


Debunking common privacy myths

Debunking common privacy myths



ALLEN + CLARKE



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

In a world of increasing surveillance and monitoring, it can become difficult to know whether your organisational and individual privacy is being protected.

This guide will separate the myth from fact when it comes to levelling up your workplace privacy.



Demystifying the Privacy Act

What is the Privacy Act 2020, and how is it different to the previous legislation?

The Privacy Act 2020 is a critical piece of legislation that safeguards the protection of personal information and recognises the importance of privacy as a taonga.

The 2020 Act replaced the previous Privacy Act 1993. The main changes are:

- Notifiable privacy breaches.
- Compliance notices.
- The Office of the Privacy Commissioner (OPC) can issue binding decisions on access requests.
- Organisations need to ensure protections apply before sending information overseas.
- Extraterritorial effect.
- There are new criminal offences to mislead a business or organisation by impersonating someone in order to access their information or have it destroyed; or to destroy a document containing personal information knowing that a request has been made for it.

What is personal data under New Zealand's privacy laws?

Personal data 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. This information doesn't need to name the individual for it to be identifiable; for example, information can be identifiable if it contains a person's home address, or another identifier which could allow their identity to be pieced together.

Who does the Act apply to?

New Zealand's privacy laws are applicable to all 'agencies', which includes virtually every type of organisation – including private businesses, government entities, charities, and more.

The term 'agency' is used in the Privacy Act to mean a person, business, or organisation that collects and holds personal information about other people. Technically, this term also applies to individuals, though an individual acting in their personal or domestic capacity is not considered an 'agency.'

This means that even a business owned by only one person is subject to the Privacy Act for the information held by the business, even if the business is not yet a registered company.

What are the principles of privacy, and why are they important?

The Privacy Act governs how organisations and businesses can collect, store, use, and share personal information.

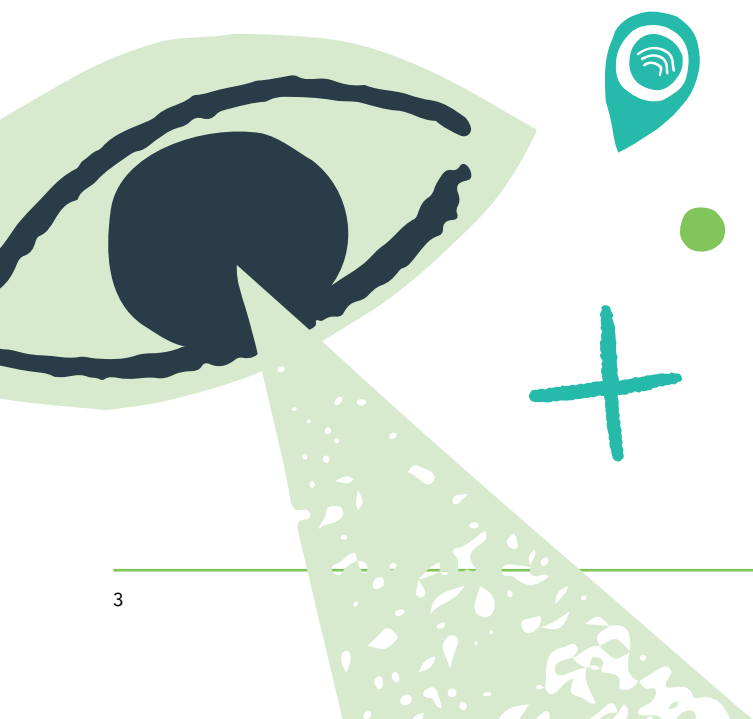
The information privacy principles, enshrined in the Act, ensure that, for individuals:

- They know when their information is being collected.
- Their information is shared and used appropriately.
- Their information is kept safe and secure.
- They have access to their information.

The information privacy principles govern the 'life cycle' of personal information – for organisations, this means making sure that there is a good reason for collecting information before you collect it, then telling people about what you're going to do with it. Once you've got it, you have to keep it secure, and know you have to give it to people if they ask for it or correct it. You shouldn't be keeping it forever – some recent high-profile privacy breaches have been the result of information being kept for longer than needed.

Only use information and disclose it for the reason it was collected, unless another exception applies (e.g., the individual consents to you sharing it or using it for another purpose).

