

Privacy ABC

Learn about the Privacy Act,
what's covered, and how it's
applied in practice.

September 2024



Privacy at home and at work



You can also do this as e-learning at privacy.org.nz

Agencies



The Privacy Act applies to agencies (businesses and organisations).

Domestic



The Privacy Act also applies to domestic relationships if the subject matter is highly offensive.

But not...



The Act **does not** apply to domestic relationships when the subject matter is not highly offensive.

A notifiable privacy breach happens when an organisation or person either intentionally or accidentally:

- Provides unauthorised or accidental access to someone's personal information.
- Discloses, alters, loses or destroys someone's personal information
- A privacy breach also occurs when someone is unable to access their personal information due to, for example, their account being hacked.

These are all examples of privacy breaches:



A bar owner tells a woman's employer that her debit card often declines for small transactions.



A GP's office accidentally sends a letter with details of a man's chronic sickness to the wrong address.



A construction company's customer database is loaded onto a USB, which is then lost.

What is 'highly offensive?'

These are three good examples:

- A person shares intimate photos of their former partner on social media.
- A person sets up a camera outside their neighbour's bathroom window.
- A home CCTV camera capturing the activity of small children in the next door neighbour's house.

Domestic affairs

The Privacy Act doesn't normally apply to domestic affairs. Here's some examples of when the Privacy Act **would not** apply.

- A person's flatmate takes a picture of their dirty dishes and posts it on social media.
- Someone's cousin gossips to the rest of the family about that person's relationship troubles.
- A person takes detailed notes about what time their neighbour comes home at night.



Agencies and individuals

An organisation can be held accountable for the actions of a person within that organisation. For example:

- A DHB breaches someone's privacy after a nurse looks at their neighbour's medical history.
- A tennis club breaches the Privacy Act after one of its members steals a customer list and starts calling people to ask them if they want to take part in a pyramid scheme they just signed up for.
- A consultancy breaches someone's privacy after an employee accidentally emails a spreadsheet of client details to every person on that spreadsheet.

Defining personal information



Identifying information

Personal information is information that could identify a person.

Personal information doesn't have to specifically identify someone with their name. It only needs to include enough information to identify the person.

Some examples are:



A spreadsheet of names and driver licence numbers.



Security camera footage of a person.



Notes from a conversation between a manager and an employee.

When you can collect personal information





Meet B

B owns a small food truck selling tacos from various places around town.

His phone number is on the side of his food truck, and customers occasionally text ahead with their orders. B has those numbers in his phone so thinks he'll start texting them to let them know where he'll be parked each day so they can buy a taco.

Noting down phone numbers is an example of information collection. Businesses – like B's taco truck – are only allowed to collection information for lawful purposes, connected to the function of the business.

Learning check

Read the scenario here and decide whether it would be okay for B to note down customer's numbers.

As we know, B wants to tell existing customers where he is parked so they can buy a taco from him. Is this allowed?



B is in the business of selling tacos, so collecting information to help people buy tacos is both lawful and connected to a function of his business – as long as he tells them he's collecting their information.

Learning check

Read the scenario here and decide whether it would be okay for B to note down customer's numbers.

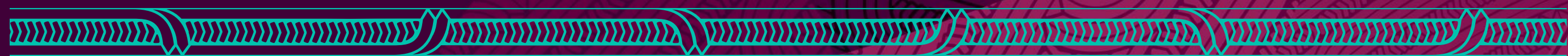
Personal information must be collected for a lawful purpose, and the purpose has to be connected to what the business does.

B's friend is a mechanic and he wants B to give him the phone numbers as potential clients.



The mechanic may want the phone numbers for the lawful purpose of running his business, but this is not connected to the function of B's taco truck – so it's not okay for B to collect information for this purpose.

What to tell people when you collect their information



Meet L

Agencies need to tell people certain things when they collect personal information.

L works at a small community organisation that provides support and advice for low-income families.

L wants to find out more information about the organisation's clients.

They decide to start documenting the name and address of each client, as well as some details about their living arrangements and which other community organisations they work with.

Is L allowed to ask for that information?

Privacy statement



L can ask for extra information from their clients, but must take steps to make sure people are aware of certain things.

- **WHAT** information is being collected
- **WHY** it's being collected
- **WHO** will see it
- **WHAT** will happen if they do not give L the information.

