Governance

Overview

Doing privacy well requires a comprehensive and consistent approach from leadership that aligns with your wider *organisation's goals, values, and risk. It also means that governance members need to have a clear understanding and effective oversight of their organisation's privacy risk and deliberately make privacy a priority.

For guidance on assessing your organisation's privacy risk profile, see our Know your Personal Information pou.

This is not only essential for compliance and risk management but will also enable your organisation to improve its data quality, innovation, customer and stakeholder trust, and decision-making processes.

The role of governance is to define and provide this consistent approach.

This pou covers four core elements of effective privacy governance:

- **Leadership** – setting clear expectations about what is important and how the organisation operates.
- **Oversight** of new proposals that may affect privacy, ongoing work, and the overall privacy programme.
- **Accountability** at a senior level for the way in which the organisation handles personal information.
- **Senior sponsorship** of the *privacy function, including managing resourcing

Defined terms used throughout the Poupou Matatapu guidance:

*Organisation – to refer to any person or agency that has obligations under the Privacy Act.

*Privacy function – your organisation's privacy officer or team. We know that organisations will have different names for the roles or teams that do this work, but we've used the term 'privacy function' to describe this consistently throughout the guidance.

Who is this for?

Boards of Directors and business owners or those who:

- Appoint senior management.
- Approve major policies.
- Make major decisions.
- Oversee the organisation's performance.

This includes executive and senior leadership team members of public sector agencies.

These roles are generally referred to as "governance members", and relevant groups of governance members (such as boards of directors or governance committees) are collectively referred to in this pou as "governance groups".

Your organisation's privacy function, including those who:

- Work to ensure the organisation complies with the Privacy Act.
- Advise the organisation on compliance with privacy requirements.
- Advise the organisation on the potential privacy impacts of changes to business practices, and whether improving privacy practices might improve the business.
- Are familiar with any other legislation governing what the organisation can and cannot do with personal information.

Key objectives of the Governance pou

What would we expect to see?

- The governance function can demonstrate that it takes action to ensure that privacy risks, gaps or issues are appropriately identified, documented and addressed.
- The governance function actively supports embedding privacy in operational practice.
- Ownership and accountability for oversight of privacy within the organisation is clearly documented (for example, in an organisational chart, role descriptions, or other administrative documents).
- Resourcing of the privacy function is appropriate for the organisation's privacy risk profile and is regularly reviewed.

What does a governance function look like?

Governance can take a range of different forms and be performed by different people, depending on the size and structure of your organisation.

The leader or leaders of a small organisation are likely to be close to what's happening already and are often actively involved in the work. As a result, specific groups, and complex communication and reporting structures are often unnecessary. The same person may wear multiple hats.

Larger or more devolved organisations, with wider work programmes, are more likely to need a governance group. They may even have several layers of governance, such as an internal governance group made up of senior staff members, with only the most high-risk issues being escalated to their Board

It's common for privacy to be one of several related issues that a governance function is responsible for (for example, security, IT, or health and safety). It's not necessary to create something bespoke or distinct for privacy, so long as the governance function understands and accepts that privacy is one of the issues it is accountable for and has the authority to make decisions on behalf of the organisation. Where a specific governance group has been established to provide oversight of issues including privacy, it should have a reasonable understanding of privacy issues (either through training or inclusion of someone with privacy expertise) and work closely with the organisation's privacy function.

The role of the governance function

To better understand the responsibilities of a governance function, it's useful to distinguish between governance and management responsibilities.

Governance:

- Focus on determining organisation's purpose.
- Develop effective governance culture.
- Hold management to account.
- Ensure effective compliance.
- Work with management to develop strategy, corporate policies and work programmes that are then implemented by management.

Management:

- Make operational decisions and policies.
- Keep the governance group educated and informed.
- Bring well-documented recommendations and information to the governance group, including on budget and resourcing.

Some groups, like executive leadership teams in government departments, can wear both governance and management "hats". This pou focuses on their governance functions.

Leadership

A key feature of good privacy governance is informed leadership. This includes:

- Setting the tone from the top about the importance of treating personal information well.
- Identifying a clear strategic direction for privacy management within the organisation to ensure continuous improvement.
- Communicating clear expectations about what to do in relevant areas of practice and following through to ensure those expectations are met.
- Seeking advice from the privacy function or privacy officer regularly and taking their advice seriously.

Taking a strategic approach to privacy

A privacy programme should be strategic and SMART – specific, measurable, achievable, relevant and time-bound.

