Privacy Commissioner
Te Mana Mātāpono Matatapu

Working with third-party providers: understanding your privacy responsibilities

November 2024

Do you currently share, or are you considering sharing your information with a third-party provider?

No → End here.

Yes ↓

Check:

- What personal information are you sharing?
- Why are you sharing it?
- Can you be confident that the information will be protected?

Will the third-party use or share your information for their own purposes?

No → The third-party is holding personal information solely on your behalf.

You are responsible for what the third-party does with your information.

Check their terms of service or make sure your agreement covers: security, access, notifiable breach, retention, and use of information.

Yes ↓

The third-party is not holding the information solely on your behalf

Both you and the third-party will have responsibilities regarding your information.

Check their terms of service/agreement.

Consider who notifies about privacy breaches, security arrangements, access, use.

Third-party providers: understanding your privacy responsibilities

Your responsibility for the personal information stored or processed by a third-party provider comes from Section 11 of the Privacy Act.

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. Read more about what we mean by personal information.

Who is this for?

This guidance is for organisations who are thinking about using a third-party provider, or those who already do.

If you use a third-party provider to store or process personal information on your behalf, you are still responsible for what happens to that information.

This guidance explains what you must think about when you are choosing a third-party provider and what your ongoing responsibilities are.

We have a wider suite of guidance 'Poupou Matatapu' to find out more about how to 'do privacy well' and what good privacy practice looks like.

Your organisation is responsible for your personal information when stored or processed by a third-party provider

The key thing to remember is that you remain responsible for personal information that you send to a third-party provider.

What do we mean by third-party provider?

'Third-party' means an organisation external to your organisation. 'Third-party provider,' also known as a 'third-party' or 'service provider,' is a broad term that can be applied to a range of external organisations that provide services to your organisation, such as storing or processing information on your organisation's behalf. Software as a Service (SaaS) or cloud service providers are a classic example.

However, there is a wide range of other third-party providers you might contract with who may need to store or process personal information provided by your organisation to deliver their service to you.
For example, you might:

- Share employee pay information with an external payroll provider or accountant.
- Contract a company to collect information for a survey.
- Use another organisation to provide personalised services for your customers.
- Use an intermediary platform that shares the information with other third parties.

Before using a third-party provider

Before you engage a third-party provider, you need to understand:

- What types of personal information you'll share with them, or they'll collect on your behalf.
- What they will do with it.

Do they need personal information?

First, understand whether your organisation needs to provide personal information to the third-party provider at all. You should consider if you can achieve the results you want from a third-party provider without providing any personal information.

For example, your organisation might like to use a third-party marketing agency to provide advertising services. Marketing agencies can offer a range of services, from sourcing advertising on billboards or online advertising (which would not require any personal information), to using the information collected from an organisation's existing customer database to create marketing strategies (which might require personal information, depending on the task). Think about whether supplying aggregated, non-personal information might enable the marketing agency to perform the service adequately.

Please note: when changing the way you use clients' or staff's personal information, you need to assess the privacy risk and make sure you're being transparent through your privacy statement to reflect any changes in use of personal information. We have guidance on how to improve your privacy transparency. We also have a PIA toolkit available to help assess the privacy risks.

What kind of personal information is it?

It's important to understand the level of privacy risk that you'll need to manage with your third-party provider. We have guidance on different kinds of personal information that may carry higher privacy risk, such as where the information is sensitive or confidential.

For example, an organisation might employ the use of a third-party software provider to manage their payroll. Information required to process payroll can be sensitive, such as bank account and IRD numbers. Appropriate security measures need to be in place. We have guidance on handling sensitive information.

Due diligence

You will need to be confident that the information is protected wherever it is, and whatever organisation is handling it. Ask questions that enable you to have that confidence (this is normally referred to as 'due diligence'), and ask those questions early, before you commit to using the provider. Any subsequent contract with that provider should satisfactorily reflect the key protections that you expect to be in place. It should also require the third-party to ensure that any subcontractors or support agencies will equally protect the information. Your organisation needs to know whether the third-party provider will use or disclose the personal information that you provide for its own business purposes.

What will the third-party provider do with the information?

There are a range of services that third-party providers offer. Some third-party providers will merely store the information and some will process the information for you (for example, a service providing data analytics). Some may themselves use third-party services such as generative AI tools to store or process the information. A key thing to understand is whether the third-party provider will use the information for their own purposes or not. Some examples of third parties using information for their own purposes could be when your information is used as AI training data or using the information you provide for services to other organisations.

If the third-party provider is storing or processing the information solely on your behalf (for example storing information as a cloud service) and will not use or disclose it for its own purposes, section 11 of the Privacy Act says that the third-party provider is not deemed to "hold" the personal information for the purposes of the Privacy Act. This also means that you are not "disclosing" the information to them, which means you do not need to worry about the Privacy Act's disclosure principle (IPP 11). But as a result, your organisation remains fully responsible under the Privacy Act for what happens to that information. The third-party is "you" for the purposes of the Privacy Act.

If the third-party provider will use or disclose the information for its own purposes, as well as performing services for you, then both the third-party provider and your organisation will be deemed to "hold" that information for the purposes of the Privacy Act. That means you will both be responsible for the information in various ways depending on how it is being stored or used. Sharing personal information with that third-party provider could also be a "disclosure" and you will need to make sure that sharing the information is allowed under IPP11. IPP12 may also be relevant if the third-party provider is not based in New Zealand.

In addition, both your organisation and the third-party provider may be accountable if there is a privacy breach. This means that your organisation and the third-party provider need to have a plan to outline who will notify OPC and individuals affected in case there is a breach. We have guidance on who should notify OPC and affected individuals.

