PRIVACY IMPACT ASSESSMENT TOOLKIT

July 2015

Privacy Commissioner
Te Mana Matapono Matatapu

Foreword by Privacy Commissioner, John Edwards

Since I became Privacy Commissioner in early 2014, one of the things I've emphasised is that I want to make it easy for government and business to get privacy right.

One of the ways my office can help is to provide guidance and tools that let organisations spot the opportunities for good privacy practice, help them avoid getting into difficulties, and show them what to do. This toolkit is one of the new tools that people have told me they need.

A Privacy Impact Assessment – or "PIA" – is an increasingly useful tool that organisations of all sizes can fit within their existing decision-making structures to help them to manage privacy successfully. It's not simply about complying with the law – it's about achieving business aims in an increasingly complex information environment, while also enhancing customer service and fitting in with how individuals expect their privacy to be looked after.

PIAs aren't a new concept – they're an internationally accepted framework for considering how new projects might affect personal privacy. We've had an excellent PIA handbook since 2007 and several of my fellow privacy and data-protection regulators have similar resources available.

However, a wider range of organisations are now wanting to do PIAs – from Ministries developing information-sharing proposals, new policies or legislation, right through to small businesses and NGOs. We've often been told that a more detailed, practical toolkit would be useful, one that would help people decide whether they need to do a PIA in the first place – and then, if they do, help them carry out a PIA that fits their own needs.

We've talked to a range of people about what they need and how to achieve it. This toolkit is the result.

We'll add to it over time. Feel free to drop us a line and let us know what else might be useful.

John Edwards

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

How to use this toolkit

This Privacy Impact Assessment Toolkit is in two main parts. The first part helps you decide whether you need to do a PIA, the second part explains how to do one.

Deciding whether to do a Privacy Impact Assessment

Part 1 of this toolkit describes what a PIA is and when doing one may be useful. If you decide a PIA will be worth doing, Part 1 will also help you work out whether the PIA can be kept relatively simple, or whether it's going to be a more complex and resource-intensive exercise.

We've included a template for a "Brief Privacy Analysis" (see page 17). This can be a useful way to present information to assist decision-making. It also acts as a reference point for later actions.

How to do a Privacy Impact Assessment

Part 2 of the toolkit provides a step-by-step guide to doing a PIA. It includes:

- identifying privacy risks and how to mitigate them (and identifying opportunities that good privacy management will create)
- producing a PIA report
- acting on the decisions that your organisation makes
- reviewing and adjusting the PIA as the project develops
- additional steps your organisation can consider taking, particularly if your project is large or more complex, such as consulting with stakeholders.

There are additional resources included:

- a full PIA report template (download Appendix A, "Template: Privacy impact assessment report")
- a risk and mitigation template setting out the privacy risks for your project (download Appendix B, "Template: Risk and mitigation table")
- Examples of common privacy risks and measures for mitigating them (see Appendix C, in Part 2, page 18). You may find it useful to refer to these examples as you complete the Risk and mitigation table in Appendix B
- A list of some published PIAs as examples that may help you (see Appendix D in Part 2, page 18). These published PIAs show that there are a number of different ways in which a PIA can be done effectively.

Note:

Each part can be downloaded separately from our website. You can also download the whole toolkit as a single pdf.

We'll be adding to this toolkit from time to time, so check our website (www.privacy.org.nz) for new tools and resources.

Acknowledgements

We are grateful to the people who responded to our PIA survey and who agreed to be interviewed as part of this project. What you told us has made a real difference to how we have approached the shape and content of this toolkit.

We acknowledge the work of our international colleagues who have produced guidance on privacy impact assessment, particularly Privacy Victoria (Australia), the Information Commissioner's Office (ICO) in the United Kingdom, the Office of the Australian Information Commissioner (OAIC), and the Office of the Privacy Commissioner in Canada. Their published guidance has been an invaluable source of inspiration and ideas.

