# Assessing Risk

## Overview

Privacy Impact/Risk Assessments (PIAs/PRAs), and privacy threshold assessments are good operational tools for organisations to analyse projects or initiatives that involve new or changed ways of handling personal information. For example, when adopting new technology for your organisation's business processes.

Assessment of privacy risks should be tailored to the specific needs of your organisation and should consider your obligations under Te Tiriti as well as the broader cultural context of your collection, use, and disclosure of personal information. For example, there may be cultural characteristics that mean you collect and use information in ways that reflect the specific needs of that community.

You may want to look at the Data Protection and Use Policy (DPUP) Principles for guidance on this.

You can find guidance on assessing your organisation's privacy risk profile in the Know your Personal Information pou.

## Who is this for?

Your privacy function and those with responsibility for completing or reviewing privacy risk analysis and assessment, such as those writing and approving Privacy Impact Assessments.

## Key objectives of the Assessing Risk pou

### What would we expect to see?

- Organisation has evidence of privacy assessment process, training, and completion of assessments.
- Policies and procedures in place covering how PIAs are completed, and who completes them.
- Evidence that assessments have been used to design or review systems, products, services, processes or initiatives that use personal information.

## Privacy by Design

Privacy by Design is a methodology that includes privacy as a key requirement in the design of any new system, product, service, process, or initiative. This methodology also ensures a more meaningful risk management process, by requiring engagement with your organisation's privacy function throughout the lifecycle of a project, rather than at a single point in the process when it may be too late.

Principles of the Privacy by Design methodology include:

### Proactive not reactive, preventative not remedial

Privacy must be considered at the beginning of a project and throughout its lifecycle. Privacy considerations should help drive the design and prevent or mitigate privacy risks, rather than being tacked on at the end of the project design phase.

### Privacy as the default

The default setting of any design should protect individual privacy, which means privacy protective settings should be the starting point. For example, minimising the collection of data to only what's necessary to achieve your lawful purpose, and limiting the use of that data to the purpose it was collected for.

### Privacy embedded into design

Privacy should be a foundational piece in the design of a product, system, process or initiative and should be so essential to the design that it won't function if the privacy settings are changed or removed.

### Full functionality

Privacy requirements should not be delivered at the expense of other core functionality. It shouldn't be a trade-off. Privacy requirements should support and enable the delivery of other requirements.

### End-to-end security

Data must be protected at every stage of the information lifecycle for a new product, system, or process. This includes the collection, storage, use, disclosure, and disposal of personal information.

### Visibility and transparency

There should be visibility of the privacy risk assessments, design decisions, and privacy controls that have been established for the product, system, or process. This will increase trust in the project.

### Respect for user privacy

If the product, system, or process will be used by people (such as customers) then those people and their experience should be central to design decisions.

## How do you implement Privacy by Design in practice?

Some of the things you'll need to do to successfully embed a privacy by design approach are:

### Define accountabilities

As outlined in the Governance pou, your organisation must clearly define roles and responsibilities, accountability and ownership, and escalation processes. The privacy function and the project team need to know:

- Who is accountable for privacy risks.

- Who is responsible for embedding privacy mitigations.
- Who needs to be consulted about compliance with the Privacy Act.
- Who should be informed of the privacy outcomes.

If these aren't clearly defined, there's a risk that all responsibility and accountability will be placed on the privacy function alone. This isn't an appropriate or sustainable approach.

## Strategic intervention

Your privacy function needs to be involved at the right times in the project lifecycle. Most importantly, they need to be engaged early in the design stage of a project to make sure that privacy requirements can be properly considered and embedded into the product, system, or process from the start.

For projects with high privacy risks (for example, new biometrics, AI, or automated decision-making projects) your privacy function should attend design meetings and be part of early design conversations. They also need to be involved at critical stages of the project's lifecycle, such as testing and launch. At the start of a project, the privacy advice can be general and theoretical, but at the later stages it should be more detailed and practical.

## Being responsive and timely

Your organisation's leaders need to ensure your privacy function is capable and available to the project. Delays in providing privacy advice in time for important project decisions could result in the project team thinking it's okay to bypass privacy requirements. This will increase risk. It's important to note that the capability of your privacy function relies on adequate resourcing and allocation of priorities.