The best way to make people aware of these things is through a privacy statement.

The Office of the Privacy Commissioner has Priv-o-matic, a privacy statement generator that you can use for free at [privacy.org.nz](https://www.privacy.org.nz)

Learning check

L begins preparing their privacy statement. Are the following statements true or false?

L can request certain information from the organisation's clients?



TRUE – L just needs to clarify that if the clients don't want to give their information they won't be able to engage with the organisation's services.

However, L chooses not to do this because they would rather engage with people anonymously than not at all.

Learning check

L begins preparing their privacy statement. Are the following statements true or false?

L's privacy statement needs to be drafted by a lawyer



FALSE – a privacy statement just needs to convey information to people.

Limits on collecting information



Privacy statement

When you collect information, such as by making a video recording of your customers, you need to do so in a way that is fair, reasonable and not overly intrusive.

A pub owner is concerned about the number of assaults that have happened in his place of business. One of the 'problem areas' is in the bathrooms, so he installs a security camera. The easiest place to install the camera is directly about the toilet.



Let's check in



In an effort to be upfront with his customers, the pub owner puts up a sign telling people that there is a camera in the bathroom and why it has been installed.

Has the pub owner fulfilled their privacy obligations?



NO – it's not enough to just put up a sign.

You also need to be fair and reasonable about how you collect information.

What else?

Even with the sign in place, a customer still complains that the camera is an invasion of privacy because of its location. What can the pub owner do?

Select two correct answers:

1. Remove the camera
2. Amend the sign to add more detail
3. Move the camera to somewhere less intrusive.

The answer is 1 and 3 The pub owner can do either the first or third option Amending the sign

does not make the situation more fair and reasonable.

What happened next?



The pub owner chose to move the camera to a part of the bathroom where they can get the information they need without filming people as they use the toilet.

This allows them to comply with the Privacy Act while also getting the information they need to prevent assaults.

Storing information safely



Meet C

When you collect information from people you need to take reasonable steps to keep it safe. The more sensitive the information, the more you need to do to keep it safe.

C volunteers at his local tennis club. Every time a new member joins, they fill out a form with their name, address, date of birth, tennis skill level, and other information. C then stores that form in a three-ring binder, which is kept behind a desk.

One evening, the club gets broken into and a number of things, including the binder, are stolen. Did the tennis club take reasonable steps to protect their members' personal information?

Learning check

In this case, the tennis club has probably not taken reasonable steps to keep the information secure.

Since the break in, the tennis club has changed the steps they take to protect their member's personal information.

C now keeps the binder in a locked cabinet. Is that a good change?



YES – that is safe, but they're not completely in the clear. A locked cabinet is fairly easy to break into, but is a step above just keeping it on a desk.

What else did C do?



Agencies have an obligation to take reasonable steps towards security, given the circumstances.

C types up the information from the binder and puts it in a spreadsheet, which he stores on a password-protected computer. Is that a good step?



YES that's a great option because it is more secure.

Sensitivity of information



Agencies have to take greater care with more sensitive personal information. The more sensitive the information, the more steps they need to take to keep it secure.

Agencies have an obligation to take reasonable steps towards security, given the circumstances.

Is it okay that C takes the binder home with him to add some additional information?



YES – as long as the information is kept equally secure.

Learning check

Agencies have an obligation to take reasonable steps towards security, given the circumstances.

A receptionist from a sexual health clinic takes some client files home so they can finish some work they didn't get to during the day.

Is that okay?



NO – this is not acceptable, because the information in question is much more sensitive than tennis club registration information.

If you have a breach

If you have a privacy breach, where the wrong person sees someone's information, or you lose someone's personal information, you may need to tell the Privacy Commissioner.

It is mandatory to notify serious breaches and it's better to be safe than sorry.



Privacy Commissioner
Te Mana Mātāpono Matatapu

If you have a breach

Our tool NotifyUs at privacy.org.nz helps you work out if you need to report a breach to us, then helps you report it if you do.

Or call us on 04 887 6650 or 0800 803 909.



Privacy Commissioner
Te Mana Mātāpono Matatapu

Seeing your own personal information



Meet T

The Privacy Act gives you the right to see the personal information that agencies hold about you.