We are also grateful for the help of PricewaterhouseCoopers New Zealand, who conducted the survey and interviews, produced some of the templates in the toolkit, and advised on content.

PART 1: DECIDING WHETHER TO DO A PRIVACY IMPACT ASSESSMENT (PIA)

Privacy Commissioner
Te Mana Matapono Matatapu

Part 1: Contents

Do you need to do a PIA?

A privacy impact assessment (PIA) can be useful for many projects, particularly those that involve significant risks from collecting, using or handling personal information.

To get the most of the PIA process, it's a good idea to do a PIA early on in the life of a project. The PIA will help you get the system and operation design right, and avoid expensive and time-consuming pitfalls further down the road.

Part 1 of this toolkit will help you decide whether a PIA will be useful. It will also help you work out whether the PIA can be simple and quick, or whether it will be a more complex exercise needing more time and resources.

If you decide a PIA would be helpful, **Part 2** of this toolkit, "How to do a Privacy Impact Assessment", will provide you with a step-by-step guide to completing a PIA successfully.

Why is managing privacy important?

> **"I don't find any aspect of the PIA challenging. What I do find challenging is convincing people working on projects that involve customer/staff personal information to carry out a PIA."** (survey respondent)

People care how their information is handled. They're more likely to engage with organisations that treat them fairly and openly and that can clearly justify how they handle personal information. By managing privacy successfully and showing you take care with personal information, your organisation will be able to provide better service and be better able to meet people's expectations of you.

By contrast, people object to unreasonable intrusions into their personal space and their private activities. They quickly lose trust in organisations that don't treat their information properly or that act intrusively.

So, while protecting privacy is something your organisation is legally required to do, there are other good reasons for taking care with personal information.

How can an organisation know whether a new venture or a new way of handling information will affect its customers' privacy, for better or for worse?

The answer is to do a Privacy Impact Assessment.

What is a PIA?

A Privacy Impact Assessment (PIA) is a practical analytical tool you can use:

- to **identify** whether a proposed project is likely to impact on the privacy of individuals affected by your project, either positively or negatively
- to **check** whether your project is likely to comply with privacy laws
- to **make decisions** about whether and how to adjust the proposal to manage any privacy risks and to maximise the benefits of protecting privacy well
- as a **reference point** for future action as the project, or your business, changes.

What a PIA can achieve

A PIA can identify problems and opportunities early, and make it easier and cheaper to address them. It's much simpler to build in good privacy management throughout the process, rather than trying to bolt it on at the end.

It will not be possible to identify and eliminate every risk, or identify every opportunity, and a PIA does not aim to do so. However, it gives you a good chance of identifying the most serious and the most likely problems.

"Use the PIA as an independent view of a process or system, rather than as a justification for policies already decided."(survey respondent)

PIAs – Making them business as usual

A PIA should generally not be a "once-and-for-all" exercise. If your project is long-running, has different phases, or changes over time, then it's worth going back to the PIA to update it, or even doing a fresh version.

Although this toolkit focuses on using a PIA as part of assessing and managing change, you can also use a PIA to assess how good your existing systems are – particularly if customers or others are raising concerns about how your organisation manages their personal information.

Make PIAs part of your business-as-usual thinking where possible, and use your existing systems to help. Don't create a whole new structure for a PIA if it can easily fit into your existing processes for review, assurance, risk management, or policy development.

What sorts of projects will benefit from a PIA?

