Transparency

Overview

Transparency is a well-known privacy concept. Being open about how personal information is collected, used and shared is required by the Privacy Act, and is a critical part of building trust in the way your organisation will handle personal information. Your organisation also needs to communicate with individuals in a way they can understand to ensure transparency is meaningful.

This pou provides guidance on:

- Creating privacy statements.
- Ensuring your privacy statements can be trusted.

Who is this for?

Your organisation's privacy function.

Key objectives of the Transparency pou

What would we expect to see?

- The organisation can provide evidence about its privacy practices e.g. policies, processes, risk assessments, and statements.
- Privacy notices and policies are reviewed regularly and kept up to date.
- Privacy notices and statements are accessible and can be understood by their intended audience.

Creating privacy statements

The Privacy Act requires organisations to be open about why they are collecting personal information and what they will do with it.

An organisation must take reasonable steps to make sure people know:

- That their information is being collected (if it's not obvious).
- What information is being collected.
- Why it's being collected.
- What it's being used for.
- Who will receive it.
- Whether they must provide the information and what will happen if they don't.
- That they can access the information held about them, and they can correct it if it's wrong.

These steps should be taken before the information is collected or, if that's not possible, as soon as practicable after the collection.

Privacy statements are a useful tool that your organisation can use to meet these obligations. Other ways may include:

- A verbal explanation.
- Notices on display at entry.
- Enrolment forms.
- Information brochures.

OPC has created a way for organisations to make their own simple privacy statement. You can use our online privacy statement generator, the Priv-o-matic, as a starting point. You can also use our website privacy statement as an example.

Considering your audience

It's important that the people who will be affected by your privacy statement can understand it.

For example, if you are collecting personal information from children and young people, you should provide summaries of your privacy statements that are written in a way they can access, read and understand.

Information privacy principle 4 says that you need to take particular care when collecting information from children and young people. It may not be fair to collect information from children in the same manner as you would from an adult. Ensuring your privacy statements make this distinction, and are easy to understand, can help address any power imbalance. It can also ensure that any authorisation given is meaningful and can be properly relied on.

It is important to make sure that any service providers you use to collect personal information from individuals include your privacy statement and are clear about whether information is being collected on behalf of your organisation only, or will also be used for their own purposes, at the point where personal information is being requested. This is because when you use a service provider you are still responsible for ensuring that the collection obligations are met. Examples of service providers include recruitment software, payroll, and external IT providers.

Considering your context

In some cases where you are collecting personal information, it might not be realistic or practical to immediately or directly provide the individual with a comprehensive privacy statement as described above. For example, when speaking to a customer over the phone, or collecting information in a mobile app.

There may also be cases where it's appropriate to provide an individual with additional or more specific information than is generally included in your full privacy statement. For example, when you are about to collect particularly sensitive or unexpected information, such as biometric, location, or health information.

In cases like these, you should consider the use of a 'just-in-time' style privacy notice. This is a notice which provides more specific, contextual, and timely information at the moment it is relevant or necessary. Just-in-time privacy notices can take various forms, such as a pop-up, banner, notification, dialog box or pre-recorded message. It is not a substitute for a full

privacy statement but rather aims to enhance trust and transparency by improving understanding and control.

A just-in-time privacy notice should follow these design principles:

- Be clear and concise. Use plain language and avoid jargon or legal terms.
- Be relevant and contextual. Focus on the information that is related to the individual's current activity or interest.
- Be timely and visible. Appear at the right moment and in the right place, without interrupting the individual's experience or requiring extra clicks.
- Be actionable and informative. Provide the individual with meaningful choices and options, explain the consequences and benefits of their decisions, and let them know where they can find further information or a full privacy statement.

Ensuring your privacy statements can be trusted

To be trusted, privacy statements need to be complete, accurate, up to date, and known and complied with by your employees. Organisations should develop a framework that ensures their privacy statement is properly integrated into the way they operate and can be truly trusted by their audience. This framework could include the following steps:

1. Consult and engage across your organisation before drafting a privacy statement. Collect the facts you need to make sure that it accurately captures the personal information you are collecting, the ways you are using it, and who you will be sharing it with.
2. Once you have published your privacy statement, make sure your employees know about it and read it. It's your privacy statement that should dictate how you use and share personal information, rather than an internal privacy policy. However, you still need to make sure your internal privacy policy requires employees to use and share personal information in the ways set out in the privacy statement.
3. Use your privacy statement as a starting reference point for when employees consult the privacy team on using or disclosing personal information, to make sure personal information can be used or shared in that way. If the use or sharing is not clearly covered in the privacy statement, your organisation will need to determine what lawful basis it might have to use or share information in a new way.
4. The contents of your privacy statement need to be taken into consideration whenever you undertake a privacy impact assessment for a new project. This can be a good way to check if a proposed project strays a little too far from customer expectations and needs to be reined in. It should also capture any changes that may be required to the privacy statement to reflect the project.
5. Regularly review and update your privacy statements. You should do this annually, as well as whenever you are offering a new service, or using new technology. This will help you to make sure that the privacy statement remains accurate and up to date, reflecting any changes to privacy laws or internal processes and practices that have come up since you last reviewed the privacy statement.
6. Make sure you keep individuals informed of any big changes to your privacy statements. Remember, while you might not be relying on authorisation to use or share personal information in a certain way, your customers might have decided to use your organisation based on what you told them you were going to do with their information. If you want to use personal information for a new purpose that wasn't

