PART 2: HOW TO DO A PRIVACY IMPACT ASSESSMENT (PIA)

Privacy Commissioner
Te Mana Matapono Matatapu

Part 2: Contents

ISBN No. 978-0-478-11743-1

A step-by-step guide to doing a PIA

What's included in this part of the toolkit

This second part of the toolkit sets out:

- questions to answer before you start any Privacy Impact Assessment
- key steps involved in any PIA and what each of those steps involves
- further steps to consider if your project is more complex or the risks are more significant.

We've also included other tools in the appendices:

- a PIA report template to record the information you gather and make decisions based on that information
- a risk management template to record any risks you identify and what you can do to mitigate them.

Deciding what steps you'll need to work through

The scale and complexity of your PIA will depend on the scale and complexity of your project. Only go as far as you need to for your particular project. For simple projects, the PIA process may be very quick and the PIA report may end up being only a couple of pages long. If your project is more complex, the resulting PIA report may be long, detailed and highly technical – but if that's the tool you need to do the job successfully, then it's likely to be worth the investment.

There are a number of steps that need to be a feature of every thorough PIA. Then there are some other steps that may also be useful, depending on the size and complexity of your project.

Steps that feature in every PIA

The basic steps in every PIA are:

1. Gather all the information you need to do the PIA and sketch out the information flows
2. Check against the privacy principles
3. Identify any real privacy risks and how to mitigate them
4. Produce a report (use our report template to help)
5. Take action
6. Review and adjust the PIA as necessary as the project develops.

See page 8 for more detail.

Other steps that may be useful

If your project is more complex, you may need to add various other steps into your planning. These can include:

- Get an external view of your PIA
- Consult with stakeholders
- Establish better governance structures to manage personal information
- Manage any risks with using third-party contractors
- Align the PIA with the organisation's existing project-management methodologies
- Publish your PIA.

See page 16 for more detail.

Questions to answer before you start

This section sets out some basic questions to answer before you start doing your PIA:

- At what point in my project will a PIA be most helpful?
- How long do I need, and how detailed should the PIA be?
- Who should do the PIA?
- Who do I need to talk to as part of the PIA?
- Do I need to involve the Privacy Commissioner? And if so:
  - At what stage?
  - What can they do to help?

At what point in my project will a PIA be most helpful?

A Privacy Impact Assessment isn't a last-minute legal compliance checklist – rather it's an active tool to help inform the major decisions involved in planning and implementing your project. Therefore doing a PIA early in a project's life is going to be most useful.

The PIA will help you get the system and operation design right, and avoid expensive and time-consuming pitfalls further down the road. Flushing out the potential issues at the conceptual stage of the project will show you what implementation details you're going to need to address. It will help you craft a more accurate project plan, as well as providing greater assurance that the project will be successful.

EXAMPLE

PIA as part of the design of a new IT system

If your project is a new IT system that collects, stores or processes personal information, it will be risky to put off doing a Privacy Impact Assessment until after you've already tendered for and designed the system. The PIA will help you design the system to manage that personal information well. You'll find it much harder and a lot more expensive to redesign or rebuild the system later to address any risks that the PIA exposes.

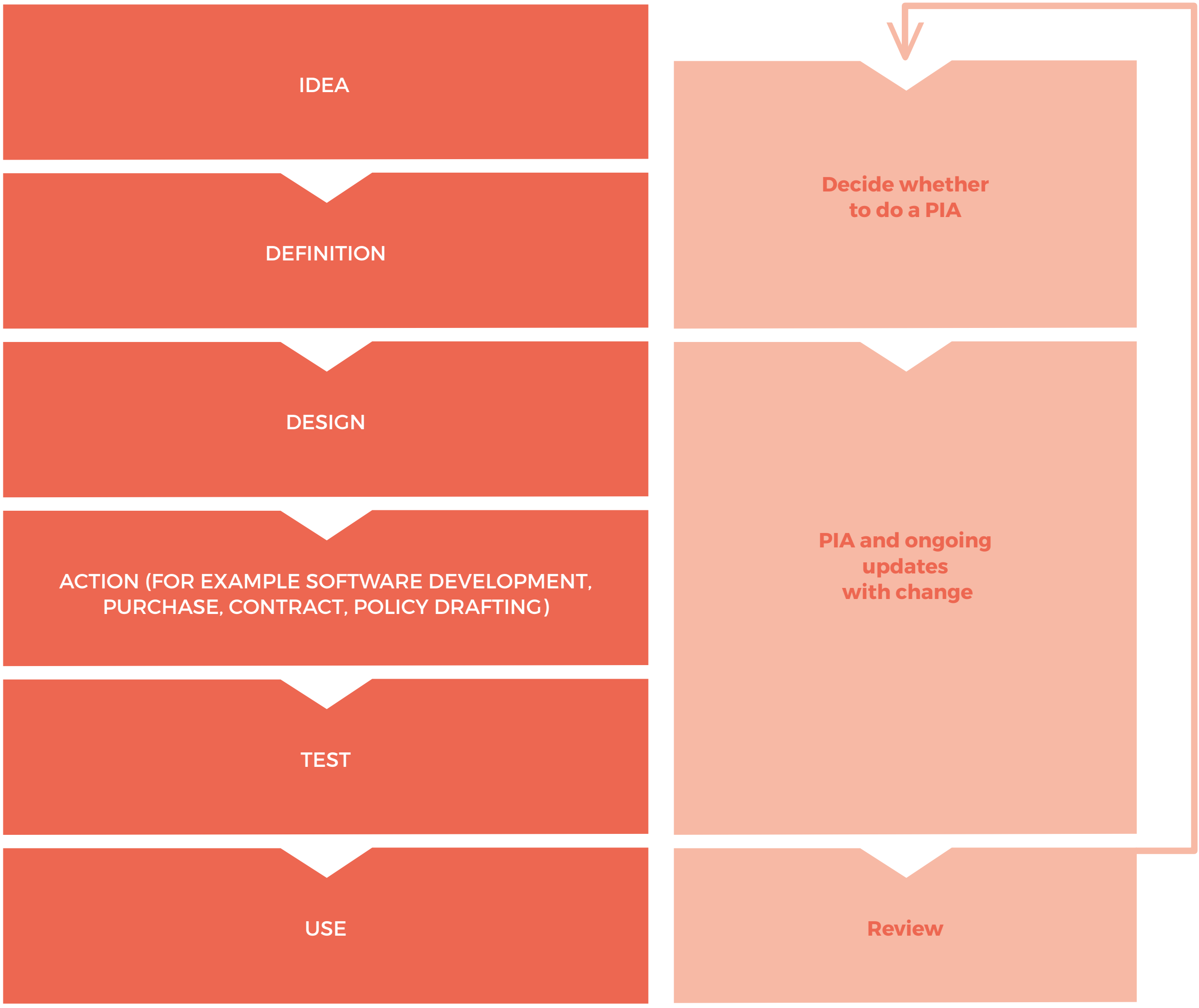
Building PIA checkpoints into your project plan

Inevitably, projects change during their lifetimes. You may not be able to answer every question in an early PIA – more information may come to light later. This is normal.

To manage this, build one or more **PIA checkpoints** into your project plan, where you'll ask whether anything significant has changed since you did the PIA. If it has, then slot that information into a new version of the PIA, and go back through the steps to check that there are no new privacy risks or, if there are, that the new risks are clearly identified and managed.

This diagram shows how a PIA fits into the life of a project.

Privacy Impact Assessment throughout an initiative


IDEA
DEFINITION
DESIGN
ACTION (FOR EXAMPLE SOFTWARE DEVELOPMENT, PURCHASE, CONTRACT, POLICY DRAFTING)
TEST
USE
Decide whether to do a PIA
PIA and ongoing updates with change
Review

How long will I need, and how detailed should the PIA be?

The information you gathered when you decided you needed a PIA should give you a good indication of the likely size and scope of the PIA process. Now it's time to ask further questions – this will check that you know exactly what the PIA will involve, what resources it's going to consume, and where it fits in the overall project plan.

Developing clear terms of reference for the PIA is a useful way to tease out the scope of the PIA.

Here are some of the key questions you'll probably need to answer about the size and scope of the PIA:

SIZE AND SCOPE OF THE PIA

Key questions to answer

- What will the PIA cover?
- What areas are outside scope?
- Is this just a "desk-top" information gathering exercise, or do I have to get information from a wide variety of sources?
- Who needs to be involved and when will they be available?
- Where does the PIA need to fit in the overall project plan and timelines?
- Who will make decisions about the issues identified by the PIA? What information do they need and how long will it take to get sign-off from them?
- Do I need to consult with anyone (for instance the individuals whose personal information the project will involve)? When and how should this happen?
- Are there any third parties involved and how long do I need to allow for them to play their part?

Who should do the PIA?

You don't need to be a privacy specialist to put together a straightforward PIA. It doesn't have to be done by your organisation's privacy officer, or a lawyer. However, it's useful if the project team includes someone who is reasonably familiar with privacy – someone who is able to advise you about the privacy principles and the potential privacy impacts of the project.

If the PIA will be particularly complex, or particularly central to the success of the project, it's worth thinking about hiring an external expert. Even where an external specialist is brought in, though, it's good practice to involve internal staff as well – this builds knowledge inside the organisation, and will make it easier to do future PIAs without outside help.