The information privacy principles are important because they are the framework that ensures that personal information is protected and respected – and that individuals affected by organisations who hold their personal information can access that information and hold organisations to account when things go wrong.



How can you protect digital information in your business/organisation?

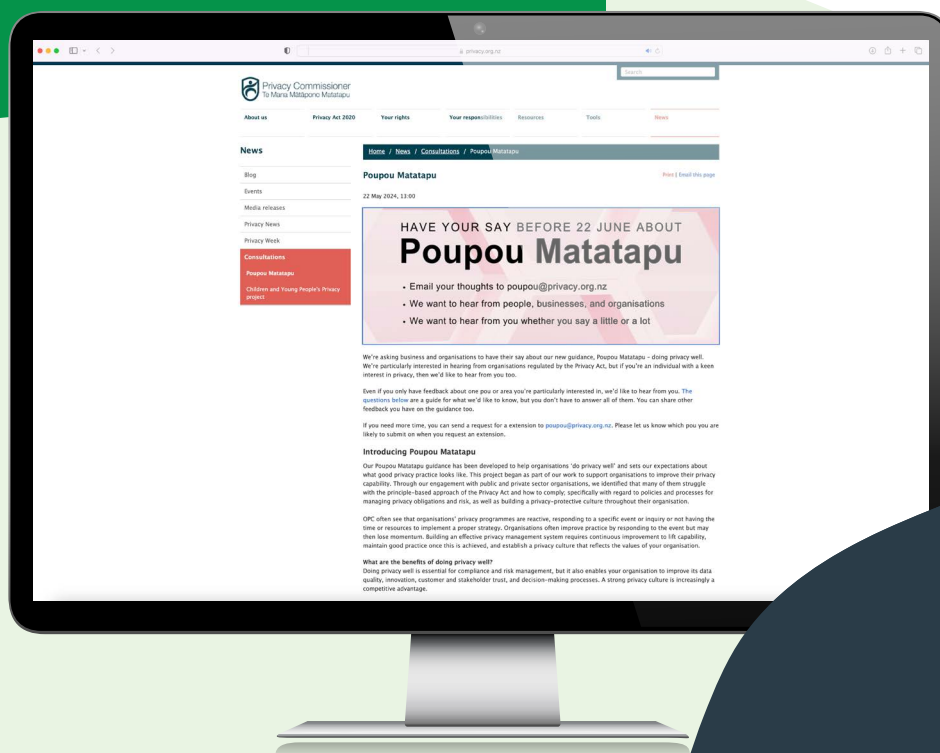
Security of information and IT infrastructure is a critical component of a robust privacy programme.

Cyberattacks are on the rise and being able to respond appropriately is a key responsibility for organisations. Organisations must take reasonable steps to make sure the information they hold is kept safe and secure. The most effective strategy to do so is to have a well-developed security plan for all personal information your organisation holds.

The Office of the Privacy Commissioner recently released their draft guidance [“Poupou Matatapu – Doing Privacy Well”](#), which describes key security controls across three areas – physical, technical, and organisational.



