Privacy Commissioner
Te Mana Mātāpono Matatapu

Know your personal information

Overview

One of the first steps in preparing to plan and implement a privacy programme is to understand what personal information your organisation collects, uses, stores and discloses. This will allow you to work out what your organisation's risk profile is.

Knowing your personal information, and assessing your organisation's privacy risks, will help you work out how best to apply the guidance in our Poupou Matatapu framework.

Who is this for?

Your privacy function and anyone else with a responsibility for privacy or data within your organisation.

Key objectives of the Know your personal information pou

What would we expect to see?

- The organisation has a data inventory or equivalent and has used this to assess its risk profile.
- Staff understand what personal information is and how they can use it in their role.
- There is a central log or record of the organisation's current data/information sharing agreements.
- Policies for data classification, including handling and retention, are documented and compliance with these policies is assessed.

Understanding your organisation's privacy risk profile

It's important to know your organisation's privacy risk profile, which requires an assessment of your organisation's privacy risk. Undertaking activities such as data inventory is a core component of this.

Key aspects you need to consider are:

- The legislation that governs how you can collect, use, share and dispose of personal information. Your legal and regulatory obligations will likely extend beyond just the Privacy Act. If you offer products or services overseas or are collecting personal information about individuals outside of New Zealand, you should also make sure you're aware of any local laws which could apply.
- The quantity and sensitivity of the personal information that your organisation holds. For example, a lot of non-sensitive personal information may be less risky than a smaller amount of highly sensitive information.
- Your organisation's objectives, cultures, and policies – how important is personal information to your business operations and goals? How is privacy reflected in your values, policies, and culture?

A privacy risk assessment will enable your organisation to:

- Identify privacy risks.
- Identify potential mitigations.
- Prioritise resources to areas of greatest risk.
- Identify opportunities for improvement.
- Ensure a risk-based approach to privacy, that accommodates other important risks to the organisation.

Assessing agency privacy risk is a useful resource that outlines key steps in assessing and setting your organisation's risk profile, including guidance on completing a data inventory.

Understanding personal information

What is personal information?

Personal information is any information which tells us something about a specific individual.

People's names, contact details, financial, health and purchase records can all be personal information. The information doesn't need to name the individual, if they are identifiable in other ways, like through their home address or another identifier, or if their identity could be pieced together.

Any information that you can look at and say "this is about X" may be considered personal information if X is an identifiable person. If someone can link the information with other information to identify the person it's about, then the information is considered personal information.

The information doesn't need to identify the person to the world at large for it to be considered personal information. For example, sharing information that someone at a particular address has previously been convicted of serious offending doesn't identify the individual to the world at large, but it would be identifiable to those who know who resides at that address, and is still personal information.

Similarly, sharing a list of National Health Index numbers (NHIs) of people who have been screened for bowel cancer might not identify those people to the world at large, as NHI numbers aren't known by everyone – but it still clearly tells you something about particular people, and could be identified by anyone with access to NHI numbers.

The Privacy Act is concerned with personal information in any format. This means that all sorts of things can contain personal information, including notes, emails, recordings, photos and scans, whether they are in hard copy, electronic form, or can be shared verbally.

What is sensitive personal information?

The Privacy Act applies broadly to all personal information, and is not limited to private, secret, or sensitive information. However, if the personal information is considered sensitive, then extra care needs to be taken.

Sensitive personal information is information about an individual that has some real significance to them, is revealing of them, or generally relates to matters that an individual might wish to keep private.

Certain types of personal information can generally be regarded as sensitive if the inferences that can be drawn about the individual from that information are potentially sensitive. For example, information about a person’s race, ethnicity, gender or sexual orientation, sex life, health, disability, age, religious, cultural, or political beliefs can reveal details that are very personal and that could result in the individual being treated in a certain way if used or revealed in a particular context.

Health, genetic, biometric, and financial information is inherently sensitive, as well as personal information of children and young people, given their vulnerability and more limited agency than adults.

The Privacy Act doesn’t prescribe fixed categories of “sensitive” personal information. Rather, any personal information can be sensitive, even highly sensitive, depending on the context, including cultural perspectives.

Read our guidance on working with sensitive information.

Data inventory

Completing a data inventory for your organisation will give you a comprehensive view of the personal information you are responsible for and how it’s organised.