## Adaptability

Over the course of a project, requirements may change. Deliverables may be updated according to changing project objectives or new design limitations, timeframes may be shortened or lengthened, or external factors may alter the project risks. Your privacy function will need timely updates on any changes to project deliverables to adapt their advice or risk assessments.

## Enable and support

Your privacy team should help a project team to get privacy right by providing clear and practical guidance on how to put privacy principles into practice. Privacy training for key project team members could further enable positive privacy outcomes and provide important relationship building opportunities for your privacy function.

## Content

Privacy impact/risk assessments should consider the breadth of privacy issues raised by a project. They should include issues such as ethical considerations, indigenous and/or cultural privacy considerations, and the importance of data ownership and governance. This could include working with other subject matter experts, such as information security and data governance experts, and leveraging the capabilities of other internal teams.

## Risk-based approach

Engagement with the privacy function, and any recommended privacy controls, should be targeted based on clearly defined thresholds and risks. For example, you may consider some initiatives higher risk if they will involve a large amount of personal information, use of a novel technology (e.g. biometrics), or if the risk of harm is high, should a privacy breach occur.

### Balance

Privacy impact/risk assessments will inform your organisation of both risks and opportunities for a project. Generally, good privacy practices will assist rather than prevent the achievement of a project's goals. Often a risk for privacy is also a risk in other areas of the project. It's just as important for a privacy impact/risk assessment to identify and highlight privacy opportunities and improvements as it is to call out the risks.

### Targeted communication

Privacy advice should be communicated in a way that is meaningful and understandable to the target audience. Documents should be succinct and easy to understand, with risks and recommendations clearly outlined. Privacy messaging to operational staff should be practical and detailed, whereas privacy messaging to senior leaders may be more strategic and high-level.

### Visibility

Internal privacy impact/risk assessments and controls are important to ensure privacy is protected, but if they're not visible to the people concerned, they do nothing to build trust and confidence in a product or process. Visibility could mean making privacy assessments public or, if this isn't appropriate, making efforts to provide the public with assurances that privacy has been designed into the product or process, and how this has been achieved.

## Privacy Impact Assessments

A privacy impact assessment (PIA), also known as a privacy risk assessment, is an essential part of many projects and proposals and can be used to help your organisation identify the potential risks arising from the collection, use, or handling of personal information, and to find out if you're meeting your legal obligations.

PIAs focus on identifying the ways a new proposal or operating system, or changes to an existing process, may impact personal information. This helps organisations make more informed decisions and better manage privacy risks.

It's important to decide whether to do a PIA early on in a project or new initiative. OPC's brief privacy analysis template can help you assess whether a full PIA is appropriate. If you fail to identify how your project is likely to impact the individuals whose information you are collecting and using, there are real risks for your organisation and for the success of the project. In many projects, it may be that privacy advice is provided throughout the design phase and a PIA is done at a suitable stage further down the track.

A PIA is a practical analytical tool you can use to:

- Identify whether a proposed project is likely to impact on the privacy of individuals, either positively or negatively.
- Check whether your project is likely to comply with privacy laws.
- Make decisions about whether, and how, to adjust the project to manage any privacy risks and to maximise the benefits of protecting privacy.
- Highlight future action points as the project, or your business, changes.

For full guidance on whether you should do a PIA, and step-by-step templates and tools on how to do one, check out our PIA toolkit.

## Privacy analysis in policy development

If you're a public sector organisation, we encourage you to undertake privacy analysis when developing legislative or other policy proposals. That will help shape the proposal to be privacy-protective and decrease the likelihood and severity of any privacy risks. Privacy analysis should be considered through the Regulatory Impact Assessment process.

In general, privacy analysis done at a policy level will have a different focus compared to analysis done from an operational perspective. For example, there will be a greater emphasis on whether the privacy intrusion is justified given the policy objective and privacy risks. At an operational level, the privacy analysis focuses more on mitigating specific privacy risks within a system, product, or service, or developing privacy enhancing processes and procedures.

It's also important you're considering the operational impact and practicalities of implementation early in the policy development process.

OPC would expect any privacy analysis for a policy proposal to cover:

### Proportionality analysis of privacy risks

- Evaluate the privacy risks of your proposal and weigh them against the intended benefit of the proposal.
- Calculate the level of privacy risk, take account of factors such as the sensitivity of the personal information, the amount of personal information being collected, the risk of a privacy breach occurring, and the nature of potential privacy harm to individuals.
- Is the impact on privacy sufficiently justified by the expected benefits of the proposal?
- Is there a strong evidence-base to support the expected benefits of the proposal?
- Is there evidence from international jurisdictions that you can use to support your case?