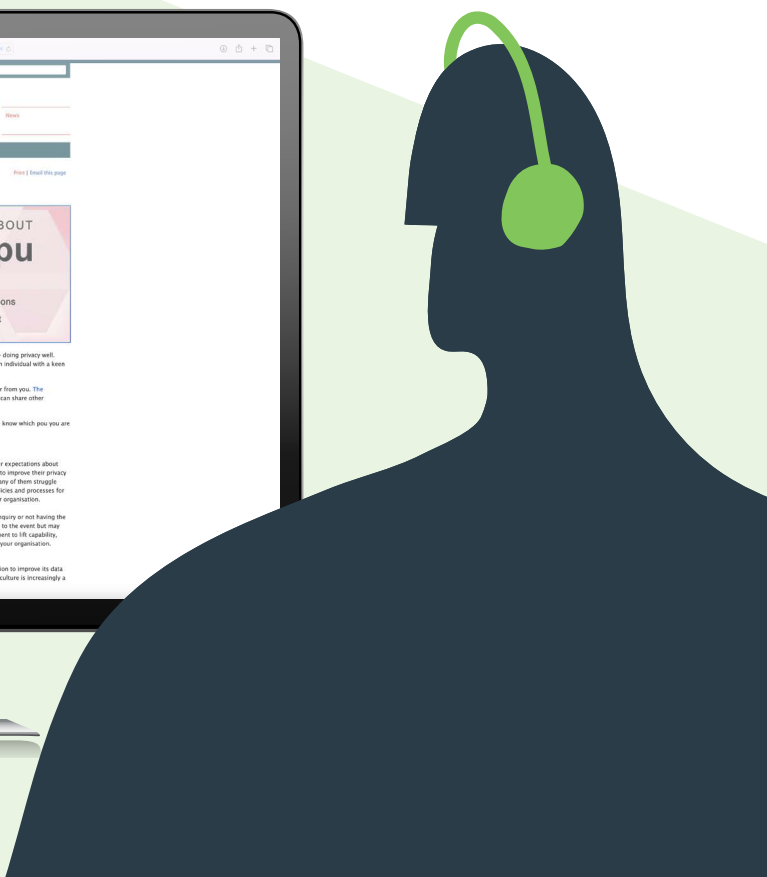
View Poupou Matatapu here



How can we ensure we're protecting people's data whilst also gaining the benefits of using AI tools?

Thinking about privacy is vital if you're going to use AI tools well. The Privacy Act applies whenever you collect, use, or share personal information, and this includes when you're using AI tools. The uptake of AI tools presents some specific challenges for privacy. Privacy protections rely on people and organisations who can understand context and take responsibility for their actions. This may become harder as AI tools take on more tasks, because they enable new ways to gather and combine personal information, and because they can make it harder to see, understand, and explain how personal information is used.

The best time to do this privacy work is as soon as possible, especially for AI tools and other emerging technologies. Take proactive steps early on, including doing a privacy impact assessment (PIA) before you start, to check you're upholding your Privacy Act obligations. OPC has published guidance on [AI and the Privacy Act](#).



Common privacy myths

Myth #1: Privacy makes it harder to get stuff done.

Privacy is an enabler. Those who see privacy as a barrier often do so as they view privacy as a compliance cost. However, privacy is a critical part of building trust and confidence in the community you serve and in your client base.

Myth #2: Privacy stops businesses from using cloud services.

This is not true – if you are sending information to a cloud service provider, and they aren't using the personal information you're sending for their own purposes, it's not even technically a 'disclosure' for the purposes of the Privacy Act. The main thing is doing due diligence on any third-party service provider before you start sending data to them – know what they will do with your data, how they'll keep it safe, how you'll each respond to privacy breaches, and what remedies you have if something goes wrong.

Myth #3: Privacy stops government information flow.

While the Privacy Act does apply to government agencies, a lot of information-sharing happens across government. There are particular information-sharing arrangements within the Act that anticipate sharing across agencies, such as the Approved Information Sharing Agreements. There are also built-in exceptions to the Privacy Act that anticipate sharing information across agencies for research purposes.

While there are exceptions in the Act that allow for the use and disclosure of personal information for the maintenance of the law (prevention, detection, investigation and prosecution of offences), the Act still applies to law enforcement.

OPC has guidance available on their website for agencies who might need to disclose information to law enforcement on understanding how to do so safely and appropriately.

Myth #4: Privacy officers need to have formal training.

Under the Privacy Act, every agency is required to have a privacy officer.

No special training or qualification is required to be a privacy officer, but the privacy officer does need to understand the principles of the Privacy Act, as they are responsible for ensuring their agency complies with the Act. They also deal with requests made to the agency for access to, or correction of, personal information, and they are responsible for working with the Privacy Commissioner during the investigation of complaints.

Myth #5: You must always get a person's consent before dealing with their personal information.

The Privacy Act is purpose driven. This means that if you have a legitimate business purpose for collecting personal information, and you are clear about that purpose and transparent with the affected people, you don't need consent. Where an organisation decides that it wants to use this information for a new purpose that wasn't the original reason for its collection, then authorisation is one option which can apply. However, it is not a prerequisite.

Myth #6: The privacy principles do not apply to information my agency stores overseas.

The 2020 Act expressly brought in extraterritoriality. This means that if your agency wants to share information overseas, you will first need to check if the overseas organisation is going to use this information for their own purposes.

If not, you don't need to comply with Principle 12 of the Act, which concerns disclosure of information to organisations outside of New Zealand. However, you should consider contractual protections in case something goes wrong.