Overview

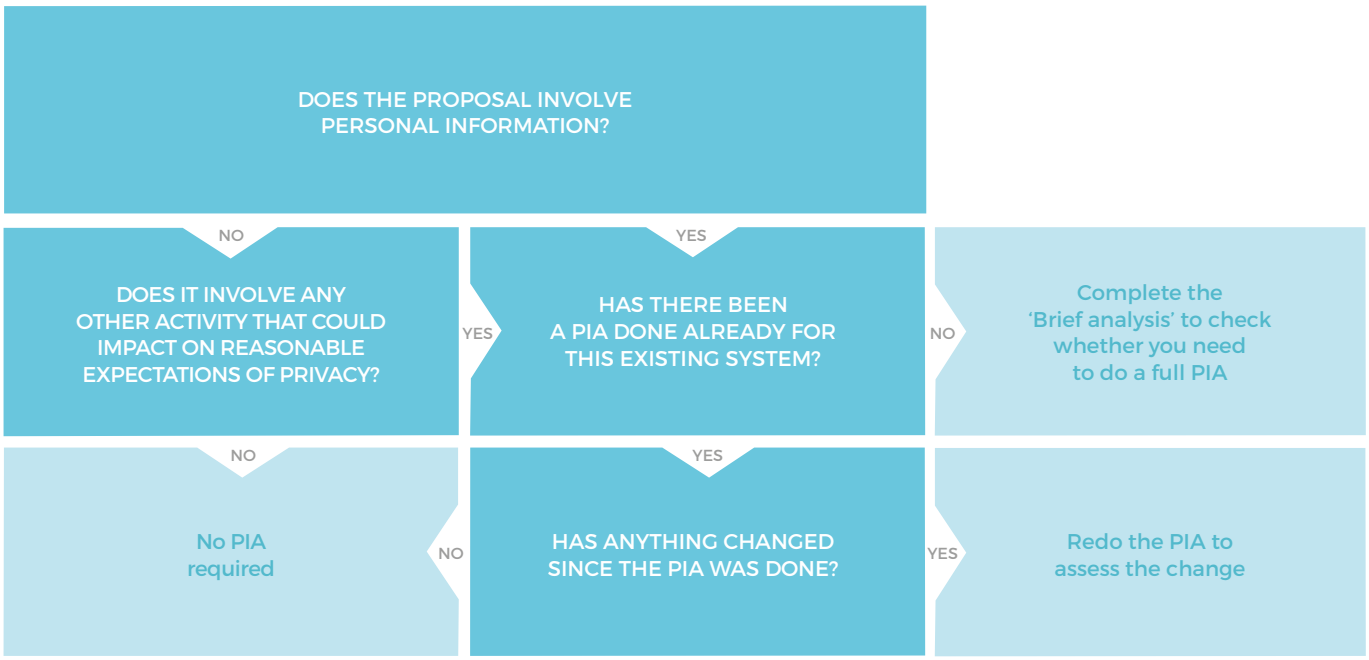
A Privacy Impact Assessment will usually be a useful part of any change project – large or small – that:

- involves **personal information** – that is, information about identifiable individuals, or
- involves information that may be used to **identify or target** individuals, or
- may result in **surveillance** of individuals, or **intrusions** into their personal space or bodily privacy, or
- may otherwise affect whether people's **reasonable expectations** of privacy are met.

EXAMPLES
Outsourcing a business or IT service where personal information is going to be held or processed off-site – even off-shore – or may be accessible to the host provider (for example storing or processing personal information in the 'cloud')
Developing data analytics to analyse existing customer information so you can better target services or advertising
A public policy change, or new legislation, that requires sharing of personal information between different agencies, or collecting new information from individuals
Developing a website or mobile app that collects names, contact information, or locations; or that allows the customer to share information with others
A major change project to introduce a new business process and supporting IT tools (for example switching from requiring clients to fill in paper forms, to enabling them to access services and information online)
Installing a new CCTV camera system, or using other technology to oversee an area where individuals might be or to monitor activities

Flowchart: An initial filter

Use this flowchart to help filter out those projects where a PIA is not going to be of sufficient use to you.



Projects more likely to benefit from a PIA

Not all projects that appear to have some kind of privacy impact will necessarily benefit from a PIA – for example:

- the use of the personal information might be uncontroversial
- the level of the possible harm, or the likelihood that the harm will in fact occur, might be negligible
- the change to how the information is managed might be only very minor and clearly consistent with what the individuals concerned would expect you to do.