anticipated by your previous privacy statement, you may need to seek authorisation from your customers.

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 used the Know your Personal Information pou to understand what personal information it collected, uses, stores and discloses. It has also looked into the different individuals it collects personal information from and has created a small number of privacy statements to cater for the different relationships. Fern Leaf monitors developments from projects and keeps a track of any changes that need making to the privacy statement. It schedules a yearly review date and starts working on the privacy statement a few months in advance.

Small business (charity) – Reach High

Reach High's small size does not change the extent of its transparency obligations under IPP 3 of the Privacy Act. They apply to Reach High in the same way as a large organisation. In fact, Reach High recognises that clear and meaningful privacy transparency is critical to client and stakeholder trust. For this reason, Reach High has put effort into creating a full set of privacy statements, as follows:

- Client privacy statement – which explains what personal and health information Reach High collects to deliver its counselling and mentoring services.
- A summary of its Client Privacy Statement for children and young people - given that many of Reach High's clients are young people, it takes the time to create an even more engaging two-page summary of its Client Privacy Statement, with clear options to contact the Privacy Officer for more information. The summary focuses on the things Reach High believes that young people care about, including who else might have access to their information.
- Fundraising Privacy Statement – which explains what personal information Reach High collects about potential and actual donors.
- Employee Privacy Statement – which explains what personal information Reach High collects about its employees. This is important, because Reach High is required by law to complete several vetting checks on its counsellors and mentors, so it wants to explain this clearly to its employees.

Start-up – Swiftstart NZ

As a small, new business, Swiftstart NZ didn't have much in place in the way of privacy statements when it hired its first employees and on-boarded its first clients, but it understands this is something that it will need to get better at as the business expands.

The Operations Manager decides that they will use a recruitment company for any new employees it recruits and works with the company to create an 'Applicant Privacy Statement'

which will be available with any future job listings. They also create an 'Employee Privacy Statement' that is approved by Swiftstart NZ's founders.

Swiftstart NZ knows it isn't directly responsible for notifying its clients' customers how their personal information is managed within Swiftstart's platform. However, to make it as easy as possible for their clients, Swiftstart work with an external legal adviser to help draft template wording that their clients use. At the same time, they ask the lawyer to review their standard client services agreement to make it crystal clear that the client will be responsible for providing any required notices to their customers.

Small business (non-tech) – Green Gardens

Regardless of Green Gardens' small size, their transparency obligations under the Privacy Act apply in the same way as a larger organisation. Client trust is important to Green Gardens, so they have developed the following privacy statements:

- Client privacy statement – this explains what personal information Green Gardens collects to deliver its gardening services, and lets clients know that they may share the information with another business as part of outsourcing their arborist services.
- Employee privacy statement – this explains what personal information Green Gardens collects about its employees.

Independent contractor – Jo Jones

Jo Jones has transparency obligations under the Privacy Act, which apply in the same way they would to organisations large or small. Client trust is at the heart of Jo's services, and she has developed a client privacy statement which explains what personal information she collects to provide her services, and the purposes for which she collects and uses it. The client privacy statement is on the enrolment form that each new client completes. Generally, new clients will complete the enrolment form at their first visit or consultation with Jo – this gives her an opportunity to talk through the privacy statement with them to ensure they understand.

Government agency – The Ministry

While the Ministry has not completed a full retrospective review of all its personal information holdings, it knows what is currently collecting and what it can be used for, both under the empowering legislation and the Privacy Act. As a public sector agency, the Ministry also recognises that it has obligations to communicate with people in a variety of different ways to meet their audience needs – so it has privacy statements available in writing in different languages, audio recordings, and a video in NZSL. It has different privacy information available depending on the way that the person is interacting with the Ministry – for example, the call centre phoneline clearly says that calls are recorded and what will happen with the information provided over the phone, and application forms also include privacy information as well as links to the Ministry's overarching privacy statement. All the privacy material includes details on how individuals can access and correct their own information and make a privacy complaint, including a specific email address for privacy complaints.