> **"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." (Privacy Victoria)**

Whoever you use to do the PIA, it's important that they have access to all the people who can give them the information that's needed.

Who do I need to talk to as part of the PIA?

Most of the people with the information you need for the PIA are going to be involved in the project. However, there may be some external stakeholders you also need to talk to.

Make sure you're aware of who has the information you need, and when they're going to be available.

If you're a small organisation, there will only be a few people in the organisation you'll need to look to – the information might even all sit on one person's desk. In these cases, think about whether there are people outside your organisation who you can get some advice from – for example, business colleagues, the local Chamber of Commerce or the Privacy Commissioner.

PEOPLE WHO MIGHT NEED TO BE INVOLVED OR WHO CAN PROVIDE ADVICE:

- People who are familiar with privacy, particularly the organisation's privacy officer
- People who deal with security in your organisation – they're likely to be familiar with what you're trying to achieve
- Business analysts and other project staff who will understand the business aims, what's being put in place, and when various steps need to be taken
- IT advisers who'll be able to provide information on the systems being used, how the personal information will flow through the system (including how it will be stored and processed), and whether there are any security implications
- Marketing and communications advisers who will help in understanding how the organisation uses information and can help coordinate any consultation needed for the PIA
- Risk and assurance people who can help you identify risks, controls and other actions
- Specialist staff groups who are affected by any proposals for handling personal information, such as call centre staff, information management staff, or human resources – they can give you the best information about how things will work on the ground
- Customer or consumer groups.

Do I need to involve the Privacy Commissioner?

Are you required to talk to us?

If your project involves draft legislation that affects personal information, or an authorised information-sharing or information-matching programme, or if a statute says the Privacy Commissioner has to be involved, then the lead Government agency is required to consult us.[1]

Otherwise, it's not compulsory to come and talk to us. However, many organisations find it useful to use us as a sounding board for projects that are larger, or that could result in serious harm to individuals if not done properly, or that use technology to collect or use of large quantities of personal information.

We won't do the PIA for you, but we can give you some basic advice and point out possible misconceptions or danger areas.

At what stage should you talk to us?

It's best if you start your PIA early on the life of your project, and then consult with us as soon as you've completed a reasonably full draft PIA report, but while the project is still at the concept stage.

In this way we may be able to give you a heads-up early on about some potential areas that tend to raise concerns with the public, or that lead to complaints, or that we, as the regulator, may have a problem with later on.

Having a reasonably full draft PIA report to look at will give us a clearer view about what your project will do and why, and what personal information is involved. We can then discuss whether the project looks like it will comply with the privacy principles, or whether there are other resources or examples that you might be able to refer to for help.

By doing your PIA early in your project, you'll be able to consider whether you should adjust your project based on the advice we provide. If we hear about your project only at the last minute, we can still give you advice – but your ability to act on it may be more limited, especially if there are already a lot of sunk costs in the system.

[1] The Cabinet Manual requires government agencies to consult with the Privacy Commissioner when putting forward policy proposals or draft legislation that affects personal information. Part 9A of the Privacy Act (approved information-sharing agreements) and Part 10 (authorised information-matching programmes) specify when and how the Privacy Commissioner has to be consulted.

Steps that feature in every PIA

IT'S ABOUT COVERING ALL THE BASES – NOT THE ORDER OF THE STEPS

As you work through the key PIA steps we discuss in this section, remember that it's the **content** of each step that matters – not the **order** you do them in.

A Privacy Impact Assessment often won't be a linear process. For instance, checking against the privacy principles may make you realise you need more information. Or you may realise you don't know how to take action because you haven't identified the risks sufficiently. Or sometimes once you start thinking about the PIA, a key problem may become evident – you may find that if you fix that straight away, the rest of the project will fall into focus.

So don't be concerned if you find yourself doing things in a slightly different order from how we've set out the steps below.

Step 1. Gather all the information you need

The information you put together when you were deciding whether to do the PIA will be a good start for doing the PIA itself. Now is the time to gather together all the details about what personal information the proposal involves and what is going to happen to it.

The key tasks here are:

- Describe the project – especially the purpose of changing what happens with personal information
- Describe the personal information involved and what will happen with it
- Describe the organisational context.

As you complete each of those tasks, add the information to a draft report. You can use our "Privacy impact assessment report" template (see Appendix A, at page 18) as the basis for the report (adjust it as necessary to fit your organisation and project).

You can use the report either as a briefing document for managers or other decision-makers, or – if the decision is your own – as a record of what you decided to do and why.

Describe the project – especially the purpose of changing what happens with personal information

A PIA is a tool to help you achieve the aims of your project or your organisation more generally while also protecting personal information. There is often more than one way of designing a project to accomplish what is intended – a PIA will help to identify the least intrusive way of achieving that aim.

A major key to success is having a clear understanding of what the change is aiming to achieve, and how it will support your organisation's work.

KEY POINTS TO COVER

- **Describe the project briefly**
- **Describe the purpose of changing what happens with personal information – what is the business aim in making the change?**
- **Is the project a one-off activity, or does it involve a change to your ongoing information-management systems?**

Describe the personal information involved and what will happen with it

The focus of any PIA is the personal information involved in the project and the positive or negative effects that the project may have on the privacy of the individuals affected by it.

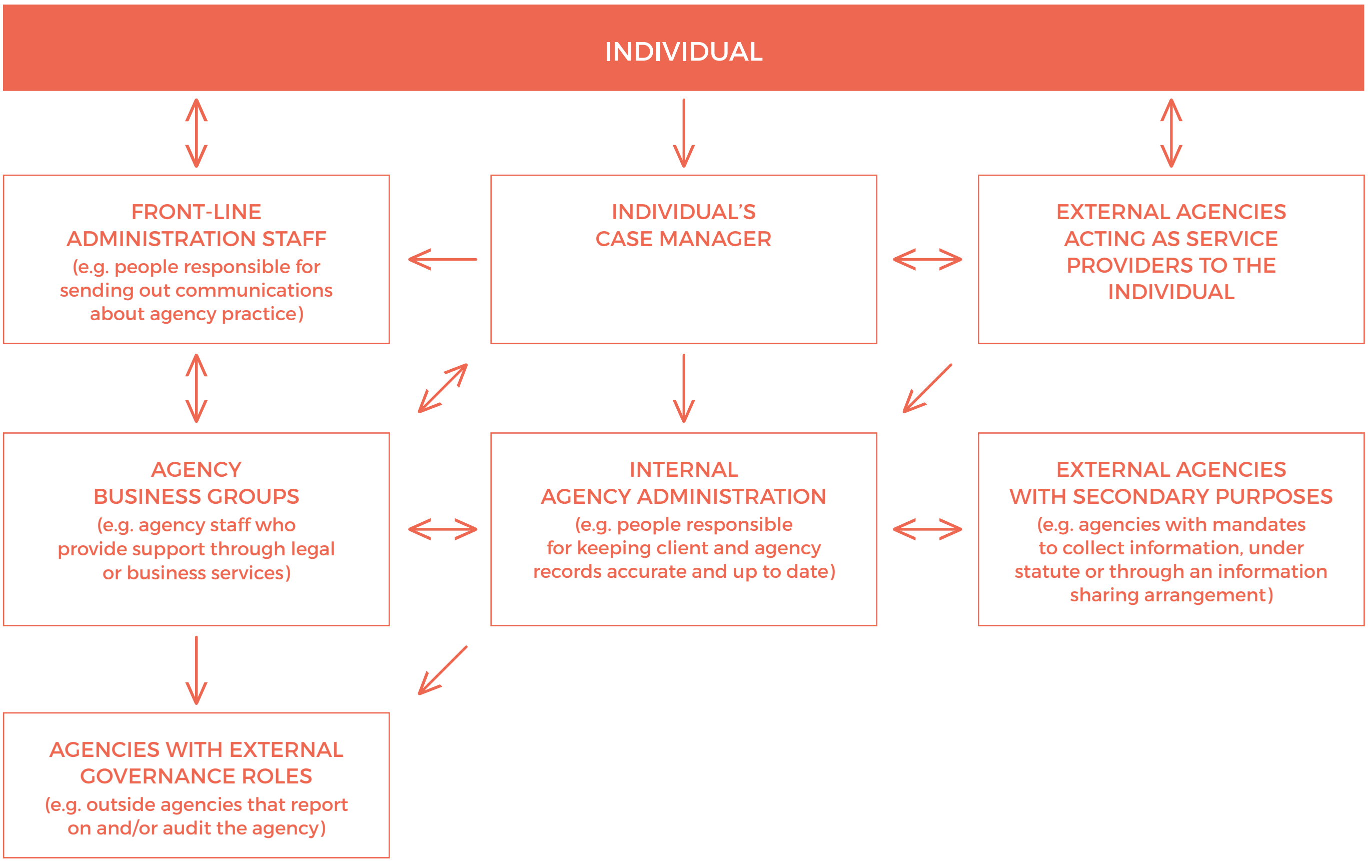
It's important to think about the whole lifecycle of the personal information. For instance, the PIA will need to consider how that information is going to be stored, who's going to use it and why, how it's going to be kept up to date, how long it will be kept for, and what will happen if the individual whose information it is asks to see it. Without considering the whole lifecycle of the information, you won't be able to spot where the problems or the opportunities occur.