It should:

- Be aligned with the broader organisational strategy and be relevant to the work the organisation does.
- Ensure the organisation will comply with all applicable laws, including the Privacy Act 2020 and relevant codes of practice.
- State specific goals for promoting a privacy culture and improving privacy practices within the organisation.
- Be 'owned' or otherwise approved by one or more members of the governance group.
- Have a timeframe, for example a 2-year plan with clear deliverables.
- Identify who the key stakeholders are, to make sure they are included in conversations or decisions.

Creating a positive privacy culture

There is a lot more to privacy than just meeting minimum legal compliance requirements – it's about being ethical, being trustworthy, meeting customer expectations, and providing the solid foundation for your organisation to operate and grow.

A culture of privacy is when respecting and protecting personal information is part of your organisation's DNA. Your staff generally know what they can and can't do with personal information and know who to go to when they're unsure. Your systems and processes support safe and trusted handling of personal information. Your ideas for innovation take full account of how people will be affected by the change and aim to improve things for them.

If your governance arrangements are focused on creating a culture of privacy, legal compliance should follow naturally. A strong privacy culture is also increasingly a competitive advantage.

Oversight

To have sufficient oversight of your organisation's privacy management, you need to receive and consider information that shows you:

- How mature the organisation is when it comes to privacy.
- Whether the organisation's privacy maturity is in line with its broader strategy and long-term goals.
- What levels of privacy risk or privacy opportunity are being created by the work being conducted in the organisation and how to manage those risks or seize those opportunities.
- Whether your organisation is complying with the law.
- Whether the privacy programme is targeted to the right areas and is effective and, if not, what needs to be done to improve it.

You also need to ensure that the governance function considers and acts on this information. Without active oversight, the information will just add noise or detract from sensible messaging. This means that the governance function – whether it is the senior leadership team or a specific governance group – will need to ensure that privacy is a regular agenda topic. Where the oversight process reveals privacy risks, capability gaps, or compliance issues, the governance function needs to take action to ensure that these risks, gaps, or issues are appropriately documented and addressed.

Accountability

The governance function makes strategic-level decisions about how to manage privacy issues: what to prioritise or not prioritise; what risks to remediate and what risks to accept; how to resource the privacy team and programme, or whether to spend energy and money elsewhere.

Accountability means accepting ownership of privacy risk. In some organisations, an entire governance group could accept collective accountability for privacy. In others, and particularly in larger organisations, accountability for privacy could sit with one senior leader, sometimes referred to as a 'privacy sponsor'. This could be the senior leader who is accountable for the part of the organisation that processes the most personal information

(such as a Chief Customer Officer) or the senior leader who is accountable for the business function within which the privacy functions sit (such as a Chief Risk Officer).

Accountability also means being able to explain (whether proactively or on request) what these decisions were and why they were made. If something has gone wrong, accountability also means making sure that matters are fixed.

Others – including subject matter experts such as the privacy officer or team – will be *responsible* to the governance function. They conduct the day-to-day work, make recommendations about what to do and then assist with implementation. It's important to note that subject matter experts may not be accountable for risk acceptance decisions or own the privacy risk for the organisation. As noted above, this overall accountability and ownership rests with the governance function, which can make decisions on the advice of subject matter experts.

Senior sponsorship of the privacy function

A key role for a governance function is to support the privacy function in the organisation.

The privacy function is responsible for delivering the work and for providing expert advice to the governance function about what is required. The governance function needs to:

- Assign accountability for oversight of privacy issues to a member or members of the governance function.
- Right-size the privacy function for the organisation.
- Make sure it is positioned in the correct place in the organisation so it can be effective (including being able to escalate significant risks as required).
- Ensure there is adequate resourcing to implement and maintain the privacy programme, including providing any necessary assurance that the organisation successfully implements its policies and procedures.

Who should be the privacy officer?

The Privacy Act requires organisations to have at least one person who fulfils the role of a 'privacy officer'. However, the number of people responsible for privacy management will depend on the size of your organisation, the work it does, and what personal information it handles.

Generally, your privacy officer should be sufficiently senior to have influence, but not so senior that they don't have operational oversight of the day-to-day duties of the privacy function. In very small organisations the privacy officer is likely to be part of the governance function, or even the CEO. In very large organisations it's more likely that the privacy officer will report to a senior leader.

You can find out more about who should be the privacy officer, and their respective duties, in our Privacy officers guidance.