### Outline a robust policy rationale for collection of personal information

- If you are proposing new collection of personal information, there needs to be a robust policy rationale for why your organisation needs to collect this information.
- Do you have evidence that the collection of the personal information is *necessary* to achieve your policy objective?
- Consider whether there is an alternative way to achieve your policy objective that involves collecting less or no new personal information.

### Clear purpose and use for personal information

- There must be a clear purpose for collecting each type of personal information you are proposing to collect, and this should be directly linked to how your organisation is going to use this information.
- An organisation may have a good reason to collect personal information, but it needs to show that this information will be used to achieve the intended outcome. For example, does the organisation have the resources to use the information it's proposing to collect?
- Remember that you can't lose information that you don't collect! Minimising the data collected is an important part of minimising risk for your policy.

## Social license

- Would the public expect you to be collecting this personal information? Would they be okay with the way you intend to use or share their information?
- What consultation have you undertaken and what evidence do you have of public and key stakeholder views?
- Have you incorporated measures to enhance transparency of the collection of personal information, and how it will be used and shared? For example, consultation, publishing policy documents, media releases, privacy policy, ability for individuals to request access to their own personal information.

## Specific impacts

- Will the proposal have specific impacts on personal information of Māori and how have these impacts been addressed?
- Will the proposal have specific impacts on children and young people, or other vulnerable populations, and how have these impacts been addressed?
- Have you sought ethical review or advice from ethics committees?

## Technological risk

- Are you proposing to use a novel technology or use an existing technology in a novel way?
- Are you using artificial intelligence (AI), automated or algorithmic decision-making to analyse personal information? What is the risk of bias? Have you allowed for human oversight of decisions made using this technology?
- Do you have the capability and resources to safely store this information? If you don't, you open yourself up to data breaches that can be harmful to individuals and to your organisation.

## Operational impacts and implementation

- Will the proposal have specific operational impacts, and how have these impacts been addressed?
- Have the practicalities of implementing the policy been considered, and how will these be addressed?
- Where the proposal involves collecting from or sharing personal information with external third parties, consider whether it's appropriate to consult with those parties to understand any operational or privacy impacts that might be relevant to their organisation.

### OPC's role

Completing your privacy analysis using this guidance is part of ensuring you've undertaken a robust policy process and built privacy considerations into the design of the proposal.

As the independent privacy regulator in New Zealand, our Office cannot endorse or approve your privacy analysis. However, we may be able to provide you with advice and direction to support your analysis of privacy during your policy development process.

### Implementation

If the policy proposal progresses, we expect the team in charge of delivering or implementing the project will also complete a privacy impact assessment and cover all the Information Privacy Principles to ensure the project meets the legal obligations set out in the Privacy Act.

The high-level decisions about the proposal will likely have been made during the policy process, for example, what personal information is collected and for what purpose. Therefore, the privacy impact assessment for the implementation phase should have a greater focus on identifying and mitigating specific privacy risks associated with the project.

Doing a privacy impact assessment will also enable the team to work through important privacy decisions, like addressing how the information will be kept safe, how long to retain the information for, and how to ensure individuals can request access to their personal information.

## Third-party privacy risk management

If you decide to use a third-party service to handle the personal information your organisation has collected and is responsible for, you remain responsible for protecting that information. Under the Privacy Act, you hold the personal information, even if you are using a third-party service. This responsibility shouldn't stop you from using third-party services, but you need to assess the risks and make sure you deal with them appropriately. Risks that you should consider include:

- Privacy capability/maturity of the third party, including their history of privacy breaches.
- Contractual protections to ensure you and the third-party service agree who is responsible for what, including a requirement that the third-party service provider notifies you of privacy breaches.
- Cyber-security readiness of the third-party service (whether they do regular penetration testing and how they respond to the recommendations of the tests).

OPC is developing a separate piece of guidance on this, which will be linked here when it's published.

## Organisation examples

We've included some use cases based on fictional organisations to demonstrate each of the pou in practice. Read more about them in Introducing the Organisation Examples.