You'll also need to consider a broader range of information-management questions if, for example, your project involves sharing information with another organisation so that the individuals can receive a service more efficiently. You'll need to consider whether the sharing of information will take the individual by surprise – perhaps because it's different from what they were told when you collected the information from them? If so, will you need to tell them what's going on? Also, how will you make sure the information is kept secure when it's being sent to the other agency, and that it won't be accessible to people who could misuse it?

DESCRIBE THE FLOW OF PERSONAL INFORMATION THROUGH ITS LIFECYCLE IN YOUR ORGANISATION

Key questions to answer

- What personal information is currently collected and used? How does it flow through your organisation's systems?
- How will your project change the information flow?
- Describe all the changes to personal information involved in the project. For instance:
  - Is new personal information being collected? If so, where is it coming from?
  - If the project involves information your organisation already holds, will you be using the information for a different purpose? If so, why and how?
  - What measures are in place to ensure the information is accurate and up to date?
  - Will your organisation tell the individuals what's happening to their information? If so, how will it tell them?
  - Who will have access to the information inside your organisation? Who will have access to it outside the organisation?
  - How long will the information be kept for? How will it be disposed of?


INDIVIDUAL
FRONT-LINE ADMINISTRATION STAFF (e.g. people responsible for sending out communications about agency practice)
INDIVIDUAL'S CASE MANAGER
EXTERNAL AGENCIES ACTING AS SERVICE PROVIDERS TO THE INDIVIDUAL
AGENCY BUSINESS GROUPS (e.g. agency staff who provide support through legal or business services)
INTERNAL AGENCY ADMINISTRATION (e.g. people responsible for keeping client and agency records accurate and up to date)
EXTERNAL AGENCIES WITH SECONDARY PURPOSES (e.g. agencies with mandates to collect information, under statute or through an information sharing arrangement)
AGENCIES WITH EXTERNAL GOVERNANCE ROLES (e.g. outside agencies that report on and/or audit the agency)

Using information flow diagrams

There are many ways in which you can set out the lifecycle of the personal information. However, an information flow diagram – or a series of diagrams – can be a particularly clear and simple way of showing exactly where personal information is coming from, where it's going, how it's going to be used, and who it's going to be used by (see example above). This can help you identify measures that can improve information security and reduce privacy risks.

Describe the organisational context

It's important to consider privacy implications in the context of the project as a whole, and in light of how your organisation works – particularly its existing approach to handling personal information. For example, you'll need to know whether any risk mitigation or other change that you recommend for the project is likely to be workable in the context of the organisation as a whole.

Considering the organisational context will also help you be aware of the likely downstream effect of the project in your organisation and enable you to predict and address potential privacy risks. For example, if your project involves one division of your organisation collecting a new piece of personal information for a particular purpose, how long will it be before another division decides they could use it too? Anticipating this kind of potential "scope creep" is an important part of any PIA.

Types of background information to include

Bring together the necessary background information about your project and organisation. This might include:

- Governance, management and roles and responsibilities describing privacy in your organisation (your privacy officer or legal team should be able to help you with this)
- Policies, standards and procedures relating to personal information (such as privacy statements, and retention or security policies)
- How privacy fits in with risk management in your organisation (for example, does your risk management framework consider risks to the people whose information you hold, rather than just risks to the organisation?)
- Overall processes and controls that affect privacy, such as disposal processes
- Security controls, such as how access to your information systems is managed
- Training and awareness programmes on privacy and security
- Monitoring and auditing of any incidents that occur, and how these are dealt with.

Step 2. Check against the privacy principles

As well as providing the legal framework that your organisation will need to comply with, the principles in the Privacy Act also provide a useful practical checklist for handling personal information properly throughout its entire lifecycle. This includes:

- collecting the information
- storing it and keeping it secure
- checking the accuracy of the information
- letting people have access to it so they can see what you know about them
- using or disclosing the information
- destroying the information.

A summary of the privacy principles is included in the template for a Privacy Impact Assessment Report at Appendix A (see page 18), and more information about common risks relevant to each of the principles is included in Appendix C (page 18). The full text of the principles is section 6 of the Privacy Act. More detailed advice about what the privacy principles entail is available on our website.

CONSIDER THE PERSONAL INFORMATION INVOLVED IN THE PROJECT AND HOW THE PRIVACY PRINCIPLES APPLY.

Key points to cover

For each privacy principle:

- Is it relevant? (if not, simply note that it is not relevant and why)
- Identify the personal information that is relevant to that principle
- Is the change consistent with the privacy principle? If so, how? Or will it enhance compliance?
- Does the change create more risks of harm to the individual? If so, how might it adversely affect the individual? Or does the change eliminate risks in the existing system?

EXAMPLE

A new mobile app

A business develops a mobile app that will collect various items of information about users, including information about their location. Questions the company will need to ask about that location information include:

- Why is it necessary to collect information about location? Is it a “need to know” or just a “nice to have”?
- What exactly will the business use the location information for?
- Will anyone else have access to the information?
- Will it be shared with third-party providers to run ads in the app, for instance?
- How will users know the information is being collected and why?
- What will happen if users don’t agree to provide the information? Do they have to consent in order to download the app? If so, is this reasonable? Can the user opt out (even if at the cost of some of the functionality)?
- Can the user change their mind and opt out of sharing location later? What will happen to the information the agency has collected if they do so?
- Is the user specifically and clearly asked for permission? How clear is the privacy statement?
- How long is user location information kept for? Is it aggregated, or linked to the user by information obtained from elsewhere or from the user?
- How is the information going to be protected against misuse and loss?

It’s important that the PIA take a critical and independent approach to these types of questions, as they will drive the design choices the business makes. It’s easy to get enthusiastic about the business opportunities resulting from collecting and using personal information, but consideration of how the individual concerned could be affected leads to better design in the long run – and a greater chance that the product will succeed and not be scuppered by concerns over privacy.[2]

[2] If your organisation is developing an app, you should look at our guidance for app development. It covers many of the privacy issues specific to the mobile environment: see www.privacy.org.nz/news-and-publications/guidance-resources/apps-guidance/

Step 3. Identify any real privacy risks and how to mitigate them

Ideally, a PIA will identify both risks for the individual, and opportunities to benefit the organisation by protecting privacy better. While this section focuses on identifying and mitigating risks, you could use a similar analysis to identify and maximise opportunities.

What is a privacy risk?

A "privacy risk" is the risk that a proposal will fail to meet individuals' reasonable expectations of privacy – for instance because it breaches the Privacy Act, or unreasonably intrudes into their personal space and personal affairs, or runs contrary to what your relationship with your clients suggests should happen.

Calculating risk is not simply about assessing whether the project will be legally compliant. It's possible to comply with the law and for the behaviour still to affect whether your particular clients' reasonable privacy expectations are met. The nature of your relationship with them may suggest that you should give even better protection than the law requires. The privacy principles provide a good framework for asking yourself the right questions – both legal and non-legal – about the impact on your clients.

Risks to an individual will often directly equate to risks for your organisation. Privacy breaches will have a direct impact on the organisation's reputation, and loss of trust can make it harder and more expensive to meet the aims of the project.

Consider not only the direct risks from the proposal, but also any knock-on effects. If you take too narrow a lens, you may miss an important, wider effect on the individuals you deal with.

How far do I have to go?

A PIA doesn't set out to identify and eliminate every possible risk to an individual from using their personal information or otherwise impacting on their privacy. However, it should:

- identify any genuine risks to the individual (that is, risks that aren't unrealistically remote or trivial)
- assess how serious those risks are.

Next:

- identify how to mitigate serious or medium-level risks
- determine your organisation's attitude to risk in the context of this project. Sometimes an agency may have a very low tolerance to risk – for instance where its relationships with its customers or clients are so important that it can't afford even relatively minor risks to eventuate.
- identify any serious or medium-level risks that the organisation decides it is not going to mitigate.

How to identify the risks

If your organisation is large, there may also be a specialist team (perhaps Risk and Assurance, Internal Audit, or Corporate Compliance) that can help you with how the organisation generally approaches the issue of identifying and managing risk. There may well be a specific format that it is best for you to use.

For organisations without specialist risk frameworks, we have provided a template for a risk and mitigation table at Appendix B (see page 18).

Populate your risk table with the risks you already know about from step 2 (see page 11), and identify the likely impact on the individuals. You can then use that as a basis for a more thorough analysis. Make sure you talk to other people involved in the project, or get a view from an external person who may be able to see risks that you have missed. Other possible steps, depending on your project, could be:

- a workshop including the key people involved
- a further desk-top review of documentation
- interviews with key people involved.

Common examples of mitigations include:

- minimising the amount of personal information collected
- better and clearer communication with the individuals
- allowing individuals to opt in instead or making it easy to opt out
- designing the system to provide better security
- providing training and support for staff to help them get it right.

Try to ensure that your mitigation solution is practical and sustainable. Reviewing the project once it is operating will help to identify whether the mitigations are actually working as you've planned.