The checklist below will help you decide whether your project may have significant privacy implications. These are all features that tend to lead to privacy concerns, or that are likely to cause harm or to breach the law unless they're managed correctly. If your proposed project involves one or more of these features, it's more likely to benefit from a PIA.

You'll find this list repeated in the "Brief privacy analysis" template at the end of Part 1 of this toolkit (see page 17). Adapt the list if you need to so that it more closely relates to the kinds of projects your organisation handles.

Checklist

PROJECT FEATURES THAT MAY INVOLVE PRIVACY RISKS	YES / NO
Information management generally	
A substantial change to an existing policy, process or system that involves personal information	
Collection	
A new collection of personal information (for example, information about location)	
A new way of collecting personal information (for example, collecting it online)	
Storage, security and retention	
A change in the way personal information is stored or secured	
A change to how sensitive information is managed	
Transferring personal information offshore or using a third-party contractor	
A decision to keep personal information for longer than you have previously	
Use or disclosure	
A new use or disclosure of personal information that you already hold	
Sharing or matching personal information held by different organisations or currently held in different datasets (for example, combining information with information held on public registers; or sharing information to enable organisations to provide services jointly)	

PROJECT FEATURES THAT MAY INVOLVE PRIVACY RISKS	YES / NO
Individuals' access to their information	
A change of policy that results in people having less access to information that you hold about them	
Identifying individuals	
Establishing a new way of identifying individuals (for example, a unique identifier, a biometric, or an online identity system)	
New intrusions on individuals' property, person or activities	
Introducing a new system for searching individuals' property, persons or premises	
Surveillance, tracking or monitoring of movements, behaviour or communications	
Changes to your premises involving private spaces where clients or customers may disclose their personal information (reception areas, for example)	
New regulatory requirements that could lead to compliance action against individuals on the basis of information about them (for example, introducing new conditions for a licence)	

What might a PIA pick up?

Types of privacy risks

A "privacy risk" is the risk of causing harm or distress to a person through collecting, holding or using their personal information, or otherwise intruding into their privacy.

Here are some common examples of privacy risk:

- **Too much information** – collecting excessive or irrelevant personal information
- **Insecure information** – having an insecure system that allows information to be accessed improperly, or that's vulnerable to staff making mistakes so that information is sent to the wrong place or lost
- **Inaccessible information** – setting up a system that doesn't allow people to see the information you hold about them or to correct it if it's wrong – for instance, information that's stored in paper files that aren't easily searchable, or information that's held offshore and can't be retrieved
- **Incorrect information** – holding information that is incomplete, incorrect or out of date, which can therefore lead to incorrect decisions
- **Information-sharing for new purposes** – sharing the information with another organisation for purposes that the individual isn't aware of or wouldn't expect.

Types of harm

The harm that individuals might experience from a breach of their privacy can range from mild annoyance to much more significant effects – such as serious embarrassment, financial loss, or lost opportunities for pursuing their rights or using services.

However, not all activities that intrude on privacy involve serious impacts on single individuals. Sometimes cumulative intrusions can lead to broader social effects that cause alarm – for instance pervasive CCTV coverage (so that everyone is always "on camera"), or wholesale profiling of internet activities to target advertising.

Identifying opportunities for better information management

A PIA need not focus only on risks – it can also identify opportunities for improving how your organisation manages personal information. This can in turn support the business case for change for your proposed project.

For instance, a PIA for a proposed new IT system might identify some security vulnerabilities in your existing system. Using a reputable cloud service to do the same job may provide much better protection for your customer and staff information. It could also reduce costs – with the cost of this higher security being shared across all the cloud service provider's customers, rather than being borne by your organisation alone.

Doing a PIA may also uncover an opportunity for a new type of customer service that you hadn't thought about before.

> **"The 'risk assessment' often needs to focus on the extent to which the proposal improves any privacy risks of the status quo/legacy systems."** (survey respondent)

Applying the privacy principles

What are the privacy principles?

