be done next?

## Doing the right follow-up

Typically, the Assessor will give the PIA Report to a project executive or team. A presentation can also be helpful to engender understanding of and support for the Report's recommendations.

Decisions will need to be made about the PIA Report's recommendations. Using a Project Action Plan, such as the sample version included in the Template PIA Report, offers one way to keep track of the acceptance and implementation of each recommendation. Another option is to add the significant risks identified in the PIA to your organisation's Risk Register.

The privacy issues identified will likely need addressing to ensure the project complies in the most efficient and confidence-building way. For example you may need to:

- seek legislative change to your own Act. For example, for some new project you may be proposing to use or disclose personal information already collected for unrelated, different purposes, and you may need to get the new use/disclosure properly authorised by an express amendment;
- clarify that the appropriate decision-makers have given clear authority for what is envisaged and that they have the requisite power under law to do so; and
- make changes to existing organisational processes and systems. For example staff may need to be retrained, information systems modified or different accountability measures introduced.

Some privacy risks of the project are likely to continue and consideration needs to be given to how these will be managed. In particular you will need to determine who will be accountable for future privacy management of the project after the project's set-up team moves on and the operation perhaps becomes "routine".

This is especially important if the project was developed by consultants, who will leave with their knowledge unless the project requires clear hand-over arrangements. Consideration also needs to be given as to how changes that occur during the life of the project will be handled, such as when and how will the PIA be updated and reviewed.

## Publishing the PIA Report

The *Information Privacy Act* emphasises the transparent handling of personal information. In the PIA context, that suggests publishing your PIA Report.

However in particular projects, security may be a consideration. A good, thorough PIA Report may necessarily analyse the data security weaknesses of a project in order that they can be minimised. To make the Report public may undercut the precautions taken and the ultimate aim–better data security. In such cases, a properly edited PIA Report will usually suffice to balance the security and transparency interests.

If you publish your PIA Report, it can be used as a springboard for running stakeholder or public consultation. This means that your PIA Report must work as a stand-alone document, so it should clearly explain the project in plain language.

One option is to publish both the PIA Report and the organisation's initial response to its recommendations, and then seek feedback through consultation on whether the proposed response is acceptable to your stakeholders. Broader questions may include whether the project should proceed, or which option/s to follow. This process can improve public understanding of your initiative, and engender the kind of public trust you will need to succeed.

A published PIA Report, especially if prepared externally, can also help to clear up any public "myths" about the project, by providing a credible, independent source of information and analysis.

Regardless of whether you publish your PIA Report to the world at large, if you consulted previously with Privacy Victoria, or if you have identified significant privacy impacts, we would appreciate being forwarded a copy.

# APPENDIX A: Threshold Privacy Assessment

Privacy Victoria recommends that this simple Threshold Privacy Assessment be routinely conducted for every project in your organisation.

If the answer to one or more of the questions below is "yes", then a Privacy Impact Assessment should be seriously considered.

| WILL THE PROJECT INVOLVE … | YES | NO |
|---|---|---|
| 1. Establishing or amending a public register (as defined in the *Information Privacy Act*)? | ☐ | ☐ |
| 2. The collection of personal information, compulsorily or otherwise? | ☐ | ☐ |
| 3. A new use for personal information that is already held? | ☐ | ☐ |
| 4. A new or changed system of regular disclosure of personal information, whether to another part of State or local government, or to the private sector, or to the public at large? | ☐ | ☐ |
| 5. Restricting access by individuals to their own personal information, e.g. by affecting the *Freedom of Information Act*? | ☐ | ☐ |
| 6. New or changed confidentiality provisions or secrecy provisions relating to personal information? | ☐ | ☐ |
| 7. New or changed offences relating to the misuse of personal information? | ☐ | ☐ |
| 8. A new or amended requirement to store, secure or retain particular personal information? | ☐ | ☐ |
| 9. A new requirement to sight, collect or use existing ID, such as an individual's driver's licence? | ☐ | ☐ |
| 10. The creation of a new identification system, e.g. using a number, or a biometric? | ☐ | ☐ |
| 11. Linking or matching personal information across or within agencies? | ☐ | ☐ |
| 12. Exchanging or transferring personal information outside Victoria? | ☐ | ☐ |
| 13. Handling personal information for research or statistics, de-identified or otherwise? | ☐ | ☐ |
| 14. Powers of entry, search or seizure, or other reasons to touch another individual (e.g. taking a blood sample)? | ☐ | ☐ |
| 15. Surveillance, tracking or monitoring of individuals' movements, behaviour or communications? | ☐ | ☐ |
| 16. Moving or altering premises which include private spaces? | ☐ | ☐ |
| 17. Any other measures that may affect privacy? | ☐ | ☐ |

## RECOMMENDATION

That a Privacy Impact Assessment is / is not needed for this project.

Name of officer completing the Threshold Privacy Assessment:

Signature: Date:

## ENDORSEMENT BY THE PRIVACY OFFICER

I agree / disagree that a Privacy Impact Assessment is / is not needed for this project.

Further comments:

Name of Privacy Officer:

Signature: Date:

## NOTES

# Victoria's Information Privacy Principles (IPPs) Summary

## 1. Collection

Collect only personal information that is necessary for performance of functions. Advise individuals that they can gain access to their personal information.

## 2. Use and disclosure

Use and disclose personal information only for the primary purpose for which it was collected or a secondary purpose the person would reasonably expect. Uses for secondary purposes should have the consent of the person.

## 3. Data Quality

Make sure personal information is accurate, complete and up to date.

## 4. Data Security

Take reasonable steps to protect personal information from misuse, unauthorised access, modification or disclosure.

## 5. Openness

Document clearly expressed policies on management of personal information and provide the policies to anyone who asks.

## 6. Access and correction

Individuals have a right to seek access to their personal information and seek corrections. Access and correction will be handled mostly under the Victorian *Freedom of Information Act*.

## 7. Unique identifiers

A unique identifier is usually a number assigned to an individual in order to identify the person for the purposes of an organisation's operations. Tax File Numbers and Driver's Licence Numbers are examples. Unique identifiers can facilitate data matching. Data matching can diminish privacy. IPP 7 limits the adoption and sharing of unique identifiers.

## 8. Anonymity

Give individuals the option of not identifying themselves when entering transactions with organisations, if this would be lawful and feasible.

## 9. Transborder data flows

Basically, if your personal information travels, privacy protection should travel with it. Transfer of personal information outside Victoria is restricted. Personal information may be transferred only if the recipient protects privacy under standards similar to Victoria's IPPs.

## 10. Sensitive information

The law restricts collection of sensitive information like an individuals racial or ethnic origin, political views, religious beliefs, sexual preferences, membership of groups or criminal record.

The full text of the Information Privacy Principles forms schedule 1 of the *Information Privacy Act 2000 (Vic).*

To determine legal rights and responsibilities, use the full version, not this summary.

The Information Privacy Principles are simply…

the right information,
to the right people,
for the right reason,
in the right way,
at the right time.

Office of the
Victorian Privacy
Commissioner

GPO Box 5057
Melbourne Victoria 3001
Australia
DX 210643 Melbourne

Level 11
10-16 Queen Street
Melbourne Victoria 3000
Australia

Local Call 1300 666 444
Local Fax 1300 666 445

www.privacy.vic.gov.au
enquiries@privacy.vic.gov.au