> **"Consider what will actually work. There is little point developing a system that your staff cannot operate."** (survey respondent)

The following page has an example of how a few lines on this risk table might look, using the earlier example of a mobile app:

REFERENCE NUMBER	R-001	R-002
ASPECTS OF INFORMATION ASSESSED	What information the app collects	Third party providing advertising through the app needs access to information (age, gender)
DESCRIPTION OF THE RISK	The app will collect more information than specified in the privacy statement	Third parties may misuse this information for their own purposes (spamming, hacking, etc)
RATIONALE AND CONSEQUENCES FOR THE AGENCY OR INDIVIDUAL	The app will have greater functionality and lead to increased monetisation, but app users may object to collection beyond the current privacy statement	Data is never truly de-identified so may be misused exposing individuals to unexpected impacts. Individuals distrust unexpected disclosures to third parties Third party access to user information is a source of revenue.
EXISTING CONTROLS THAT CONTRIBUTE TO MANAGE RISKS IDENTIFIED	The business has a clear purpose for collecting the personal information (but app policy does not currently reflect it)	De-identify data as much as possible. Contract with third party also specifies what can and can't be done with information
ASSESSMENT OF RESIDUAL CURRENT RISK	Medium/possible Moderate harm	Medium/possible Moderate harm
RECOMMENDED ADDITIONAL ACTIONS TO REDUCE OR MITIGATE RISK	Put a process in place to manage clear notification and consent for additional collection by the app in line with the new purpose	Extend contract with third party to disallow re-identification or reuse of data for different purposes
RESIDUAL RISK REMAINING DESPITE NEW SAFEGUARDS	Low/unlikely Minimal harm	Low/unlikely Minimal harm

REFERENCE NUMBER	R-003	R-004
ASPECTS OF INFORMATION ASSESSED	To function the app requires a persistent account, tied to an individual	Username and password are collected by the app
DESCRIPTION OF THE RISK	Behavioural information is collected over time, in addition to personal information collected at download/ registration	Some users use one password across multiple accounts, which could reduce the security of the system elsewhere
RATIONALE AND CONSEQUENCES FOR THE AGENCY OR INDIVIDUAL	There is an administrative need, as the app won't work without a persistent account. But app users might object to more behavioural information being collected, and might abandon it for this reason	Hard to prevent people from recycling passwords. If an external account is compromised, all other accounts using the same username and password are vulnerable, including the app
EXISTING CONTROLS THAT CONTRIBUTE TO MANAGE RISKS IDENTIFIED	Privacy notice clearly outlines what information can be used for (e.g. account persistence, and customer service – which covers targeted advertising)	Credential information is encrypted; process to change/reset passwords is secure; hashed passwords are salted, but this won't prevent use of recycled passwords
ASSESSMENT OF RESIDUAL CURRENT RISK	Low/unlikely Minimal harm People often do not read the privacy policy – system design should still protect them as much as possible	Medium/possible Moderate harm
RECOMMENDED ADDITIONAL ACTIONS TO REDUCE OR MITIGATE RISK	Amend retention policy to ensure that app user logs are deleted when they are no longer needed (easy additional protection)	Require users to create a unique password for the app, changed regularly, using criteria unlikely to have been demanded by other accounts
RESIDUAL RISK REMAINING DESPITE NEW SAFEGUARDS	Low/unlikely Minimal harm	Low/unlikely Minimal harm

Step 4. Produce a PIA report

The PIA report is a major reference point for you and for your organisation. It should at least:

- include all relevant information about the project and what it is intended to achieve
- describe how information flows through the system
- include analysis against the privacy principles and other relevant material to show what the privacy impacts are (both positive and negative)
- identify key risks and how to mitigate any negative impacts
- recommend any necessary changes
- identify whether the PIA should be reviewed during the project, and/or once the new system is operating.

See the report template at Appendix A (page 18).

Step 5. Take action

There's little point investing even modest amounts of time or resources in a PIA and then failing to take action. An action list can help you track and manage the decisions you take as a result of the PIA.

The action list may contain items to be completed as part of the project itself, or it can be integrated into normal operations (such as maintaining a risk register, or as part of a security action plan).

Make sure that the action list clearly identifies who's responsible for doing what. Also make sure that it notes any relevant timelines and contingencies (for example, Action A needs to be completed by date B so that Stage C of the project can start).

In large or complex projects, there might be several versions of a PIA. It's important that any actions or recommendations from each update of the PIA are considered throughout the project. This may require designating someone in the project to take ownership of the action plan and report on progress, either within the project or within the organisation's existing governance framework.

The PIA may identify wider opportunities for action, so you can make privacy-enhancing changes throughout your organisation. For instance, it may show that there are other parts of your business where you might also achieve better security, better accuracy of information, and more effective business processes for managing personal information. If you spot an opportunity, take it – it's likely to make your business better.

Step 6. Review the PIA and use it as a checkpoint once things are in operation

Projects are rarely static. Even small projects can morph as they progress. The PIA that was produced early on is unlikely to reflect the current state of a project.

Use your Step 4 report and your Step 5 action plan as a baseline for considering the project as it progresses. If there have been changes that have an impact on privacy, do quick updates of the report and action plan that record:

- what's changed
- what the new impact is
- how to address any new risk (or take advantage of any new opportunity).

This will ensure your PIA continues to be used as a tool to check that the project does what it is meant to do.

Once the changes are up and running, it is also worth using the PIA as a checkpoint for how the new process is operating. Is it working as anticipated, or are problems starting to emerge and further changes needed? Again, using the PIA as a reference point can save you time and trouble.

Other steps that may be useful

Get an external view of your PIA

If your project is a substantial one, or the potential impacts on privacy are particularly significant, it will be worthwhile getting someone outside your organisation to check your PIA. They may identify something you've missed. They may have a better idea of how people who are not close to the project may react to what your organisation is doing – particularly the individuals who will be affected by the project.

Examples of people who can give you an external view might be:

- colleagues within your industry
- an industry association, Chamber of Commerce or representative group
- the Privacy Commissioner's Office
- a lawyer or a specialist in privacy law or information management
- IT specialists, systems architects, security consultant and so on.

Consult with stakeholders

Some projects will benefit from very wide consultation with stakeholders, both inside the organisation and externally. In particular, some projects will benefit from consultation with the individuals whose information you are using, or who will be affected by your project.

As part of your initial analysis, or your information-gathering exercise, consider who will have the best information to contribute or who might best flush out the risks posed by the project. If the answer is that your customers, or your staff, or external stakeholders might give you valuable information that you can't get elsewhere, then think about consulting with them.

Identify:

- who can give you the information
- when consultation is needed and how long it will take (so that you have the information in time to use it)
- how far you need to go for it to be useful
- what you will ask them
- what method you will use to get information from them (for example, a targeted survey, an email request to an external agency, or an online opportunity to respond).

Establish better governance structures for managing personal information

Protecting privacy is an ongoing responsibility, not something that your organisation should only consider as part of a change process.

Writing a PIA might be the first time your organisation has had to think about privacy issues. If so, use it as an opportunity to get people thinking about how to manage privacy better across the organisation.

In particular, make sure someone in the organisation is tagged with responsibility for managing privacy. Ensure privacy is one issue that's considered at the top table – solid leadership will make it far more likely that the organisation will get privacy right.

Manage any risks with using third-party contractors

If your project involves passing personal information to third-party contractors, this is a good opportunity to consider how to manage wider privacy issues relating to third parties who may have different standards from your organisation.

Questions to ask include:

- What privacy standards will you be holding the contractors to?
- Are they capable of meeting your expectations?
- How will you know whether they are competent?
- How will you know if something goes wrong?

You may be able to rework your standard contracts, or other documentation, so that it makes it easier and quicker to think about these issues when you engage a third party contractor to do work for you in future.

Align the PIA with the organisation’s existing project-management methodologies

Large organisations tend to have in-house project-management tools. It’s important for the PIA to fit with the way your organisation usually does things so that it has the best possible chance of being integrated into your business systems and of being effective.

For instance, for very large projects, or projects using “Agile”, or Agile-like methodologies, approaching PIA as a series of linked assessments may help the PIA and the principal project align better.

Publish your PIA

One of the benefits of doing a PIA is that it can increase the trust people have in your organisation and their willingness to work with you. If they’re aware of what you have done to manage privacy, they may have more confidence in you. Publishing the PIA demonstrates that you take privacy issues seriously and that you do your best to manage them. If you’re a small firm, for instance, publishing your PIAs may demonstrate that you’re a cut above your competitors.

Public-sector agencies in particular should seriously consider publishing their PIAs to demonstrate accountability, and as a proactive release of official information.

Of course, a PIA report may need to be reworked to protect interests such as commercial confidentiality, client privacy, security of information or legal privilege. Publication is not an “all or nothing” exercise – it is better to take out certain elements of the report and publish the rest, rather than not publishing at all.

Part 2: Appendices

Appendix C: Examples – Privacy risks and mitigations

This appendix:

- gives some examples of common mitigations you could consider to address identified privacy risks
- poses some questions to help assess and understand potential privacy impacts.

Using the privacy principles to follow the information lifecycle

Each privacy principle deals with a different aspect of information management. Addressing each principle in turn will therefore help your organisation make sure it takes proper care of the information entrusted to it.

However, the principles are best viewed as an integrated whole rather than a set of separate rules.

Each principle links with the others. For example:

- disclosure by one agency often involves collection by another agency
- unnecessary collection increases risks of unwarranted use or access
- poor security or unjustified retention of information creates risks of having inaccurate or outdated records.