The Privacy Act 1993 contains 12 privacy principles that set out how to manage personal information during the lifecycle of that information – all the way from collecting it to destroying it.

Here is a rough summary of the 12 principles:

1. Only collect personal information if you really need it
2. Get it directly from the people concerned where possible
3. Tell them what you're going to do with it
4. Be fair and not unreasonably intrusive when you're getting it
5. Keep the information safe
6. Give people access to their personal information if they want it
7. Let people correct information that's wrong
8. Make sure personal information is correct and not misleading before you use it
9. Get rid of it when you're done with it
10. Generally, only use the information for the purpose for which you got it
11. Only disclose it if you have a good reason
12. Only assign unique identifiers where permitted.

Other legislation with privacy implications

Other laws can override the privacy principles: if the Privacy Act says one thing, and another Act says something contradictory, the other Act wins the day. For instance, the Privacy Act may allow you to disclose information, but another Act may limit who you can disclose it to.

So if you're dealing with a number of different laws, you'll need to be familiar with the privacy implications of all of them, not just the Privacy Act.

Doing better than just legal compliance

Usually an organisation will only have legal liability for a breach of one of the 12 principles if the breach has caused some form of harm – for example, financial loss, or loss of a benefit or opportunity, or significant emotional harm. The exceptions to this are an individual's right to see their own information (principle 6) and to ask for it to be corrected (principle 7). A breach of principles 6 or 7 will lead to legal liability even if the person didn't suffer any harm as a result.

But assessing privacy impacts isn't all about legal compliance, as things that might not breach the Privacy Act might still upset the individuals whose information you're handling. For the purposes of your PIA, it's worth considering **all** privacy risks and whether they may be a problem. Your policy project, business process or technological innovation might be legal, but it might also have a negative privacy impact that you'll be able to mitigate once you realise it's there.

Even if your organisation is exempt from the Privacy Act, use the principles to help you ask and answer questions that will identify the privacy impacts for people – your project will function better for it.

Doing a brief privacy analysis

A brief privacy analysis is sometimes called a "threshold assessment", as it lets you see whether you need to cross the threshold to a full PIA.

Use the template (see page 17) to pull together the basic information you'll need to help your organisation decide whether or not to do a PIA. You can adapt the format to meet your organisation's particular needs.

Why do a brief privacy analysis?

If you think a PIA would help, you may still need to get agreement within your organisation to do one. A brief privacy analysis will help to show whether a PIA will be useful. It will also pull together some initial information that you can later use in the PIA itself, as a starting point for further enquiries.

But even if it appears that a full Privacy Impact Assessment won't be necessary – for example, because the information use will be uncontroversial or the privacy risk negligible – there still may be some value in gathering together some basic details about your project. This makes it less likely that you will miss something. Putting the basic details into a clear format also lets managers or other decision-makers see why a PIA isn't needed in this case, and records the decision not to do one. And even just asking the question "Do we need to consider privacy?" may help to set the tone for the rest of the project.

> **"For us, PIA is a gateway in the project process to confirm that the privacy controls have made it through to the finished product with senior sign-off."** (survey respondent)

If you decide not to do a PIA...

Use the Brief Privacy Analysis template to record your decision, and store the document where you can refer to it again the next time your organisation is thinking about PIAs. Keeping a store of key information about privacy will make each new PIA process easier.

If questions arise later about whether and how you considered privacy as part of your process, you can also use this record to demonstrate that you took privacy seriously and to show the basis of your decision.

If you decide to do a PIA...

The information you record using the Brief Privacy Analysis template will form the basis for going on to do the full PIA. It provides a good platform to get further details and do more in-depth analysis. Part 2 of this toolkit, "How to do a Privacy Impact Assessment", will take you step-by-step through the process.

Part 1: Appendix

Appendix A: Template – Brief Privacy Analysis

Download here 

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