Training privacy 'allies' (people within other specialist teams who understand privacy well) can also be very effective to build a broader privacy culture. It can also help to ensure that work can be delivered safely and quickly; the basics are done in-team, while the privacy specialists can focus on more complex advice. These allies can act as the first port of call for privacy queries.

The Privacy Act also permits organisations to outsource some of the duties of a privacy function, which can allow the organisation to increase its privacy resource when necessary.

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

As a large organisation, Fern Leaf has a dedicated privacy team. This consists of the Head of Privacy, Senior Managers and analysts. Fern Leaf regularly reviews the workload and strategy for privacy to ensure that the function is staffed well. The Head of Privacy holds the Privacy Officer role however the privacy team acts as delegates for the role.

The privacy team's key senior sponsor is the Chief Risk Officer (a member of the executive), and the team regularly reports on privacy compliance to several different forums including the Board of the company. Fern Leaf has also set up a dedicated privacy stakeholder forum made up of senior executives from different business units who process personal information. The group is kept informed of key privacy initiatives and supports the privacy team in supporting their work.

Fern Leaf's privacy team also works very closely with data and marketing teams. Where needed, they feed into these governance groups and work collaboratively on strategy.

Small business (charity) – Reach High

As a small organisation, Reach High has decided that privacy accountability sits with its Chief Executive Officer. The Director of Support Services, who is responsible for the Counselling Team and Mentoring Team, is the Privacy Officer. This is appropriate for the size of the organisation and ensures that privacy matters are effectively escalated to the Chief Executive Officer.

The Chief Executive Officer, together with the Director of Support Services, agree that privacy is a core value for Reach High, which depends on the trust of its clients to effectively deliver services. Together, they develop a privacy strategy for Reach High that aims to build a positive and respectful privacy culture among all staff. The Counselling Team Manager and Mentoring Team Manager will help to execute this strategy over time.

The Director of Support Services ensures that the managers in her team provide regular reports on privacy compliance and progress on meeting the privacy strategy goals. She then escalates these reports to the Chief Executive Officer and, where required, seeks decisions on risks and support for resourcing.

Start-up – Swiftstart NZ

As a small emerging business, Swiftstart has limited resources and capacity to dedicate to privacy but knows it's an important thing to get right. The three founders (who act as Chief Executive Officer, Chief Technology Officer and Chief Product Officer) decide they will hold

overall accountability for privacy at Swiftstart NZ and decide to dedicate part of their regular strategic decision-making meetings to any issues around privacy at Swiftstart NZ.

They appoint Swiftstart NZ's Operations Manager as the Privacy Officer as part of their broader role managing any legal and compliance issues. They ask the Operations Manager to draft a privacy strategy for them to review and endorse by the end of the quarter. They anticipate Swiftstart NZ's operations may change rapidly, particularly as they grow the business and expand into international markets, so decide to complete a comprehensive review of the strategy in 12 months' time and ask the Operations Manager to provide monthly updates on progress in the meantime.

Small business (non-tech) – Green Gardens

As a small business that collects limited personal information, Green Gardens has limited resources to dedicate to privacy but knows it has obligations under the Privacy Act, and that maintaining client trust is important. The Owner/Manager and the Administrator decide they will hold joint accountability for privacy at Green Gardens, and they include privacy as a standing agenda item for their 6-monthly business strategy meetings.

The Owner/Manager appoints the Administrator as the Privacy Officer as part of their wider role, to manage compliance and other privacy related issues. At their 6-monthly business meetings, the Administrator, as part of their Privacy Officer responsibilities, reports back to the Owner/Manager about any privacy incidents (such as near misses), any updates to the maintenance of their privacy statements, and any privacy requests or complaints that have been received over the past 6 months.

Independent contractor – Jo Jones

As an independent contractor, Jo Jones is the privacy officer by default. She is both accountable and responsible for managing privacy effectively when conducting her business and providing services as a Registered Dietitian.

Government agency – The Ministry

As a medium-sized government agency, the Deputy Chief Executive has responsibility for privacy at a SLT level. The Privacy Manager is the appointed privacy officer and reports regularly to the General Manager who then reports up to the DCE. The Privacy Manager provides quarterly reporting to the DCE for SLT on numbers of privacy breaches, complaints, near misses, and other privacy issues. The Privacy Manager follows existing business planning processes to seek investment in particular privacy initiatives like additional bespoke training and works closely with other parts of the business to support privacy-adjacent activities (e.g. investment in cybersecurity). The SLT has agreed to a privacy strategy for which the Privacy team is primarily responsible for executing, supported by other teams with related functions.