On the other hand, use of privacy enhancing technology or techniques in one area can free you up in other areas. For example, if you anonymise information, it will be harder to link information to individuals. You are therefore less likely to need to restrict access so tightly.

Types of mitigations and safeguards

Strategies to enhance privacy, or to reduce or mitigate privacy risks, can include:

- technical controls – such as access control mechanisms, encryption, and design changes
- operational controls – such as organisational policies or procedures, staff training, and oversight and accountability measures
- communication strategies – such as privacy notices, and consent-based collection processes.

Examples of risk and mitigation

The following pages provide some examples of strategies you may want to use to address and mitigate common privacy risks. It is arranged by privacy principle.

PRINCIPLE 1 – COLLECTION OF INFORMATION

Personal information shall not be collected by any agency unless:

a) the information is collected for a lawful purpose connected with a function or activity of the agency; and

b) the collection of the information is necessary for that purpose.

What Principle 1 means in practice

Be focused – only collect personal information if you need to

The most effective privacy safeguard is not to collect information in the first place if you don't need it.

Good overall information management often stems from being clear about your purpose at the start. For instance, if your organisation isn't clear about why it needs the information, it's not going to know who needs to see it, or whether it's being used properly, or how to explain to the individuals concerned what it's doing with the information.

It's not enough simply to say that you might need the information sometime, or that it's easy to collect.

Key questions to ask (Collection)

- What personal information is your organisation currently using? Will your proposal change what's collected?
- Why are you currently collecting the information? Will your proposal change that purpose?
- What business process is enabled by having the information? Why is the information needed for that process?
- If you're collecting new information, why do you need it?
- Are there specific laws or regulations allowing you to collect the information?
- Are there specific laws or regulations prohibiting you from collecting the information? (If so, the Privacy Act won't help you because the other laws will override the Privacy Act. Change your proposal to fit with what the law allows. Or, if you're an agency that can influence legislation, consider what options you have to initiate a law change).
- Is all of the information a genuine "need to have" – or is it just a "nice to have"? What information can you do without?
- Will anonymous information do? If you don't need to collect someone's identity to deal with them, then don't – it makes the privacy risks a lot lower.
- Are you collecting information as a proxy for a different or less specific piece of information? For example, if you're proposing to collect people's dates of birth, do you in fact only need their age or age band?

Common risk examples (Collection)

- Personal information is collected without a clear purpose or without clear legal authority
- Information collected is either unnecessary or excessive
- Decisions affecting the individual concerned may be made using irrelevant information
- The purpose of collecting the information may be unclear, leading to possible misuse
- The individual concerned may feel a loss of control over what information is collected.

Possible mitigations to better protect privacy (Collection)

Establish the need for collection

- Clearly state your purpose for collecting the personal information
- Limit the information you collect to what is truly necessary for that purpose
- Consider whether you can use information that doesn't identify the individual

Limit unnecessary collection

- If you only need to verify identity, use accredited identity verification systems (such as RealMe)
- If you want to keep track of the numbers of visitors to a website, keep a count of visits, but don't keep IP addresses
- Use pseudonyms to distinguish people, instead of personal information that identifies them
- Constrain your IT systems so that unnecessary information can't be stored in databases
- Ensure that application forms ask only for the necessary information, and only have room for that information
- When using or installing security cameras or CCTV, use masking or pixilation technologies
- Only record images where there is a potential security risk, and delete records promptly
- Clearly identify where optional information can be provided, and explain the implications of not providing that information (this links with principle 3)
- Provide opt-ins for additional services (and easy opt-outs for services that people no longer require).

PRINCIPLE 2 – SOURCE OF INFORMATION

Where an agency collects personal information, the agency shall collect the information directly from the individual concerned, unless one of the listed exceptions applies.

What Principle 2 means in practice

Be direct – get it from the people concerned, wherever possible

When you collect information about someone, you should get it from them directly wherever possible, and you should tell them why you need it and what it will be used for. Then what you do after that won't be a surprise to them. Also, it's often the people themselves who are best placed to provide accurate information.

You can collect information from another source if you believe that one of the exceptions to the principle applies. These include:

- if the individual concerned has authorised you to collect the information from someone else
- if the information is already publicly available
- if getting it from another source wouldn't prejudice the individual's interests
- if the information won't be used in a way that identifies the individual concerned (including where it will only be used for statistical or research purposes and the individual won't be identified)
- if collecting it from another source is necessary to enforce the law, or for court proceedings, or to protect public revenue, or
- if collecting it from the individual concerned isn't reasonably practicable in the circumstances.

Key questions to ask (Source)

Defining the source of information

- Who will you collect the information from – directly from the person concerned or indirectly from a third party? If a third party, then who?
- If you're collecting it from a third party, why won't it work to get it directly from the individual?
- Will this differ from the way you already collect information? If so, how?
- Do you need to positively identify the individual concerned, to check it's the individual who's entitled to deal with you?

Common risk examples (Source)

- Individuals may not be aware that information is being collected, who will use it or what it's being used for. If they become aware only later, they may be surprised and upset
- Collecting the information from a third party could perpetuate and compound any errors that are already in the data
- Information may be out of date or irrelevant for the intended purposes if it's used outside the original context in which it was collected
- Individuals won't be able to update their information if they don't know you have it.

Possible mitigations to enhance privacy (Source)

- Change your system to collect information directly from the individual, unless you have a good reason not to do so. It's much better customer service to let the individual know what's going on
- If you're collecting information from a third party, make sure the individual that the information relates to knows you're going to do that, unless there's a good reason not to
- Have a clear privacy statement saying where you get personal information from
- Provide people with a way to see the information you hold about them (like a dashboard) and give them the opportunity to correct it if it's wrong
- Include a check box as a quick way for an individual to confirm their identity or to give authority for you to act on their behalf
- If you're getting only verbal consent, make sure you have a good system to record or document that consent.

PRINCIPLE 3 – COLLECTION OF INFORMATION FROM THE INDIVIDUAL

Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of:

a) the fact that the information is being collected; and

b) the purpose for which the information is being collected; and

c) the intended recipients of the information

d) the consequences (if any) for that individual if all or part of that information is not provided

e) the rights of access to, and correction of, personal information provided by these principles.

These steps shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.

What Principle 3 means in practice:

Be open – tell people why you need it and what you'll do with it

When you collect information from an individual, whether this is voluntary or compulsory, you should tell them what you need it for, and what you're going to do with it. If they don't have a choice about giving information to you, spell out what statutory provisions require them to do this, and any limits on how those provisions can apply.

As with principle 2, there are some exceptions that allow you to not spell out what you're doing – for instance because it:

- would frustrate the lawful purpose of collecting the information
- could prejudice a criminal investigation
- is not reasonably practicable in the circumstances.

Key questions to ask (Collection from the individual)

- Are your privacy statements easy to understand and access? (Bear in mind the device or format that people will be using to read it)
- Will you have to change your privacy statements as a result of the change that your project involves?
- Do individuals need to acknowledge that they understand what information is being collected?
- If any new or additional information is being collected, has the purpose been defined?
- If you're telling the individual they have to provide the information, do they genuinely have to provide it or are you just hoping they're happy to provide it?
- If you're not spelling out the matters listed in principle 3, will these matters be obvious to the individual? If they're not obvious, do you have a good reason for not telling people?

Common risk examples (Collection from the individual)

- Privacy statements may not be easily accessible – for example, on a mobile device with a small screen, or for individuals for whom English is a second language
- People often don't read privacy statements – if your organisation acts on the basis that the individual has knowingly consented, this could lead to clients losing trust in you
- The individual's consent for collection may not be supported by a valid, clearly explained purpose
- Individuals may be surprised by information being collected that wasn't required previously
- If they're not given advance notice, individuals may feel a loss of control over their information
- The individual may lose trust in dealing with your organisation, ultimately leading to a lack of engagement that may affect your ability to meet your objectives.

Possible mitigations to enhance privacy (Collection from the individual)

- Make sure your privacy notice is in plain language. Provide brief, key information first, and put explanations and details later (for instance, provide a link that people can click on for more information)
- Allow people to opt in if that's feasible. If it isn't possible, make sure people can clearly opt out
- Make it clear to the individual whether providing the information is compulsory or voluntary. If it's voluntary, explain why it would be beneficial to have the information
- Ensure your privacy notices are consistent and accessible in hard-copy and online
- Review your consent process to ensure that consent will be informed, current and specific, and given by someone with the capacity to provide consent (eg a parent)
- Provide a privacy notice after collecting the information if it's not practicable to do so in advance
- Publish privacy notices in formats and languages appropriate for the target group
- Design privacy notices for use with adaptive technology such as screen readers
- Update your application forms and enrolment forms to explain clearly why information is needed
- When collecting data electronically, use the technology to your advantage (for example, highlighting updates to privacy policies; using different levels of web pages for different layers of details)
- Require positive confirmation for actions by the organisation that could lead to adverse effects for the individual
- Change preference formats to yes/no options, rather than ambiguous check boxes
- Set privacy-protective options as the default wherever possible
- Use appropriate signage to ensure people are aware if CCTV surveillance is taking place
- Publish PIA reports so individuals know how their personal information will be managed.