Myth #7: Workers do not need to worry about privacy when sending messages to one another about their clients, customers, or colleagues.

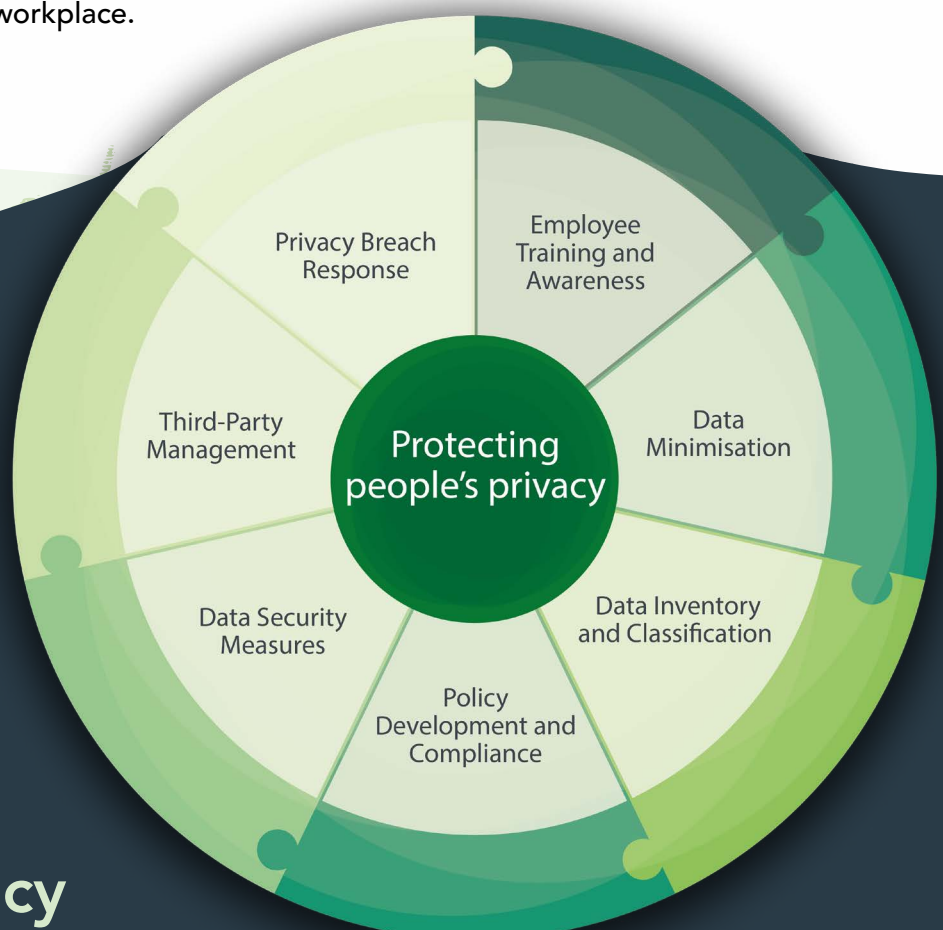
People messaging at work need to think about both what forum they're using to message (e.g., whether it is software or a method that is approved by work), and to remember that this is still personal information that is held by the workplace.

Depending on your work's policy, they can probably read the messages. Messages could be requested under the OIA if you work for an organisation that is subject to the OIA or the LGOIMA. Messages could also be requested by an individual. Embarrassment of the author is not a reason not to disclose personal information if it has been requested.

Myth #8: If I admit to a breach, I will be fined or punished, so it is not worth telling OPC.

Organisations that have notifiable privacy breaches must tell OPC – it is an offence not to. However, you won't be fined for telling OPC about a breach. One of the reasons for telling OPC about a breach, and telling them early, is that they can provide advice about how to respond. For agencies that don't comply with their privacy obligations, OPC have a Compliance and Regulatory Action Framework which sets out their compliance and enforcement approach.

Practical tips for protecting people's privacy



A+C's 7-step blueprint to protecting people's privacy

1

Employee Training and Awareness

- **Regular training:** Conduct regular training sessions on data protection and privacy best practices.
- **Incident response training:** Ensure employees know how to respond to data breaches and security incidents.

2

Data Minimisation

- **Collect only necessary data:** Ensure that only the data necessary for the specified purpose is collected.
- **Limit access:** Restrict access to data to only those employees who need it to perform their job functions.
- **Dispose of unneeded personal data:** Have a clear policy for what classification of data is to be disposed of, and by when.

