What New Zealand small businesses can learn about privacy

Insights Report May 2023

Privacy Commissioner
Te Mana Mātāpono Matatapu

www.privacy.org.nz

Introduction

Building privacy into your organisation builds trust with clients, patients or customers, and therefore opportunities to grow your business. Privacy breaches, whether caused through a malicious act, human error, or system malfunction, work to erode that trust.

At the end of 2022, the Office of the Privacy Commissioner (OPC) and business.govt.nz ran a Small Business Privacy Awareness Survey and 386 small businesses responded. We also reviewed 1487 breach reports to the Office to draw insights about small businesses and privacy.

While businesses showed they understood personal information and privacy issues they didn't always have relevant privacy policies and procedures in place. Here we've identified four insights, supported by case studies, to help small businesses better meet their obligations under the Privacy Act 2020.

Our key messages:

- Understanding privacy does not necessarily translate into good privacy practices.
- Your business sector can increase your privacy risk.
- Businesses need systems for giving people their own information, promptly.
- Whether your business is big or small, the privacy breach risk is about the same.

About the data

For the purposes of this report, small businesses have been defined as those that have 1-49 employees; 50+ employees is considered a large business.

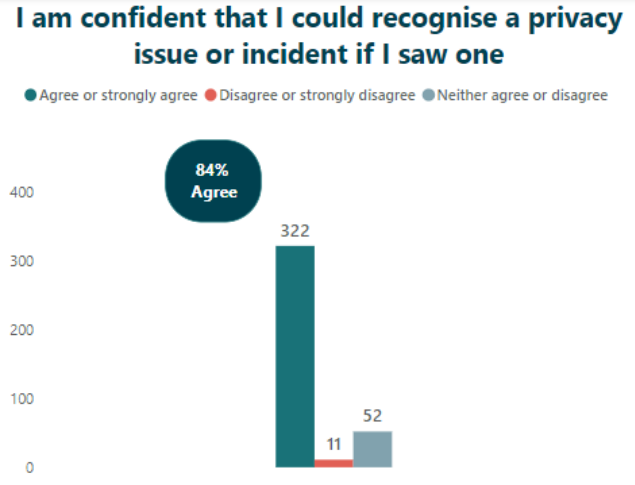
OPC internal data is based on the reporting period from 1 Dec 2020 to 30 Apr 2023. During this period, OPC received a total of 1487 privacy breaches, where organisation size information was available. Out of these, 906 privacy breaches were reported by NZ businesses (491 small business and 415 large business breaches). 323 of these reported breaches met the threshold for serious harm.

As for complaints, OPC received a total of 824 complaints where organisation size information was available. 328 of these were complaints against NZ businesses (179 against small businesses and 150 against large businesses).

Insight 1

Understanding privacy does not necessarily translate into good privacy practices

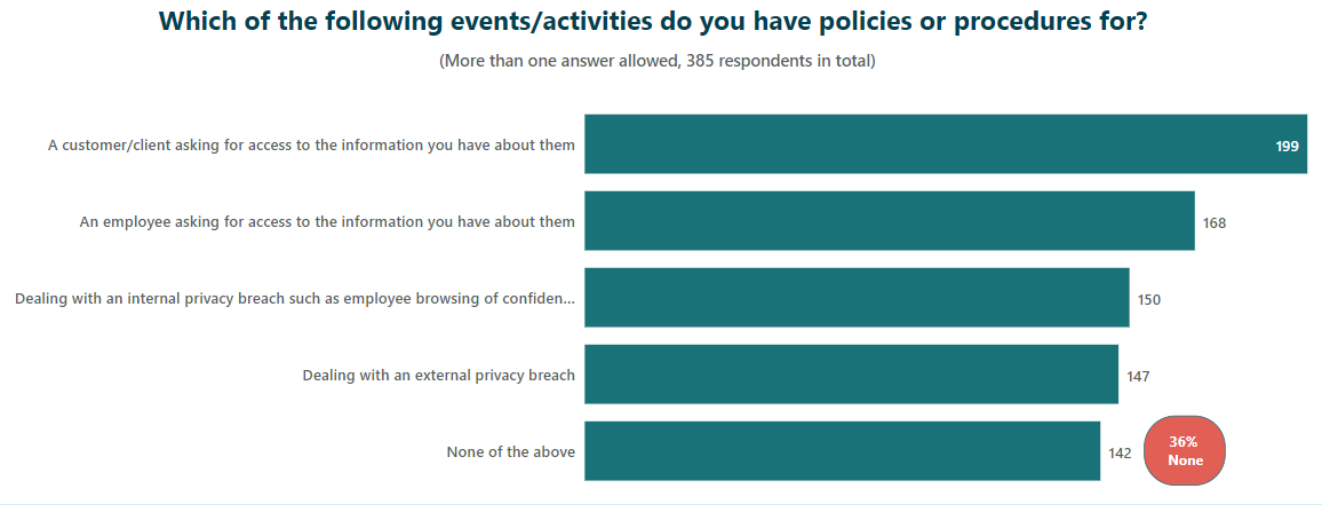
Our Small Business Privacy Awareness Survey revealed relatively high levels of confidence among respondents about identifying what personal information is, as well as identifying a privacy issue if they saw one.