T has left his employer of 15 years, and is now in a dispute over unpaid wages. They are considering taking the case to the Employment Relations Authority, but need copies of his timesheets as evidence of the hours he worked.

All T needs to do is ask for the information. T can ask in any manner: phone, email, letter, arrive in person, or contact the company on social media. T could also use AboutMe at [privacy.org.nz](https://www.privacy.org.nz) which is a tool to help people access their information.

Information request

Once T asks his previous employer for their timesheets, the company has up to 20 working days to decide whether T's request will be granted and give notice of the decision.

If the company chooses not to give the information, it must give a reason. These could be:

- The information doesn't exist
- It's too hard to get the information
- Giving T the information would disclose sensitive information about another person.

Learning check



Read these scenarios and decide whether the business has to give T their timesheets in these circumstances.

Does the business have to give the timesheets if they need to be printed out, and the admin person who knows how to use the system only comes in on Fridays?



YES – the company should provide T’s timesheets. There is no reason why the company can’t have the admin person print out the timesheets on Friday.

The timesheets are only on a master timesheet with every employee, so giving them to T would also reveal the hours worked and pay rates of other employees.



YES – but with changes. The company should provide the information, but it should black out the details of the other employees on the timesheets. This way it can give T their information without breaching other employee’s privacy.

Do T's timesheets need to be given?



Timesheets were deleted after seven years, and some of T's timesheets were deleted as part of this process. Does the employer need to give the timesheets?



NO – if the information doesn't exist, it's impossible to share it with T. If the employer has deleted some of the information as part of a routine process, this is a good reason not to share that information with T.

T's timesheets were deleted in anticipation of his legal action.



YES – agencies cannot delete information that they otherwise would not have deleted, just to avoid giving it to people who may ask for it. Destroying information to avoid giving it to the person is an offence under the Privacy Act, with a fine of up to \$10,000.

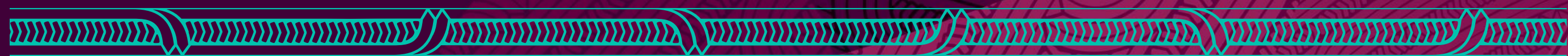
Access determinations

The Privacy Commissioner can issue an access determination to require an agency to provide personal information to the requester, or to respond to the request if the business has not done so.



Privacy Commissioner
Te Mana Mātāpono Matatapu

Making changes to your personal information



Meet R

Agencies have to review your information when you tell them it's wrong.

R is a casual construction labourer for an employment agency. The agency sends them on short-term assignments to various construction firms around town.

At the end of each assignment, the firms provide short reports of each employee's performance. This is held by the employment agency and used to determine suitability for future assignments. R's reports have always been satisfactory.



Mixed up reports

R and another employee are assigned to jobs on the same construction site. The other employee arrives an hour late. They're also not dressed appropriately (wearing jandals when they work be wearing work boots), and they are eventually sent home early after making a number of simple mistakes.

The construction firm then mixes up the two employees in its reports to the employment agency.

When R finds out, they ask the employment agency to amend their record by removing the incorrect report from their file.



Learning check

R has asked the employment agency to amend its records by removing the incorrect report from their file.

Which of these three options **must** the employment agency do in this situation?



Immediately remove the report.



Review the review to see if there's been a mistake.



Penalise the construction firm for sending incorrect information.



Statement of correction

It's generally best to correct information when it's clearly wrong, and add a statement if an agency can't confirm its accuracy or if there is a dispute.

In this case, the agency does both. When R tells the agency the information is wrong, and why, the company looks into the matter by talking to the construction form and the other employee.

This takes a few days, so in the interim it attaches a statement of correction to the report.

Once the employment agency is satisfied that R's version of events is correct, it removes the correct report from their file.

Another check in...

Read the scenarios below and decide whether the agency should correct the information or add a statement to it.

Someone mistypes a number, and the result is an incorrect birth date on someone's file.

Change the information. The correct birth date should be easy to verify. Once this has been done, the agency should change its records to reflect the actual birth date.

A person thinks they've incorrectly been characterised as angry in an incident report, and would like the word changed to 'frustrated.'

'Angry' and 'frustrated' are subjective words, so both could be correct.



Let's do one more learning check...

In these scenarios should the agency correct the information or add a statement to it?