3

Data Inventory and Classification

- **Identify and classify data:** Determine what types of data are collected and classify them based on sensitivity (e.g., personal, sensitive, financial).
- **Mapping data flows:** Understand and document how data flows within and outside your organisation.

4

Policy Development and Compliance

- **Have a privacy officer:** Appoint a privacy officer who assists you team with questions and assessments. Make their role clear to all team members.
- **Develop privacy policies:** Create clear privacy policies that comply with the Privacy Act 2020.
- **Compliance audits:** Conduct regular audits to ensure compliance with privacy policies and legislation.

5

Data Security Measures

- **Encryption:** Use encryption to protect data both at rest and in transit.
- **Regular updates and patching:** Keep systems and software up to date to protect against vulnerabilities.
- **Access controls:** Implement strong access controls, including multi-factor authentication.

6

Third-Party Management

- **Vendor assessments:** Conduct due diligence and regular assessments of third-party vendors who handle customer data.
- **Contractual obligations:** Include data protection clauses in contracts with third parties, noting your organisation remains responsible for your customers data, even if it stored or managed by a third party.

7

Privacy Breach Response

- **Incident response plan:** Develop and maintain a privacy breach response plan.
- **Notification procedures:** Have clear procedures for notifying affected individuals and authorities, including The Office of the Privacy Commissioner, in the event of a breach.

Common Questions



Who owns your personal identification details when you give it to another party for legitimate use in NZ?

The idea of 'ownership' of your personal information is somewhat of a red herring for the purposes of the Privacy Act. If you give your personal information to an organisation that is subject to the Privacy Act, they must use it in the way that matches what they told you when they collected it. If they don't do that, they need to rely on another lawful basis to use it or share it, or they could be breaching the Act.

What are the interactions between the OIA and the Privacy Act?

If an individual asks for their own information, the Privacy Act will apply, regardless of whether that information is held by a public or private sector organisation.

If someone asks a public sector organisation for information that is solely about another individual that not the requestor, a company, or other types of information – such as business information or copies of policies – then the OIA will apply, or the LGOIMA for local government bodies.

Any privacy issues need to be considered under the provisions of those Acts that allow information to be withheld on privacy grounds. Privacy is a good reason for declining an OIA request unless there's strong enough public interest to outweigh the privacy concerns. If someone asks for information that is both about themselves and about another person, the Privacy Act will apply.

When/how might I be permitted to provide parents access to children's health documentation?

If your child is under 16, you are entitled to request their health information in the same way you are entitled to request your own health information. But your right to the information is not absolute.

The agency may withhold your child's health information if:

- The agency has reasonable grounds to believe your child does not want their information to be given to you;
- The agency believes it would be contrary to your child's best interests for you to have the information; or
- Any of the other refusal grounds in sections 49 – 53 of the Privacy Act 2020 apply.



How do I get management to take privacy seriously?

Governance members need to have a clear understanding and effective oversight of their organisation's privacy risk and deliberately make privacy a priority.

It might be that governance/management need to get more reporting about the privacy risks that your organisation holds, or understand the value of the information you hold and the potential costs if something goes wrong.

In a recent survey conducted by OPC, 70% of respondents said they would likely change service providers if they heard theirs had poor privacy and security practices. A recent Talbot Mills Research survey focussing on cybersecurity found 71% said they would consider no longer dealing with a company if it lost their data in a cyberattack.

If your staff, customers, and clients have trust and confidence in you as an organisation, and in how you go about your business, then that creates 'permission space' for you to take opportunities and try new ways of doing things.

Losing that trust and confidence through privacy breaches will undermine efforts to be innovative and to improve productivity.

Data is such a quintessential element many workplaces that management and consideration of privacy concerns need to be as important as health and safety protocols or robust financial reporting.

How might you track the use of personal information throughout your organisation?

Completing a data map and data inventory for your organisation will give you a comprehensive view of the personal information you are responsible for.

It should include, among other things:

- 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.

You will need to identify all the places in which personal information is stored. As a starting point, you could develop a high-level view of data holdings, and then a plan to complete a more detailed map of higher-risk data. The main goal is to identify areas where privacy risks or opportunities may arise.