PRINCIPLE 4 – MANNER OF COLLECTION OF INFORMATION

Personal information shall not be collected by an agency:

a) by unlawful means; or

b) by means that, in the circumstances of the case,

i) are unfair; or

ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.

What Principle 4 means in practice

Be considerate, be fair and don’t be unreasonably intrusive

Even where you’re required to collect information, you often will have choices about how you collect it. Design your system so you collect information by the least intrusive method available, bearing in mind the purpose you’re trying to fulfil.

Key questions to ask (Manner of collection)

- How are you collecting the personal information?
- Is the collection overt or covert? If it’s covert, why? (Covert collection is less likely to be fair – there needs to be a clear justification)
- Do you have to collect information that way, or do you have other options that would be as efficient or that might bring different benefits?
- Is the individual likely to be upset by the fact you’re collecting in this way?
- Are you legally required to collect information in this way?

Common risk examples (Manner of collection)

- Collection methods may be unjustifiably intrusive (for example, if biometric information is collected unnecessarily, or drug testing is conducted unjustifiably, or audio or video recording or location-tracking technology is used without adequate reason)
- Recording equipment is badly located or improperly adjusted, resulting in an over-collection of information, or an unjustified intrusion
- The physical and mental health and well-being of an individual could be damaged through breach of trust and a sense of loss of control over the use of their information
- Information is collected unfairly by using duress, coercion or deception
- Information is collected from individuals who believe mistakenly that they have to provide it because the statutory limits haven’t been clearly explained to them.

Possible mitigations to enhance privacy (Manner of collection)

- Use masking technology to avoid having CCTV overlooking neighbouring properties
- Think carefully about the different options available for collecting the information, and choose the least intrusive option that still achieves the purpose
- Check that every item of information on your form or your website log-in is necessary
- Test whether people will really see and understand your privacy notices
- If providing the information is optional, say so
- Make sure you’re not going to collect additional information by accident (such as audio material as well as video, where only the video is needed for the purpose)
- Don’t drug test employees if they’re not working in safety-sensitive positions

PRINCIPLE 5 – STORAGE AND SECURITY OF INFORMATION

An agency that holds personal information shall ensure:

a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against

i) loss; and

ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and

iii) other misuse; and

b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

What Principle 5 means in practice

Take care – keep it safe

You need to ensure that personal information is protected against misuse, loss or theft. Security is going to be relevant to you whether you're maintaining or upgrading an existing database of client information, moving information into a new application or other system, or developing a new business process or access model that changes how personal information is used or who has access to information.

There are some additional things to consider if you're using a third party to support IT systems or business processes and giving them access to the system that holds the information. You'll need to check that the third party has reasonable security safeguards in place.

Key questions to ask (Storage and security)

- What personal information will be stored by the organisation and how will that change?
- What format will the personal information be stored in (paper, or electronic), where will it be stored, and who will be responsible for its safe-keeping?
- What security and access controls will protect personal information against misuse, accidental loss, unauthorised use or disclosure – whether in transit or when the information is stored and used?
- Who can access the information now, and how will that change?
- Are you using a different contractor from before?
- When did you last look at your security controls? Do they need updating?
- Do contracts with third-party providers include appropriate privacy clauses and safeguards? Will you know if something goes wrong when the information is in the third party's hands? Who from their staff will be able to see the information, and are they trained to handle it well?
- What policies, standards and procedures relating to storage will need to be taken into account (such as requirements for disposal; obligations to disclose to other agencies)?

Common risk examples (Storage and security)

Electronic and technical security measures

- Failing to limit edit-access to data, or to limit or monitor access or enforce access controls, can lead to misuse or unauthorised disclosure
- Devices in shared work areas, or portable devices, can provide for inappropriate access
- Providing online log-in access to client records raises the risk of session cross-overs, or automated scams
- The system can't trace who has accessed a file – so you can't tell whether there are problems with unauthorised access
- Unwarranted access to personal information may lead to identity theft
- The organisation doesn't comply with basic standards and expectations for information security and records management.

Physical and operational security measures

- Staff are unaware of their obligations, leading to accidents, careless actions or mishandling of information, which in turn results in unauthorised disclosures
- Co-located offices, shared workstations, uncontrolled building access and offices open to the public can pose a risk of unauthorised access to personal information
- Failing to recognise the high-risk nature of information, including the need to implement a higher degree of security to protect particularly sensitive financial or health information
- Failing to include contracted service providers in an agency's data-management strategy, elevating the risk of external breaches of data security, in particular, where contracted service providers are located outside New Zealand giving rise to jurisdictional issues
- Allowing workplace use of portable storage devices (such as USB sticks, mobile phones, personal laptops) without proper security protections
- Using regular post to send highly sensitive personal information may raise the risks that it could be sent to the wrong address or go missing
- Testing and training environments may expose personal information to risk
- Hacking, system failures, data compromise or breaches result in unauthorised access.

Possible mitigations to enhance privacy (Storage and security)

Electronic and technical security measures

- Limit the use of portable storage devices through operational policies and technical controls
- Use registered post to send particularly sensitive information, rather than regular post
- Use window envelopes to avoid mis-matching labelled envelopes and their intended contents for bulk mail-outs, but ensure that no information, beyond the name and address, is visible through the window
- Ensure any remote access to your data, whether by staff or clients, is to encrypted data, or is unencrypted data that travels only via encrypted transmission
- Use technologies such as CAPTCHA to differentiate between human and computer users of your site
- Consider two-factor authentication rather than just username and password, and build-in a “time out” limit on access
- Provide for degrees of anonymity (such as by using pseudonyms, anonymisers or anonymous data credentials) to minimise the amount of data provided, allowing customers to reveal only so much personal information as is necessary in order to complete a transaction
- Provide a degree of “unlinkability” (for example, by using multiple virtual identities and communication anonymisers) to hide real online identities (email address, IP address, and so on)
- Replace identifying details with non-traceable, disposable identities not readily associated with other identities used by the individual (for example, pseudonyms, one-time emails)
- Mitigate against loss or theft of sensitive information by protecting it in storage, in transit and in use with strong authentication
- Encrypt confidential data when it is stored or relocated to data repositories or archival warehouses, providing for decryption keys based on data receivers’ credentials
- Keep processed data in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were originally collected
- Ensure access and handling protocols define who has the authority and ability to add, amend or delete data and to assign, change or revoke access privileges
- Provide in-house users with delay-send options and pop-up reminders to check attachments before sending to outside recipients, and disable auto-complete for external emails
- Embed technically feasible default privacy settings into the systems supporting the initiative
- Use cryptographic tokens or credentials issued by organisations to allow individuals to anonymously prove statements about themselves and their relationships with public and private organisations

Physical and operational security measures

- Ensure “sign-in” procedures don’t unnecessarily reveal information about previous visitors
- Develop plain language usage policies to supplement your other data security measures
- Ensure your projects include ongoing staff training that’s relevant to the jobs people do
- Ensure physical security prevents unwarranted access to areas where sensitive data is stored
- Ensure your records practices comply with recognised best-practice guidelines or standards
- Ensure that particularly sensitive personal information, such as biometric information and health or financial records, attract the highest levels of security
- Examine your data flows to identify any weak spots that need further security measures
- Ensure your data security strategy is appropriate to the type of data stored
- Ensure that service providers are contractually bound to comply with specific privacy safeguards
- Conduct a threat and risk assessment of your database and network security
- Engage someone to conduct an ethical hacking exercise to test system vulnerabilities
- Use only dummy data in testing and training environments
- Allocate a needs-based, unique identity to each authorised user
- Take appropriate measures to identify and punish employee browsing.

PRINCIPLE 6 – ACCESS TO INFORMATION

Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled:

a) to obtain from the agency confirmation of whether or not the agency holds such personal information; and

b) to have access to that information.

What Principle 6 means in practice

Keep people informed – tell them what information you hold

In most cases, people have a right to access the personal information you hold about them. That means you need a system that enables you to find information about people when they ask, and provide it to them. There are some exceptions, though, and it's important to know what they are.

Records-management systems must take into account the fact that individuals may wish to access the information an agency holds about them. Shoddy information-management practices are not an excuse. Most organisations don't have to hold on to information forever, but while you do have it you should be able to find it – wherever it is (onsite, in archives, offshore, in people's inboxes – or even in their heads).

The clock will be ticking too – you have to provide a decision about access as soon as reasonably practicable, and not more than 20 working days after the request comes in (unless you have a valid reason to extend this time limit). You also have to provide the information itself without undue delay.

Key questions to ask (Access)

- How is personal information currently being stored and how will this change?
- What metadata is kept to allow personal information to be readily identified and located?
- Will all of the information about an individual be in one place or clearly linked to ensure a complete record can be identified?
- If you get a request for the information, how would you respond and how long would it take you to make a decision about the request?
- Who is responsible for handling information requests? How will you make sure the request gets to them?
- If information is held in third-party storage (in the cloud for example) have you made sure you can get it back when you need it? Will it be in a format that you can use, and that you can easily supply to the requester?

Common risk examples (Access)

- Changes to database structures affect the location and retrieval of information
- Backup changes alter how information is retained and whether it can be readily identified and attributed
- Individuals aren't able to easily access their personal information
- Lack of access to personal information increases the risk of poor-quality, out-dated data
- Access may be hampered if the data is held by contracted third-party service providers – there could be time delays to factor in
- Information may be stored in a different format from the one that you can use now
- Failure to file information properly leads to inefficiencies (for example, having to search through email boxes rather than retrieving the information directly from the filing system).