Example of a section 11 situation: Wonder Bottling Ltd uses third-party Big Data Analytics

Wonder Bottling Ltd wants to use the third-party Big Data Analytics Ltd to run Wonder Bottling's website. Big Data Analytics will store all website data, including personal information provided by customers to Wonder Bottling via web forms. It will also process the information stored and provided to the website to provide website analytics to Wonder Bottling Ltd.

Big Data Analytics is not using Wonder Bottling Ltd's information for another purpose or service, such as using Wonder Bottling Ltd's data insights to provide a service to another organisation. It is solely storing and processing information for Wonder Bottling Ltd. Under section 11, this means that Wonder Bottling Ltd is responsible for anything that happens to that information while it is being stored or processed by Big Data Analytics.

For instance, if Big Data Analytics is the subject of a notifiable privacy breach in relation to the personal information transmitted by Wonder Bottling, Wonder Bottling would be responsible for notifying the Office of the Privacy Commissioner (OPC) and affected individuals. In their agreement, Big Data Analytics should be required to inform Wonder Bottling about any breaches of that information so that Wonder Bottling can fulfil this requirement.

However, if Big Data Analytics were to change how it operates and start using that information for another purpose, Big Data Analytics would have its own obligations under the Privacy Act, such as responsibilities to make sure the information is accurate and fit for purpose under IPP8, and to use the information in line with IPP10.

Protecting personal information once you've chosen a third-party provider

Since your organisation is legally responsible for anything that happens to the personal information that a third-party provider stores or processes for you (whether or not that third-party is also responsible), you should make sure that you have a robust agreement in place with them that requires them to keep the information safe and gives you a remedy when things go wrong.

What should be in an agreement with a third-party provider?

Security measures

An organisation needs to do everything within its power to prevent unauthorised use or disclosure of personal information. This means that your organisation needs to get assurances that the third-party provider has the appropriate security measures in place to protect any information it stores or processes on your behalf. The more sensitive the information is, the stronger those assurances may need to be. Our guidance on security and access controls provides examples of the types of security measures the third-party provider should take to protect the personal information it stores. Your organisation may wish to seek regular reporting from the third-party provider on the effectiveness of the measures.

Individuals' right to access and correct the information your organisation holds about them

The Privacy Act requires you to give people access to their personal information if they ask you to, and correct that information if it is wrong. There are also strict statutory timeframes for responding to requests. Those timeframes don't change when the information is stored by a third-party rather than by you. You need to ensure that your agreement with the third-party provider includes provisions that make sure you can locate and retrieve information quickly, so you can meet your obligations. Read our guidance on access and correction of personal information.

Reporting notifiable privacy breaches

The reporting of notifiable privacy breaches also needs to be factored into your agreement with a third-party provider, including how it will notify you of any breaches it has, and whether it will notify you of all breaches or only ones that it considers are notifiable. We strongly recommend that the contract requires the third-party provider to notify you of all breaches that affect the personal information it is storing or processing on your behalf, so that you can then decide what to do.

Your organisation will be responsible under the Privacy Act for reporting notifiable privacy breaches to the Office of the Privacy Commissioner so you need to be satisfied that the third-party provider will promptly notify you of breaches. The Office of the Privacy Commissioner generally expects to be told about notifiable breaches within 72 hours of the breach becoming known. That period starts when the third-party provider knows about the breach, not when they tell you, so it is important to make sure that you are told as soon as possible. Poupou Matatapu has more information on notifiable privacy breaches, including the obligation to notify affected individuals.

Third-party compliance with the Privacy Act

Your agreement should make sure there are contractual obligations on the third-party provider to comply with all applicable privacy laws.

Disposal of personal information during and after the agreement

Organisations must not keep personal information for longer than they need. It's important that your agreement outlines how long the third-party provider will store the personal information on your behalf. In short, the third-party provider should only retain the information for as long as you want it to and are permitted to yourself. Ideally, you should be able to delete the information yourself as retention periods are reached or your circumstances change. The agreement should also outline what will happen to the information at the end of the agreement. Will it be transferred back to you? How will it be disposed of? Can the third-party provider give you assurances that the information has been permanently deleted (including from backups)? Poupou Matatapu has more guidance on retention and disposal in the Know your Personal Information Pou.

Assurance that the third-party provider will only use the personal information for delivering the services

Your agreement should include an assurance that the third-party provider will only use the personal information it stores or processes on your behalf to deliver the services you have requested, as outlined in the agreement. Remember, that if the third-party provider will be using or disclosing the information for its own purposes, the third-party will have its own obligations under the Privacy Act.

Checklist for what should be in your agreement with a third-party service provider:

- ☐ Appropriate security measures.
- ☐ Facilitation of access and correction requests.
- ☐ Process and time frame for notifying you of privacy breaches, especially notifiable breaches.
- ☐ Compliance with relevant privacy laws.
- ☐ The third-party's use of the information you provide.

Other things to consider

- If you're sending personal information to a third-party provider to process, store, or use on your behalf, you need to make sure you are transferring the information securely. Poupou Matatapu has information on security and internal access controls.

- Use a Privacy Impact Assessment to assess and record the privacy risks associated with using a particular third-party provider. We have a PIA toolkit available to help.
- If you're using a third-party provider based in another country, consider your practical ability to control your personal information and ensure it is being handled in line with the New Zealand Privacy Act.
- Consult with stakeholders or affected communities if the personal information is particularly sensitive, or where there are Māori data sovereignty implications.