## Large business – Fern Leaf

Fern Leaf has an established privacy review process in place. As a large organisation it accepts that not every new initiative or change to a process can be reviewed in full by the privacy team. It has created a privacy threshold assessment which is based on key risk areas from its use of personal information. These have been built online and, depending on the answers, will indicate whether the business needs to conduct a fuller privacy impact assessment. Where they do need to, the business is asked several other questions which are then reviewed by the privacy team, who completes the PIA. At the end of the PIA, the privacy team set a date that the business should re-review the PIA by to ensure that it is kept accurate.

As Fern Leaf has been around for a long time, it accepts that there may be processes that have not had a privacy review or that have not had one conducted for a while. It uses the PIA to also identify key business processes that it should investigate, even if there isn't a specific change to the use of personal information. This is good privacy practice. The privacy team also creates stats from the number of threshold assessments and PIAs completed, regularly reporting upwards.

## Small business (charity) – Reach High

Reach High has developed a simple PIA checklist to assess any changes to the way it handles personal information about its clients. The template runs through the information privacy principles and reminds staff to think about privacy when designing and implementing the changes. This is easy for Reach High to implement because of its size and the fact that the Director of Support Services must sign off any changes that impact on client information anyway.

As a small organisation with a minimal budget, Reach High relies heavily on service providers, and particularly on cloud-based software solutions, including document management systems and productivity applications. The Reach High PIA checklist includes questions about any new service providers, to ensure that the contracts contain the right assurances.

For larger projects, where Reach High may not have the privacy expertise to properly identify and assess all the privacy risks, it uses external privacy experts to complete a more in-depth PIA.

## Start-up – Swiftstart NZ

As a SaaS platform, Swiftstart NZ was aware from the outset that it would be important to document a PIA for the proposed platform. Swiftstart NZ considered this would be necessary, not just to ensure the platform was fully compliant with privacy requirements, but also because they anticipated this would be an important piece of collateral for demonstrating to potential clients that they had taken appropriate steps to consider privacy and address potential risks.

The founders of Swiftstart NZ worked with their software developers to complete an initial draft PIA document, based on the OPC template. Once they obtained seed funding, they passed the draft document to an external privacy consultant to review and prepare a finalised PIA document which would be suitable to be shared with clients on request.

Swiftstart NZ's Operations Manager is conscious however that, while the platform fundamentals are unlikely to change significantly, the Swiftstart NZ software developers are continuously working on improvements – the founders keep having great ideas to improve functionality for clients! To make sure the PIA remains accurate, the Operations Manager decides to review it on a 6 monthly basis and provides all employees with an introduction to privacy by design concepts and the importance of assessing any new ideas for consistency against the existing PIA – and making any changes as necessary.

### Small business (non-tech) – Green Gardens

Green Gardens uses the Brief Privacy Analysis template from the OPC PIA Toolkit to assess any changes to the way it handles personal information about its clients. For example, when Green Gardens decided to outsource their arborist services so they could offer this to their clients, the Administrator in their role as Privacy Officer completed the privacy analysis template since Green Gardens would need to share personal information with the arborist business. The privacy analysis document then went to the Owner/Manager for review and acceptance of any privacy risks.

### Independent contractor – Jo Jones

Jo Jones uses the OPC PIA Toolkit to develop her own privacy analysis checklist, which she uses to assess any changes to the way she handles personal information about her clients. For example, when Jo decided she would offer virtual consultations via Zoom, she completed her privacy analysis checklist to assess any privacy risks associated with the new process, and decided what threshold of risk she was comfortable accepting to go ahead with implementing it.

### Government agency – The Ministry

The Privacy team at the Ministry understand the importance of privacy by design and have run a communications campaign targeting project managers and digital teams within the Ministry to engage early on projects or business changes that may involve a new use, collection, disclosure or other change in handling of personal information. The Privacy team has created a privacy threshold assessment for teams to complete with an identified threshold for completing a full PIA, with the ability for the Privacy team to review and sign-out. The privacy team also support teams that do complete full PIAs by providing advice and support to those writing PIAs, and occasionally the privacy team will write the PIAs themselves. The privacy team also works with the legal and procurement teams to ensure that privacy is considered when new or renewed contracts for service are being prepared so that liability is clear and understood by both the Ministry and the contracting party. The Ministry's policy teams do not complete privacy impact assessments for policy proposals that may impact privacy, but they receive training on the Privacy Act, including Approved Information Sharing Agreements, and understand how to consider privacy when preparing a new policy proposal, including consultation with the Office of the Privacy Commissioner.