Possible mitigations to enhance privacy (Access)

- Make it easy for people to access their information by setting up a process for them that suits the way your organisation works
- Make sure you keep accurate track of requests for personal information (whether they're verbal or written requests)
- Consider providing individuals with routine access to their personal information, or direct access – for example, through online accounts
- Ensure that stored information is readily identifiable and retrievable
- Ensure that contracts with external third-party service providers include provisions guaranteeing speedy retrieval of personal information when your organisation wants it
- Increase the control that users have over their personal data by allowing them to look up past transactions using their personal information, including what data has been transferred or disclosed to third parties, when, to whom, and under what conditions
- Inform users of their data access and correction rights, and who to contact if they want to request access
- Have a standard process for people to use to demonstrate that they have authorisation to get information on someone else's behalf.

PRINCIPLE 7 – CORRECTION OF INFORMATION

Where an agency holds personal information, the individual concerned shall be entitled:

a) to request correction of the information; and

b) to request that there be attached to the information a statement of the correction sought but not made.

What Principle 7 means in practice

Make it right – let them correct it if you have got it wrong

If you hold information about an individual that they think is wrong, they're entitled to ask you to correct it. If it really is wrong, it's in everyone's interests to get it right.

Sometimes, the person's opinion of what is right may differ from your own. In that case, you don't have to delete or correct the information. However, if the person wants you to, you have to add a statement of what the person thinks is correct to your file, in such a way that anyone reading it later will know what that person's view of the information is, as well as your own.

If you correct information, but you've already passed the original information on to another organisation, you should, if possible, notify the other organisation that the information has been changed.

Key questions to ask (Correction)

- How do you accommodate individuals who believe that the information you hold is inaccurate?
- Does your system or process allow information to be modified if it's wrong?
- How do you verify the accuracy of information before you change it?
- How do you monitor changes to ensure they're authorised?
- If information can't be changed or appended, what mechanism is in place to attach a statement of correction?
- Will your system track who you've sent information to, so that you can let them know if the information was inaccurate and had to be changed?

Common risk examples (Correction)

- Poorly managed correction requests can lead to poor-quality data
- Correction may be hampered if the data is held by contracted service providers
- Failing to correct personal information that has been disclosed in the past can lead to inaccurate information, affecting the individual and the organisation's services
- Computer systems aren't built to allow statements of correction to be added, or for a flag to signal that there is further information a decision-maker needs to consider
- Poor quality information is passed to other agencies, compounding the errors and the problems for the individual
- Information is duplicated in different parts of the organisation, but corrected only in one.

Possible mitigations to enhance privacy (Correction)

- Ensure there's a clearly defined process by which an individual can discuss or dispute the accuracy of the personal information you hold about them
- Ensure you have policies setting out how your organisation can action routine or simple correction requests (such as a client's formally notified change of address), and who can determine more complex requests (for example, when a client disputes your decision on their eligibility for services)
- Design your system to allow a statement of correction to appear beside the original information – or at the least for the system to display a clear flag showing that there is other relevant information to consider
- Ensure a record is kept of correction requests, and the decisions on those requests
- If you have to keep the original information (for example because of statutory or record-keeping obligations), design your system to do so
- Where services are contracted out, consider which organisation will have the most current and accurate data, and how any corrections will be communicated to the other organisation
- Specify whether correction requests are to be mediated by your organisation, or handled directly by the contracted service provider
- Let users know about their access and correction rights, and ensure they know who to contact if they have a request.

PRINCIPLE 8 – ACCURACY OF INFORMATION

An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

What Principle 8 means in practice

Keep on the mark – ensure it's correct and relevant before you use it

Poor-quality information leads to poor decision-making, which in turn may lead to unfair and inappropriate practices and unwarranted adverse effects on the individuals concerned.

Poor data may also make it harder for agencies to perform their functions efficiently and effectively and meet their objectives. Inaccurate or outdated information can be particularly problematic, both for agencies and the individuals concerned, if agencies can't get in touch with individuals when they need to in order to verify their details and circumstances.

Key questions to ask (Accuracy)

- What processes do you have in place to ensure the information you hold is attributed to the correct person (and not someone with a similar name or the same address)?
- What mechanisms are in place to ensure that information is accurate, complete and up to date before it's used or disclosed?
- What opportunities are provided to individuals to routinely correct or update their personal information, or to verify its accuracy before it's used or disclosed?
- Is this information that's likely to change over time (such as address, marital status, financial or health status) or information that is static (birth name, date or place of birth)?

Common risk examples (Accuracy)

- Poor-quality information may lead to decisions that impact negatively on individuals
- Incomplete or incorrect information can lead to incorrectly informed decisions
- Incomplete or inaccurate information may lead to financial or professional loss if used as a basis for decisions on whether an individual is eligible for a grant or benefit, or has obligations
- Information kept too long can be out of date
- Information in misplaced files or that is positioned wrongly in databases can cause information to be attributed wrongly, while at the same time being dis-associated from the person concerned
- Migrating paper records to a digital format by re-keying data risks introducing errors
- Inaccurate data can increase the risk of inappropriate use and unwarranted disclosure
- Updating personal information without creating and maintaining audit trails of the updates increases the risk of unauthorised changes going undetected
- Failing to update personal information that has been disclosed in the past or that is held by contracted service providers can lead to poor data quality and inconsistent actions.

Possible mitigations to enhance privacy (Accuracy)

- Regularly check the reliability of equipment used to collect, process or test information or samples to minimise errors and detect unauthorised changes
- Before you take adverse action against someone based on the information, give them the opportunity to question or refute its accuracy
- If information was collected some time ago, review your policies and practices to ensure it's still required for the purpose it was initially collected for and that your continued use of it is justified
- Take care when engaging in data matching or cleansing – the data may already be out of date
- Allow individuals to opt out easily for services they no longer require so you don't keep information on their current file longer than needed
- Where information disclosed to another party is found to be inaccurate, let them know
- Periodically assess the accuracy and currency of the information you hold.

PRINCIPLE 9 – DELETION OF INFORMATION

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

What Principle 9 means in practice

Don't be a hoarder – get rid of it if you don't need it anymore

Think about what you really need the information for. If you have no real reason to keep it, securely destroy it ("just in case" is not a good enough reason).

Obviously, you can't destroy documents that must be retained under other laws (for instance, to comply with the Public Records Act or Tax Administration Act). However, you need to make sure that any historical documents retained for those purposes are kept secure and can't be accessed by staff who don't need to see them. Consider whether, and when, the organisation should destroy any copies of documents that have been transferred elsewhere for permanent archiving. Also, consider de-identifying the information if it is to be retained for future business planning or research purposes.

Key questions to ask (Deletion)

- How long do you need to keep the information for?
- Do you have a system saying when it's time to dispose of it, and how to dispose of it?
- How long have you already held the information, and if it's new, how long will you hold it?
- Is the information covered by the Public Records archiving requirements? If so, what protocols are you suggesting should be applied to protect the information once it's archived?
- Are there legislative requirements that mean you need to keep the information (for example, to comply with tax obligations)?
- Are there business reasons for keeping the information indefinitely (for example, to provide proof of a qualification from an educational institute)?
- Do you need to keep information with identifiers attached, or can you reduce it to anonymised or aggregated data and still get the job done?

Common risk examples (Deletion)

- Keeping data longer than necessary increases the risk of a data security breach or unauthorised use or disclosure
- Keeping information too long increases the risk it will be out of date, misleading and inaccurate
- The careless or ineffective disposal of files may lead to unauthorised access or disclosure
- Destroying information when you still need it creates problems of its own – if you don't have a plan, you're likely to make mistakes.

Possible mitigations to enhance privacy (Deletion)

- Have clear retention policies and disposal schedules, and monitor their use to ensure they can be updated as the need to keep information changes with time
- Where you no longer need information for the purpose you collected it for, but you need to retain documents to comply with specific legislation (such as the Public Records Act or Tax Administration Act), add safeguards to remove it from view and prevent access except by properly authorised staff
- Destroy transactional data when the transaction is complete and keep only metadata
- Ensure personal information is disposed of promptly once the minimum retention period specified has expired, unless you have a legitimate purpose for retaining it for longer
- Design your database to include a facility to flag records for review or deletion when the minimum retention period expires
- Ensure hard disks are entirely wiped or encrypted before disposing of computers. Use a shredder or secure disposal bins for disposing of paper records
- Minimise the amount of information that needs to be disposed of by minimising the amount of information collected in the first place.

PRINCIPLE 10 – USE OF INFORMATION

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds, the specified exceptions apply.

What Principle 10 means in practice

Stick to the plan – only use it for the purpose you initially collected it for

Use information for the purpose you initially collected it for unless additional permissions and safeguards are in effect.

When information is going to be used for a different purpose that isn't directly related to the original one, you may sometimes need to notify the individuals in the same manner as if the information was new or additional information. There are exceptions – for instance, if the information is only being used for research or statistical purposes, and the individuals will not be identifiable in any material published at the end.