99% of respondents confidently identified at least one form of personal information and 84% agreed that they are confident in identifying a privacy issue if they see one.

However, when looking below the surface, it became clear that good privacy policies and practices are not always in place. We found that 36% of businesses didn't have policies or procedures for a range of key events/activities.

It is important for all businesses, big or small, to understand their obligations under the Privacy Act. For example, it is mandatory to report privacy breaches that meet the threshold for serious harm to our office within 72 hours of identifying the breach. Once a breach has been brought to our attention, OPC is able to assist, if necessary.



Case note: Sometimes it pays to think big picture

The privacy principles in play are:

- **Principle 11 – disclosure of personal information**
- **Potential breach of Principle 5 – storage and security of information**

Inspired by fads and fashions from the US and Europe, a cleaning company posted before and after photos of their cleaning jobs to their social media channels.

However, some of the jobs they were hired for were cleaning crime or accident scenes including places where deaths, assaults, and other activities had occurred. They photographed these jobs too without making sure that personal or private information was removed prior to photos being posted.

One of the photos they shared was taken at the home of a deceased person and included a family photo sitting on a mantelpiece in the rear of the image. The family members were identifiable in the image. Under New Zealand Privacy law, deceased people don't have the same privacy rights as those who are alive. However, this image included a photo that potentially breached the privacy of those alive, at an extremely vulnerable time in their lives.

The people who were identifiable in the photo contacted OPC in 2020 and found that while many of the photos used, while inappropriate, didn't breach people's privacy, the ones that included people's faces did, where those people were alive and identifiable.

During the investigation OPC also learnt that the photos being taken were stored on private phones rather than company phones. Once these findings were discussed with the company, steps were taken to fix the problems including removing all the photos from social media and the company invested in an app that can be used on personal phones to take and store images that aren't accessible to anyone except for authorised people.

Learn and do:
Think about the bigger picture of your businesses actions. Are you unwittingly oversharing personal information? How are you storing content to keep it safe and private?