It should include:

- What personal information you hold.
- Where it’s coming from, e.g. data sources and information flows.
- Who it is about, e.g. employees, customers, or contractors.
- What laws apply to it.
- Where it’s located (offices, the Cloud, third parties, etc.).
- How it’s being stored (hard copy, digital, database, etc.).
- Who has access to it, including third parties.
- How it’s shared – within your organisation and externally.
- How it’s used.
- How long it needs to be retained for.
- When it’s disposed of.
- Who in the organisation is accountable for it (this is sometimes referred to as the ‘data owner’ or ‘data steward’).

You will need to identify all the repositories in which personal information is stored. A repository is any place that holds data, makes data available to access and use, or organises data. For example, a database, spreadsheet, or paper filing system. It also includes data stored on laptops, and photos or messages held on mobile devices.

You will also need to know how and when you’re collecting personal information, and the legal basis for that collection, to comply with information privacy principle 3. You can read more about this in our Transparency pou.

There are a range of different solutions for arranging and understanding the personal information your organisation holds. The goal is to have a fit for purpose solution that enables you to have a clear view of your data holdings. A data inventory is just one example of how to achieve this.

Categories of personal information

Completing data inventory exercises can be a large and time-consuming task. However, you don't necessarily need a list of every piece or type of data that you hold. As a starting point, you could develop a high-level view of data holdings, and then a plan to complete a more detailed inventory of higher-risk data.

The main goal is to identify areas where privacy risks or opportunities may arise. For any new initiative that collects or uses personal information, you should complete a data inventory or add to an existing one.

Some basic examples of information categories include:

Employee information

- Names.
- Personal contact information (addresses, phone numbers, email addresses).
- Employment records (contracts, performance reviews, salaries or wages).
- Candidate or Applicant information.

Customer information

- Depending on your organisation you might break this category down further based on products and or services you provide.
- You might categorise by 'account information' and provide fuller explanations to reference more granular descriptions.

Marketing

- RSVP lists for events.
- Email marketing lists.
- Customer databases.

If you're a public sector organisation, it's also important to keep a register of your information sharing agreements. See guidance on information sharing catalogues at Create an information sharing agreement | NZ digital government.

Responsibility and ownership

Depending on the size of your organisation, how much personal information you are responsible for, and the sensitivity of the personal information, you might need to consult with a range of staff or business groups to complete your data inventory.

You should also assign 'data owners' within the business who are responsible for different datasets and categories of personal information and supported by your privacy function. Ownership should be assigned to a specific role within a business unit or group.

These groups may include:

- IT
- Security, information, and records management
- Risk and assurance
- Legal
- HR

- Finance
- Procurement
- Operations
- Customer or product
- Marketing and Communications

As outlined in our Governance pou, without clear and formalised data owners for various categories of personal information, it's difficult to establish lines of accountability for the maintenance, access, use, and disclosure of that information.

If your organisation already has initiatives in place that give you good oversight of your personal information holdings, then you may decide to build on these rather than create something new. For example, where there is common or overlapping goals with related areas (such as IT, Security, or Information Management) it may be a good opportunity to work with these teams and develop cross-functional networks within your organisation to achieve these.

Retention and disposal

It's important that your organisation has clear policies on how long you will retain different types of personal information you collect, and the lawful purpose for retaining it. You should consider whether your systems have the technical functionality to action your retention and disposal decisions in an automated way. This is a common factor in over retention issues across organisations and should be considered as part of the procurement of any new technical solution. For example, if you have decided you will dispose of incomplete draft application forms received via your website after 30 days, can the system automate the deletion of these?

Once you have undertaken your data inventory exercises, these could also be used as your retention and disposal plan. Take the opportunity to decide:

- How long will you keep each category of information?
    - Make sure you include any minimum retention periods required by law, as well as maximum retention periods required for your legitimate business purposes.
- How will you dispose of each category of information?

You'll need to take note of any other legislation that may dictate how long you can keep certain types of personal information, and whether you're able to dispose of them. You'll also need to ensure that retention periods can be tailored for different circumstances. For example, some call centre phone calls may need a longer retention period than others, and organisations should avoid blanket retention periods.

Don't forget that if personal information is the subject of a Privacy Act request, you must take steps to retain it to respond to the request, even if it would otherwise be deleted or destroyed as part of your routine retention processes.

Your retention and disposal plan can also be used to tag personal information as you collect it so that it can be flagged when it reaches its "use by date". This is a great way of automating your "data privacy hygiene" and reducing the risk to the organisation of holding onto data for too long.