Other exceptions may also apply on a case-by-case basis: for instance where the individual concerned has authorised you to use the information for another purpose, where you took the information originally from a publicly available publication, or where it is necessary to enforce the law or for court proceedings, or to protect public revenue. You can also use information for a purpose other than your original one if you consider it's necessary to protect public health or safety or the life or health of the individual concerned or another individual.

Key questions to ask (Use)

- What personal information will be used and for what purposes?
- Is the purpose the information is to be used for directly related to the purpose for which it was collected initially? In other words, would the individual concerned expect that this was what you would do with it?
- Are there any controls or systems in place to restrict how information can be used?
- Are you using information for a new purpose. or is what you're doing within the scope of the original purpose?
- Will the intended use be communicated to the individuals concerned? If not, why not?
- Is the use of the personal information authorised, enabled or required by legislation?
- What training has been provided to staff on the use of information?
- Can you achieve what you need to do with anonymised information?

Common risk examples (Use)

- Information provided for one purpose may be used inappropriately
- Individuals may be surprised or upset by an unanticipated secondary use and any implied "consent" to a secondary use may not be valid
- Ill-defined purposes result in ad-hoc use in a manner unrelated to the original intended use
- Personal information collected on behalf of another agency is used without legal authority.

Possible mitigations to enhance privacy (Use)

- Clearly define the proposed information use and convey that to the individuals concerned
- Check that any proposed uses won't breach contractual or implied confidentiality undertakings
- Develop robust access control protocols that limit access to a "need to know" basis so that users can access only the information they need for their legitimate functions
- Ensure that access controls are updated constantly and quickly, to accommodate departing staff, changes in roles, and the expiry of contractors' terms
- Provide for regular auditing of access by both authorised and unauthorised users
- For voluntary secondary uses, consider seeking consent first. Ensure that the voluntary nature of any choices is clearly communicated by providing opt-in rather than opt-out mechanisms
- When relying on consent to a secondary use, ensure there is a workable mechanism by which a person who refuses consent, or provides conditional consent, can be recognised
- Ensure that secondary uses are provided for by statutory authority or contractual terms
- Ensure that you have included all routine uses in an appropriate privacy notice
- Make it easy for people to see what you're doing with their information – make it easily available to them and invite their comments.

PRINCIPLE 11 – DISCLOSURE OF INFORMATION

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds, the specified exceptions apply.

What Principle 11 means in practice

Keep the control – only share information if that's why you got it

You can disclose information for a particular purpose if that's one of the purposes you originally collected it for. However, if you're being asked to disclose for a different purpose, check that you have a good reason and legal authority to do so.

Nobody can use principle 11 to force you to disclose information. Only other statutes or court orders (such as warrants) can make you give information to anybody other than the individual whose information it is. However, principle 11 allows you to disclose information to other organisations if one of the exceptions applies.

The exceptions include:

- where you need to disclose information to an appropriate authority to protect someone (for instance a child who may be at risk)
- where the individual concerned has authorised you to disclose the information to someone else (or you're disclosing it to them)
- where the original source of the information is already publicly available
- where it is for statistical or research purposes and the individual concerned won't be identified
- where disclosing the information is necessary to enforce the law or for court proceedings, or to protect public revenue.

However, as with the use of information (principle 10), these exceptions should be applied on a case-by-case basis and shouldn't be used to justify bulk or regular information-sharing.

Key questions to ask (Disclosure)

- Are you creating or changing any information-sharing arrangements with other organisations?
- Is the purpose of disclosure directly related to the original purpose of collection?
- Will information be disclosed as individual records, or in bulk files or aggregated?
- Will personal information be disclosed routinely? For what purpose?
- Is that purpose required, enabled or authorised by any law?
- Whose information will be disclosed or exchanged, and how might that affect them?
- Will the subject be aware their personal information will be disclosed for this purpose?
- Would other disclosures also be contemplated from time to time?
- How will information be exchanged, and what security measures will ensure it's transferred safely?
- If information matching may be required, what databases would be involved?
- What information will be retained in the system once it's transferred?

Common risk examples (Disclosure)

- Incorrect or inaccurate information is shared with other agencies
- Non-compliance with statutory or contractual obligations or implied confidentiality undertakings results in breach of trust
- De-identification of personal information before disclosure doesn't prevent re-identification
- Information with negative connotations is shared with another party leading to embarrassment, stigma, or damage to a person's reputation
- Risk aversion means you don't share information that you should be sharing, for instance to protect someone's safety
- Concerns over personal safety arise if sensitive information about a person's activities or whereabouts could fall into the wrong hands
- Secondary disclosure is not necessary or legally justifiable
- Individuals don't have an opportunity to question the manner in which data received from another agency has been processed to arrive at an adverse decision
- People are unaware of, or have failed to opt out of a voluntary secondary disclosure
- Information is disclosed for a use not directly related to the primary purpose of collection
- Individuals may be surprised or upset by an unanticipated disclosure for secondary use.

Possible mitigations to enhance privacy (Disclosure)

- Ensure that appropriate privacy protections are transferred along with the information you're disclosing, through contractual arrangements or terms and conditions in sharing agreements or MoUs
- Ensure that secondary uses have appropriate statutory authority or contractual terms
- If you're transferring data to another agency, ensure that its records-management processes have levels of protection that are similar to or greater than what your own organisation requires
- Remove unnecessary identifying details before releasing the information to ensure that it can't be matched to other information that could establish an individual's identity
- Put clauses in contracts prohibiting use of anonymised information in a way that could re-identify someone
- Ensure that each participating organisation has a lawful authority to collect and/or disclose the information, and check that proposed disclosures won't breach secrecy provisions or other restrictions in governing legislation
- Be open with individuals (in advance, if possible) about information-sharing arrangements, and where possible, make secondary disclosures to third parties voluntary – that is, seek consent first
- For voluntary secondary disclosures, provide opt-in rather than opt-out mechanisms and ensure that the voluntary nature of any optional choices is clearly communicated
- Ensure you've included all foreseen routine disclosures in an appropriate privacy notice
- Use stakeholder consultation to test community expectations about proposed disclosures.

PRINCIPLE 12 – USE OF UNIQUE IDENTIFIERS

An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any 1 or more of its functions efficiently. Where a unique identifier is to be assigned it must comply with specific conditions.

What Principle 12 means in practice

Be unique – don't use other agencies' personal identifiers

A unique identifier (usually a number) is a record assigned by an organisation to uniquely identify an individual in their interactions with the organisation. You should only assign unique identifiers where this is expressly permitted and necessary for you to carry out your functions efficiently. You should not use unique identifiers that have been developed by another organisation, or for another purpose, unless there is an explicit authority to do this and it's necessary for the purpose of your project.

Limiting the use of unique identifiers reduces the risk that a universal identifier will be established that could be used to link a wide range of information about an individual without their knowledge or control. It also decreases the risk of identity fraud.

Key questions to ask (Unique identifiers)

- How will individuals be identified? Will a unique number or other identification device be used?
- Could the method of identifying individuals result in more than one person being assigned the same information (for example, through information on identities being inappropriately merged)?
- Are you using the same unique identifier as another organisation, such as a tax number, or student number? If so, where is your authority to do so?
- Will any identifying number create a unique record across the population that could be used to link other unrelated personal information to expand an individual's visible profile?

Common risk examples (Unique identifiers)

- Service provision is conditional on supply of a unique identifier assigned by another agency
- Unrelated information about an individual can be linked by association through the use of another agency's unique identifier
- Use of the same unique identifier by different agencies creates a de-facto universal unique identifier.

Possible mitigations to enhance privacy (Unique identifiers)

- Only collect a unique identifier provided by another organisation if you have specific legal authority to collect it and you need a record of the number to perform your functions
- Check that the unique identifier has been designed with your intended purposes in mind – is it fit for the purpose to which you're putting it?
- If you need to verify eligibility by using identifiers issued by another organisation, note that the identification has been sighted but do not assign the number to the individual for your own use
- Ensure that your records-management systems are not designed to use unique identifiers issued by another organisation as the primary means of identifying the individual (for example, as part of an a matching algorithm)
- Use agency-specific unique identifiers when working across different business units within an organisation to minimise the use of identifying personal information
- Minimise the amount of human-readable or attributable information by use of unique identifiers and other identification methods such as bar codes
- If using another agency's unique identifier to match data, use it as an attribute, not as your primary identifier for your organisation's processes.

Appendix D: Other resources

Information about the Privacy Act and the privacy principles

- Privacy Act and codes – Introduction
- Privacy Act and codes – Privacy principles
- Human Rights Review Tribunal of New Zealand (the Human Rights Review Tribunal privacy cases since 2002 are all available free online)

International resources

- Privacy Victoria **Privacy Impact Assessments Guide** (2009)
- Information Commissioner's Office **Conducting privacy impact assessments Code of Practice** (2014)
- Office of the Australian Information Commissioner **Guide to undertaking privacy impact assessments** (2014)
- Office of the Privacy Commissioner of Canada **Privacy Impact Assessments**
- Pacific Privacy Consulting

Examples of PIAs

New Zealand

- Immigration New Zealand Identity and Biometrics Programme
- Department of Statistics, Integrated Data Infrastructure
- Health Practitioner Index

Australia

- Extension of Document Verification Service to private sector organisations

United States

- Department of Homeland Security inventory of privacy impact assessments