Insight 2

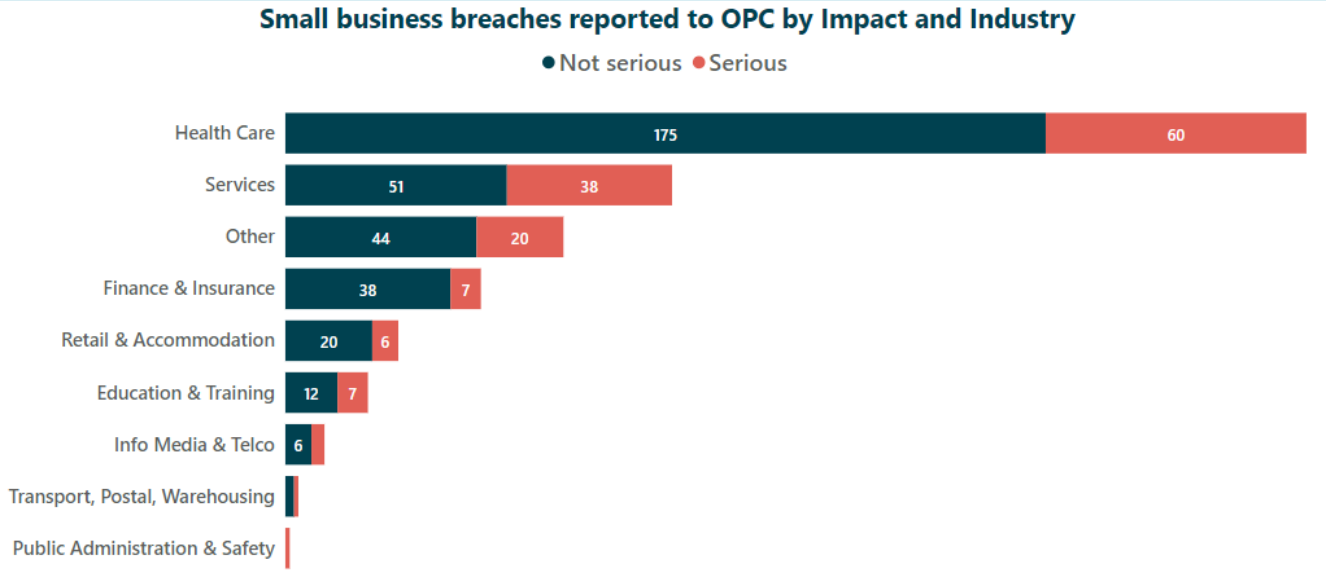
Your business sector can increase your privacy risk

Some businesses have greater risk of privacy breaches. For example, a medical clinic with two doctors, a nurse, and a receptionist is far more susceptible to a serious privacy breach than a retail store with 30 staff selling video games and movies because of the information they hold.

Small businesses in health care, public administration and safety, and education and training are OPC's top reporters of privacy breaches. This might be due to the lack of resourcing or training, the absence of dedicated privacy officers or internal privacy practices not being followed, or more generally a lack of privacy maturity being accidentally or intentionally exploited.

In previous OPC surveys we've learnt that six out of ten New Zealanders would be likely to change service providers if they heard their current provider had poor privacy practices. This should be motivation for businesses to ensure privacy is as important in their business as health and safety. Businesses, regardless of size or sector, need to work to the highest standards with the information that's entrusted to them.

Businesses can make a start by ensuring their privacy statements are as clear and concise as possible. **OPC's free, award-winning privacy statement generator** is a good starting point for ensuring your clients' personal information is protected from harm but isn't a 'one and done' exercise – you need to give due consideration to your privacy policies and processes too.



Case note: You can tell the story without telling the whole story

The privacy principles in play are:

- **Principle 11 – disclosure of personal information**

The Health and Disability Commissioner referred a medical practice to OPC in 2022. The incident began with the misunderstanding of a medical procedure.

After the procedure was completed, the patient notified the practitioner that they were intending to lodge a complaint with the governing medical board.

Once the patient had left the clinic, the medical practitioner contacted a retired member of their medical field. This retiree happened to be the current neighbour of the affected patient. In this conversation, the identity of the patient was discussed, and once this conversation concluded, the retiree contacted the patient to discuss the complaint.

The patient felt their privacy had been breached and asked the medical practice to apologise. They received no reply.

After an investigation was conducted, the medical practice issued an apology to the patient and provided further training for staff using tools on the OPC's website.

Small and large businesses can use this as an example to show that even well-intentioned actions can breach people's privacy if the proper precautions are not taken. There was no problem with the affected medical practice contacting a professional within their field for advice, but the name and any identifying details of the patient were not necessary in that discussion.

Learn and do:
Think about how much of the story you need to tell. There was no issue with the practice seeking further advice, but they could have done that without identifying who they were talking about. If a person seeks an apology from your business, deliver it quickly.