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 that has been operating for a long time, most people could guess what personal information it holds. However, the privacy team is using recent privacy breaches to improve their compliance. They are starting small, trying not to run before they can walk. They have created an inventory and identified business units. They approach the head of each business unit to get their buy in on creating the inventory and how it can ultimately help them.

The privacy team take stakeholders through the inventory, and, through these conversations, they populate the first cut of the inventory. This is then verified by stakeholders and further information provided where needed. When reviewing privacy impact assessments, the privacy team cross references whether the personal information is already in the inventory. Where the purpose is different, they add this information to the inventory. The inventory is also reviewed once a year with business units confirming that the information is still accurate. This helps the privacy team with the privacy statement review.

Small business (charity) – Reach High

Reach High has developed a Personal Information Inventory to document all the different datasets of personal information it holds. The inventory is an excel spreadsheet with tabs for the following business functions:

- Counselling and mentoring
- Fundraising
- Employees

The Director of Support Services manages the inventory and uses it as a “source of truth” to manage privacy breaches, access requests, and to ensure that the various privacy statements Reach High has developed are accurate and up to date. She has also used this as an opportunity to assign data owners for the datasets – she is the data owner for client information, the Director of Fundraising and Outreach is the data owner for fundraising information, and the CEO is the data owner for employee information. Because she is also the Privacy Officer, the Director of Support Services ensures that any data owner decisions about client information are checked with the CEO as well. This process has helped Reach High ensure full accountability and proper escalation of decisions on the use of personal information.

Start-up – Swiftstart NZ

As a SaaS start-up providing a platform for clients to manage customer data, Swiftstaft NZ knows that appropriately documenting the personal information it holds and manages is essential. Not only will it help Swiftstart NZ to manage its own, reasonably limited in scope, employee and client information, but it will enable them to provide transparency and assurance to its clients and their customers.

The Operations Manager works with the Chief Technology Officer, Chief Product Officer and Swiftstart NZ's software developers to ensure there is functionality within the platform so that clients can generate a "Customer Information Inventory". The inventory captures information about types of data fields which have been populated by the client and the ways in which this information is used within the platform (e.g., depending on the specific services the client is using within the platform and the settings which have been selected by the client).

The Operations Manager also conducts a stocktake of the personal information Swiftstart NZ holds about its employees and clients and documents this in a spreadsheet which they manage and review on a 6 monthly basis.

Small business (non-tech) – Green Gardens

Green Gardens has developed a Personal Information inventory to document the different categories of personal information it holds. The inventory is an excel spreadsheet and it's categorised by separate tabs into:

- Employee information
- Client information

The Client information tab documents what information is collected and the point of collection, for example, via the online enquiry form or over the phone. It also documents what information is shared, and how it's shared, with another local business as part of outsourcing Green Gardens' arborist services

The Employee information tab documents what information is collected and the point of collection, for example, via a job application form during the hiring process.

The Administrator for Green Gardens manages the inventory and uses it to ensure that the privacy statements Green Gardens has developed are accurate and up to date. For example, Green Gardens has a privacy statement on its website, which is also linked to its online enquiry form, as well as a privacy statement on its job application forms.

Independent contractor – Jo Jones

Jo Jones has developed a Personal Information Inventory in a spreadsheet to document the personal information she collects and holds. The spreadsheet contains a separate tab for health information, so that Jo can manage this within the rules of the HIPC.

Each new client of Jo's must complete an enrolment form, which is how Jo collects their personal information (including health information). If Jo ever needs to make updates to the enrolment form that involves collecting additional types of personal information, she ensures that this is added to the Personal Information Inventory so that she has an accurate and up to date record of all her personal information holdings.

Government agency – The Ministry

The Ministry holds a large amount of personal and non-personal information, some of it unstructured and some still not digitised. Creating an inventory of all this data poses some practical challenges. The Privacy Team has scoped and planned a project with the Ministry's Information Management team to do a more fulsome data mapping project, but until this can be resourced the Privacy Team has ensured that any new data collections, uses and disclosures are recorded and mapped. They have done this through updating their internal Privacy Impact Assessment template and recording the results from PIAs in a spreadsheet. They are also considering what high-risk data the Ministry might hold and where it is kept so that they can triage and plan for completing the inventory more fulsomely over time.