Privacy Act 2020 changes

Information sheet 1

New Zealand's Privacy Act has been modernised to reflect changes in the wider economy and society and to ensure it is fit for the technological world in which we live.

Notifiable privacy breaches

If a business or organisation has a privacy breach that has caused serious harm to someone (or is likely to do so), it will need to notify the Office of the Privacy Commissioner as soon as possible. It is an offence to fail to notify the Privacy Commissioner of a notifiable privacy breach.

If a notifiable privacy breach occurs, the business or organisation should also notify affected people. This should happen as soon as possible after becoming aware of the breach.

For more information, see Information sheet 2: Breach notifications

Compliance notices

The Privacy Commissioner will be able to require a business or organisation to do something, or stop doing something, if it is not meeting its obligations under the Privacy Act.

Binding decisions on access requests

The Privacy Commissioner will now be able to make decisions on complaints relating to access to information. This will mean a faster resolution to information access complaints.

For more information, see Information sheet 6: Access directions

Disclosing information overseas

A New Zealand business or organisation may only disclose personal information to an overseas agency if that agency has a similar level of protection to New Zealand, or the individual is fully informed and authorises the disclosure.

For more information, see Information sheet 3: Cross-border disclosure

Extraterritorial effect

The Privacy Act has extraterritorial effect. This means that an overseas business or organisation may be treated as carrying on business in New Zealand for the purposes of its privacy obligations – even if it does not have a physical presence in New Zealand. This will cover businesses such as Google and Facebook.

New criminal offences

It will now be a criminal offence to:

1. mislead a business or organisation by impersonating someone, or pretending to act with that person's authority, to gain access to their personal information or to have it altered or destroyed.
2. destroy a document containing personal information, knowing that a request has been made for that information.

The penalty in all cases is a fine up to $10,000.

For more information, visit privacy.org.nz/askus or find us at:

PrivacyNZ @nzprivacy

Privacy Commissioner
Te Mana Mātāpono Matatapu

Breach notifications

Information sheet 2

What is a privacy breach?

A privacy breach is where there has been unauthorised or accidental access to personal information, or disclosure, alteration, loss, or destruction of personal information.

It can also include a situation where a business or organisation is stopped from accessing information – either on a temporary or permanent basis.

What is a notifiable privacy breach?

If a business or organisation has a privacy breach that has caused serious harm to someone (or is likely to do so), it will need to notify the Office of the Privacy Commissioner as soon as possible. It is an offence to fail to notify the Privacy Commissioner of a notifiable privacy breach. Failure to notify could incur a fine of up to $10,000.

Our Office has an online tool on our website, NotifyUs, to lodge notifications.

Notifying affected people

If a notifiable privacy breach occurs, the business or organisation should also notify affected people. This should happen as soon as possible after becoming aware of the privacy breach. Failure to do so may be an interference with person's privacy under the Privacy Act.

There may be valid reasons why an agency would not notify affected individuals.

What should I include in a notification?

There are key details businesses or organisations must include when notifying our Office and affected people. These details will enable people to protect themselves from harm. Our online reporting tool, NotifyUs, will guide you through this process.

Why is this important?

When there has been a privacy breach, notifying people lets them take action to protect themselves and their information.

For example, if your online account information is compromised, you can protect yourself by changing your password. If your credit card details are stolen, you can cancel your card. But if you don't know that your privacy has been breached, you can't taken any protective action.

What does it mean for me?

Check whether you have robust systems to secure the personal information you hold both in physical and digital forms. Check whether you have systems in place to identify and report privacy breaches. If you have a 'near miss', even if it does not reach the threshhold of a notifable privacy breach, learn from the mistake — improve your systems to stop the same thing happening again in the future.

If you are an individual, the Privacy Act will provide better protection to you if there is a privacy breach involving your personal information.

For more information, visit privacy.org.nz/askus or find us at:

PrivacyNZ @nzprivacy

Privacy Commissioner
Te Mana Mātāpono Matatapu

Cross-border disclosure

Information sheet 3

The Privacy Act 2020 contains a new information privacy principle, principle 12, which sets rules around sending personal information to organisations or people outside of New Zealand. Sending personal information overseas is known as "cross-border disclosure."

Purpose

Principle 12 aims to ensure that personal information sent overseas is subject to privacy safeguards that are similar to those in New Zealand.

Businesses and organisations will now be responsible for ensuring that any personal information they disclose to organisations outside New Zealand is adequately protected. Businesses and organisations must be able to demonstrate that they have undertaken necessary due diligence before making a cross-border disclosure.

Controls

A business or organisation may only disclose personal information to another organisation outside New Zealand if the receiving organistion:

- is subject to the Privacy Act because they do business in New Zealand
- is subject to privacy laws that provide comparable safeguards to the Privacy Act – or they agree to protect the information in such a way, e.g. by using model contract clauses.
- is covered by a binding scheme or is subject to the privacy laws of a country prescribed by the New Zealand Government.

Permission of the person

If none of the above criteria apply, a business or organisation may only make a cross-border disclosure with the permission of the person concerned. The person must be expressly informed that their information may not be given the same protection as provided by the New Zealand Privacy Act.

Cloud storage

A business or organisation may send information to an overseas organisation to hold or process on their behalf as their 'agent'. This will not be treated as a disclosure under the Privacy Act.