A woman has changed banks, and wants to change the details on the direct debit portion of her file with the power company.

Change it: agencies always need to take steps to ensure information they hold is accurate, and this is particularly true with sensitive information such as bank account details.

An employee was the subject of an internal sexual harassment investigation. The allegations that led to the investigation could not be substantiated, and now the employee wants the record of the investigation removed from their file.

Add a statement: the fact that the allegation could not be substantiated, the investigation still occurred, so the agency chooses to leave it in his file, but with a statement from the employee outlining why they think it should be removed.



Keeping information accurate



Meet M

Agencies need to take reasonable steps to make sure the information they use is accurate.

M has developed a disability that will prevent them from working for the rest of their life. They are living off a weekly payment from an income protection insurer.

One day, M receives a letter from their provider outlining that payments will stop, because it has determined that M is not actually disabled.

M goes without income for several weeks while they resolve the issue with their insurer. It turns out that a letter from a member of the public about another client was accidentally stapled to M's file. The letter said that M spends afternoons going for walks and hanging out washing.



Reasonable steps

The insurer assumes the letter refers to M, and uses it as a basis to cut off their payments.

The law requires the insurer to **take reasonable steps** to check whether the information is accurate.

Reasonable steps take into account:



How old the information is.



Where the information came from.



What the information is being used for.

Inaccurate information

If an agency, such as M's insurer, does not take reasonable steps to check the accuracy of the personal information it uses, it could be breaching the individual's privacy.

Older information requires more checking than recently-acquired information. Information from third parties requires more checking than information that came from the individual.

Finally, information that is being used in a way that negatively affects someone needs more checking.

Learning check

Read the scenario and select whether the agency needs to take many, some, or a few steps to verify that the information is accurate.

An employer does an internet search for a potential employee's name, and finds a number of articles about that person's fraud convictions.

The employer should take **some steps** to verify this, as the information will have a negative impact on the person and it is also second-hand (through newspaper articles). It may be a different person with the same name.

Using and sharing information



Using information



Generally, you can only use information for the purpose you told the individuals about when you originally collected it. There are some exceptions, such as when there are safety issues.

B owns a food truck. You may remember him from earlier where he's asking his repeat customers for their cell phone numbers so that he can contact them with updates, like where he's parked each day and any special deals he's offering.

This is the privacy statement he gave them when he asked for their phone numbers.

I'd like to take your phone number so that I can send you updates.

Learning check

Read the scenario below and decide if Bill is permitted to use his customer's phone numbers in this way. Remember, Bill's privacy statement said: I'd like to take your phone number so that I can send you updates.

B is adding new items to his menu, and wants to tell his customers about it.



Yes – B is allowed to do that because changes to the menu would be covered by his privacy statement.

Learning check

Read the scenario below and decide if Bill is permitted to use his customer's phone numbers in this way. Remember, Bill's privacy statement said: I'd like to take your phone number so that I can send you updates.

The butcher that provides B's meat for his tacos wants B's customer list so that he can sell them meat directly.



No – this new use would not be permitted – Bill's customers did not give permission for their phone numbers to be shared.

Exceptions

There are times when you may use information for other reasons.