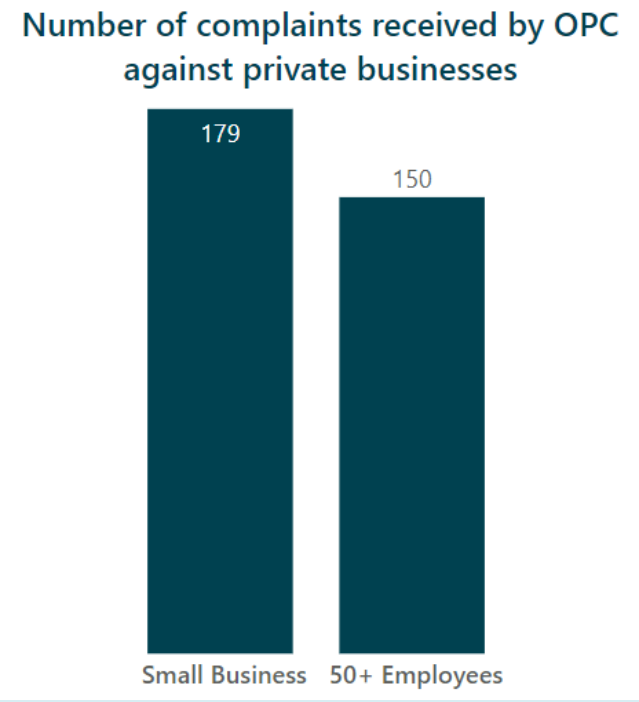
Insight 3

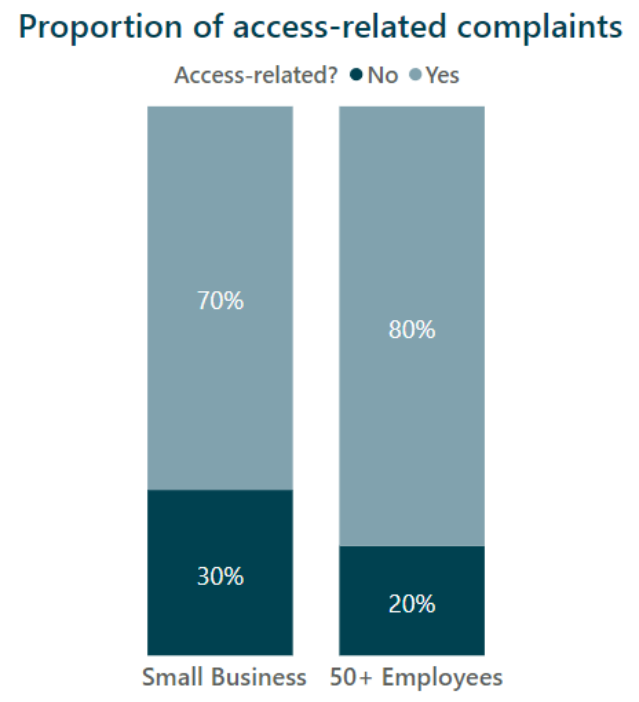
Businesses need systems for giving people their own information, promptly

What people complain most to OPC about is not getting their own information from businesses that hold it. Nearly two thirds of all complaints OPC receives against small businesses are related to privacy principle 6 – Access. Either people can't access their information, it's missing detail, it took too long to get, or businesses refused to share.

Principle 6 of the Privacy Act 2020 says that people have a right to ask for access to the information a business or organisation holds about them. They can only ask for their own information and businesses need to respond within 20 working days.

The **AboutMe** tool on OPC's website is a popular way for people to apply to a business for their own information, but businesses also need to make sure they've got good systems and processes for delivering this mahi. Although it's the law, quick turnaround says to your customers that they matter; it's a boost to the trust and confidence that your customers or clients have in your brand.





Insight 4

Whether your business is big or small, the privacy breach risk is about the same

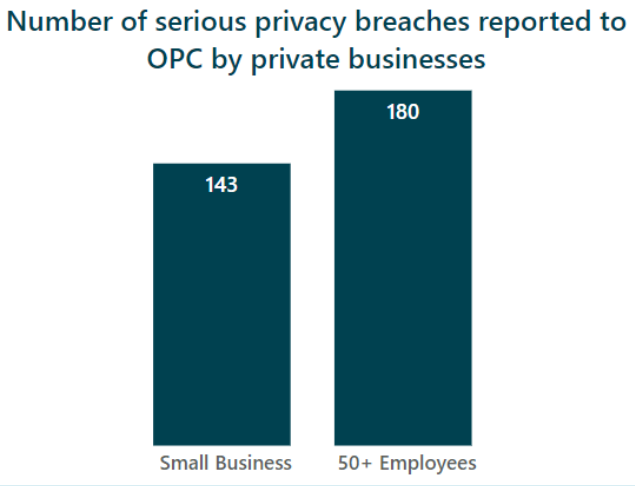
The more people in a business, the greater the potential for privacy accidents, right? Wrong. Our research shows small businesses are more likely to report serious privacy breaches caused by human error than large organisations.