A typical example of this is an overseas company providing cloud-based services for a New Zealand organisation. The New Zealand organisation will be responsible for ensuring that their agent – the overseas company – handles the information in accordance with the New Zealand Privacy Act.

Urgent disclosures

A business or organisation may need to make a cross-border disclosure in certain, urgent circumstances where it would not otherwise be allowed. IPP 12 allows cross-border disclosure when it is necessary to maintain public health or safety, to prevent a serious threat to someone's life or health, or for the maintenance of the law.

For more information, visit privacy.org.nz/askus or find us at:

PrivacyNZ @nzprivacy

Privacy Commissioner
Te Mana Mātāpono Matatapu

Enforcement powers

Information sheet 4

The Privacy Act 2020 gives the Privacy Commissioner greater powers to ensure businesses and organisations comply with their obligations. The two key new powers in the Act are access directions and compliance notices. The Act also introduces new offences and greater potential fines for those who commit them.

Access directions

Principle 6 gives people the right to access their personal information. If a business or organisation refuses or fails to provide access to personal information in response to a principle 6 request without a proper basis, the Commissioner may now compel the agency to give this information to the individual concerned.

Access directions may be appealed to the Human Rights Review Tribunal.

Compliance notices

The Privacy Act 2020 allows the Commissioner to issue compliance notices to agencies that are not meeting their obligations under the Act. A compliance notice will require an agency to do something, or stop doing something, in order to comply with the Privacy Act.

Compliance notices may be appealed to the Human Rights Review Tribunal.

Refusing to comply with a compliance notice

Refusing to comply with a compliance notice is an offence under the Privacy Act. A business or organisation that has been issued a compliance notice and fails to change its behaviour accordingly can be fined up to $10,000.

Misleading an agency to get personal information

There is a new fine of up to $10,000 for misleading a business or organisation to access someone else's personal information. For example, it will be an offence to impersonate someone else in order to access their personal information.

Destroying requested information

If someone requests their personal information and a business or organisation destroys it in order to avoid handing it over, the business or organisation can be fined up to $10,000.

Failing to notify a privacy breach

If a business or organisation has a privacy breach that has caused or is likely to cause serious harm, it must notify the Privacy Commissioner. Failing to inform the Commissioner of a notifiable privacy breach can result in a fine of up to $10,000.

For more information, see www.privacy.org.nz and Information sheet 2: Breach notifications

Updated Privacy Principles

Information sheet 5

The Privacy Act 2020 is based on the 13 privacy principles. In the new Act, some of the principles have been updated and a new principle has been added.

These changes help ensure the Act is relevant and useful in regulating new privacy challenges. The key changes to the principles are outlined below.

Principle 1

Principle 1 has been updated to clarify that you can only collect identifying information if it is necessary. If you don't really need identifying information, such as a person's name or their contact details, you shouldn't collect it.

Your goal should be to collect and use the least amount of information possible to meet your objective. This is called data minimisation.

Principle 4

The new Act specifically requires businesses and organisations that are collecting personal information from children or young people to consider whether the way they collect the information is fair in the circumstances. It may not be fair to collect information from children in the same manner as you would from an adult.

Principle 12

A new principle 12 has been added to the Act which regulates how personal information can be sent overseas. Sending information to an organisation outside New Zealand is known as cross-border disclosure.

Principle 12 states that personal information may only be disclosed to organisations in other countries where there are similar protections to those in the New Zealand Privacy Act. If a jurisdiction does not offer similar protections, the receiving organisation may agree to sufficiently protect the information, e.g. using **model contract clauses**, or the person concerned must be fully informed that their information may not be adequately protected and they must expressly authorise the disclosure.

For more information, see Information sheet 3: Cross-border disclosure

Principle 13

Principle 13 now states that businesses and organisations must take reasonable steps to protect unique identifiers from being misused. Unique identifiers were previously in principle 12 but this has been renumbered principle 13 in the new Act.

Unique identifiers are individual numbers, names, or other forms of identification allocated to people by organisations, such as your National Health Index number. It is important that organisations protect the unique identifiers that they use and only use those that are appropriate for their services to reduce the frequency and impact of identity theft.

Access Directions

Information sheet 6

The Privacy Commissioner frequently investigates complaints about businesses or organisations failing to give people access to their personal information.

After an investigation, the Privacy Commissioner will be able to make binding decisions on these complaints and issue an access direction to the business or organisation concerned.

What is an access direction?

An access direction is a binding written notice issued to a business or organisation by the Privacy Commissioner. The notice directs the business or organisation to release personal information to an individual.

The Commissioner can issue an access direction if there has been an investigation of a principle 6 complaint and the Privacy Commissioner has determined that the person is entitled to some or all of the personal information they requested.

What is included in an access direction?

All access directions will outline the steps or conditions the business or organisation needs to take to comply. This will include what information the business or organisation needs to release, the process they need to follow, and the date by which they must take those steps.

What organisations need to do

If a business or organisation receives an access direction, it must take steps to comply as soon as possible.

If a business or organisation disagrees with an access direction, it can appeal to the Human Rights Review Tribunal. An appeal must be lodged within 20 working days of receiving the notice.

Enforcement

If a business or organisation does not comply with an access direction, the complainant may bring proceedings in the Human Rights Review Tribunal for an order to enforce the access direction.

It is an offence to fail to comply with an access order issued by the Tribunal without reasonable excuse. A business or organisation can be fined up to $10,000 in such cases.