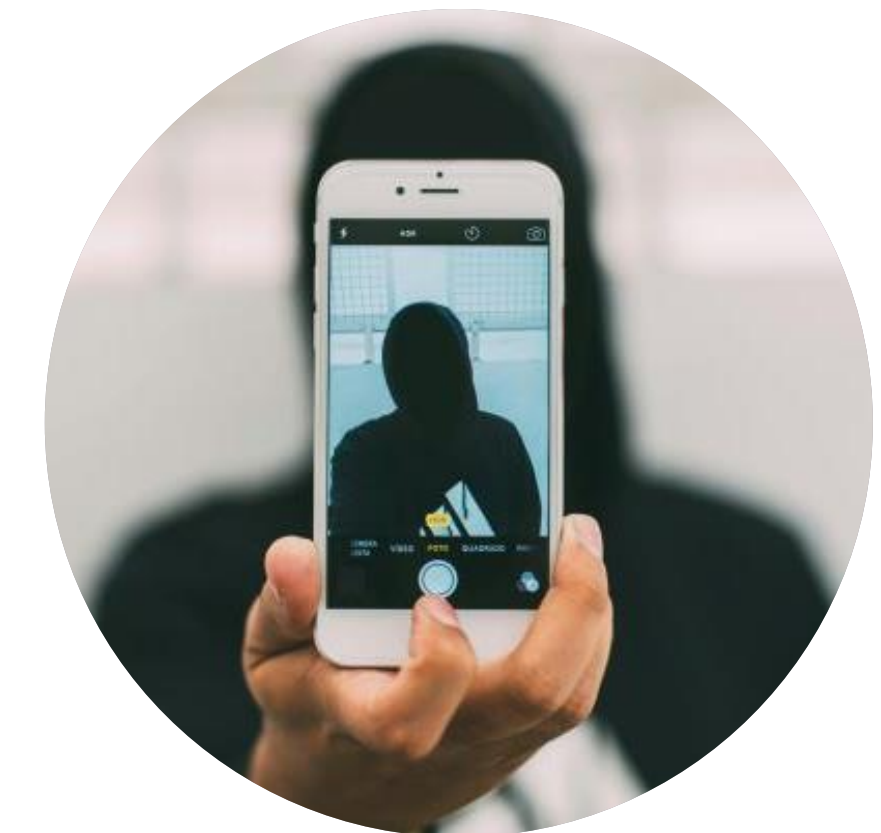
Some reasons for exceptions are:



Someone's life or health is at risk.



The information came from a publicly available source.



The information is used in a way that can't identify the individuals.

Let's check in

Read the scenario below and decide if B is permitted to use his customer's phone numbers in this way.

B's drink supplier has told him that the batch of fizzy drinks is off, and anyone who drank one needs to go to the doctor immediately. Can B use his list to call his customers and let them know?



Yes – Their health is in danger, so B should call them immediately.

Can B share?

A hospitality industry association is doing market research, and wants to know how many customers B has via the number of phone numbers he collected.



Yes – by counting the customer’s phone numbers to determine the number of customers, B is not disclosing any personal details that could be used to identify individuals.

The same industry association wants to build its own database, and asks everyone with a food truck to share their customer’s details.



No – the association will be able to identify the individuals if B provides this level of detail and B’s customers haven’t agreed to this.

Disclosing information overseas



If you send information overseas, there are additional rules you need to follow. These are:

- The overseas country needs to have laws comparable to the New Zealand Privacy Act OR
- The contract needs to ensure there are comparable safeguards OR
- The overseas agency needs to have a presence in New Zealand.

Otherwise, you need to get specific permission from the person the information relates to.

Holding onto information



Meet E

Under the Privacy Act, you may not keep information for any longer than you need it.

E runs a company that organises concerts, stand-up comedy gigs and other events.

E allows people to buy tickets by transferring money and then emailing them their name. People can then collection their tickets at the door by giving their name.

Let's check in

E has a list of names of people who have pre-paid the admission for a concert they're promoting. When should E dispose of the list of people's names?

1. Before the concert.
2. Immediately after the concert.
3. Three months after the concert, along with every other list from the other concerts she put on in the interim.

The answer is 2 – disposing of the list of names in the next few days would also be okay, as it may not be practical to dispose of the list late at night on a weekend.

Deleting information

You don't necessarily have to delete information immediately. You only have to delete information once you no longer need it. This could be a long time, depending on why it was collected.

Learning check in

Read both scenarios and select the scenario that lets the agency keep the information for longer.



A call centre records phone calls for quality assurance and training purposes.

That's right! The call centre can keep the information as long as it has quality assurance and training to do.



A builder records a phone call with a client to make sure they capture all the relevant details about a job.

The builder won't need the recording once they've done the job, so should delete the recording at that point.

Learning check in

Read both scenarios and select the scenario that lets the agency keep the information for longer.



A GP office holds medical records about current and former patients. This information will be made available to the patients or their medical practitioners in the future to assist with their medical care.

That's right! Health records are relevant for a long time. GPs are required to keep them for at least 10 years after the last time they see a patient. Billing records on the other hand probably won't be relevant or needed after 10 years.



The same GP office holds billing information about each patient, such as how many times they have been late to pay their bill. This information is held in order to work out which patients need to pay ahead of their appointments and which patients can be billed later.

**Congratulations! You've
completed your training.**



Privacy Commissioner
Te Mana Mātāpono Matatapu