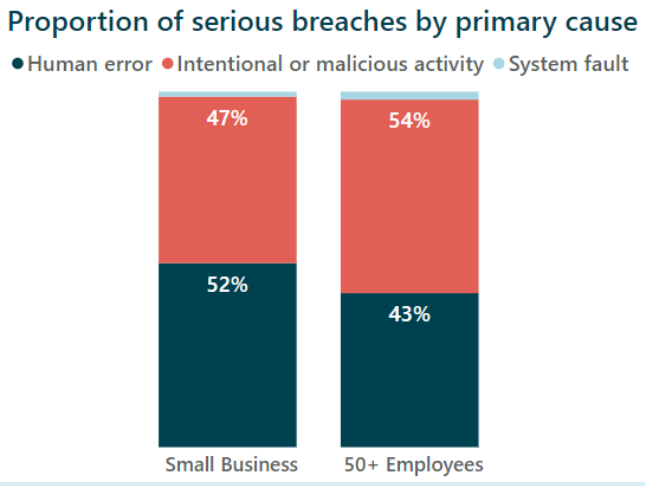
In smaller places of business there's an almost equal chance of intentional or malicious activity causing a breach. Regardless of their size businesses need privacy safeguards in place.

One of the simplest intentional breaches is through employee browsing; employees looking up personal records of others for their own interest. That includes people looking up where their ex-partner lives, looking to see how much people get paid, and checking out whether members of their organisation have filed any complaints or been the subject of complaints. We suspect that employee browsing activities are often unreported to OPC, or 'filed' by organisations broadly as misconduct. But it is still a privacy breach that small businesses need to keep an eye out for, especially because it is so easy to do, and should be reported to OPC if it meets the threshold of serious harm.

Businesses are obligated to stop their employees from inappropriately accessing people's information. That means ensuring information is gathered appropriately and protected from loss, accidental, or unauthorised disclosure, access, use, or modification. You also need a clear privacy statement, and processes that outline what to do if a breach happens.

Take time to educate your staff about employee browsing, ensure you have processes and audits in place to review staff access to information, and report it to OPC if it happens.





Case note: It's not what you know...

The privacy principles in play are:

- **Principle 5 - storage and security of information**
- **Claimed breach of principle 11 – disclosure of personal information**

In 2021 a patient complained to OPC that their medical clinic had potentially breached their privacy. The patient had organised medical tests through the clinic and then returned to the clinic to discuss the results.

A staff member initially looked at the patient's records to check them in for their appointment, but later (when the information was no longer related to their work) took another, unauthorised, look at the results. The patient then claimed that the staff member discussed their results with their ex-partner, who happened to be the current partner of the patient.

When OPC investigated they learnt that the clinic's system audited who'd looked at which files, which confirmed the staff member had accessed them beyond what was reasonable. Employee browsing is the term for staff reviewing files for their own, not work-related, interest and it's considered a privacy breach.

Because of a lack of evidence, OPC was unable to make a finding about whether there had been a breach of principle 11 but we did discuss our findings with the clinic. This discussion resulted in an apology being issued to the patient by all of those involved as well as a rework/ updating of the privacy practices and policies at the clinic. It also resulted in the clinic ensuring all their staff knew of the Privacy Act 2020 and used the free online training available on the OPC website.

Learn and do:

Make sure your employees know about the Privacy Act 2020, what it is and their obligations. OPC has free, online training and resources on our website, which are an easy way to train staff (**OPC's Free online learning**).

Privacy Commissioner
Te Mana Mātāpono Matatapu

Office of the Privacy Commissioner I Te Mana Mātāpono Matatapu
PO Box 10094, The Terrace, Wellington 6143
T +64 4 474 7590 Fax +64 4 474 7595
E enquiries@privacy.org.nz
www.privacy.org.nz