UnderCover
Insurance and legal news from the VL desk
vero liability insurance limited
September 2021 | Issue 4

Privacy Matters

The laws around privacy have changed and protecting private information is more important than ever.

The new Privacy Act 2020 came into force in December last year and modernised the old Privacy Act to reflect changes in our economy and society; and the wider technological world in which we live. There are now greater protections for individuals and significant new obligations and penalties for businesses and organisations.

Who does the Privacy Act 2020 apply to?

The Privacy Act 2020 is wide-ranging and applies to any organisation or business (referred to in the legislation as an 'agency'). This includes:

- government departments
- companies
- small businesses
- social clubs
- other types of organisations.

What key changes have been made to the Privacy Principles?

There are important changes to some of the Privacy Principles (the Principles) which underpin the Privacy Act 2020. The Principles govern how agencies should collect, handle and use personal information.

Personal information is any information which tells us something about a specific individual. The information does not need to name the individual, as long as they are identifiable in other ways, like through their home address. Personal information is not limited to sensitive, intimate or private information. It can be personal information even if publicly available. It may include a person's name, contact details, financial records, health records, purchase history, date of birth and log in details.

Principle 1 has been updated to clarify that agencies can only collect identifying information if it is necessary. If agencies don't really need identifying information, such as a person's name or their contact details, they shouldn't collect it. The goal should be to collect and use the least amount of information possible to meet an agency's objective. This is called data minimisation.

Principle 4 now requires agencies 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.

A new Principle 12 has been added which regulates how personal information can be sent overseas. Sending information to an organisation outside New Zealand is known as cross-border disclosure. This is discussed further below.

Principle 13 now says that agencies must take reasonable steps to protect unique identifiers from being misused. Unique identifiers are individual numbers, names, or other forms of identification allocated to people by organisations. It is important that agencies 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.

A useful summary of all the 13 Principles is available here.

New legal obligations to notify privacy breaches

If an agency 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 (OPC) as soon as possible. The OPC advises this should be no later than 72 hours after agencies are aware of a notifiable 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. Importantly, it can also include a situation where a business or organisation is stopped from accessing information – either on a temporary or permanent basis, for example, after a denial-of-service attack.

© Vero Liability Insurance Limited 2021

'Harm' can include:

- loss, damage or disadvantage
- loss of a benefit or right
- emotional harm, such as significant humiliation or loss of dignity.

There were 76 serious privacy breaches notified to the OPC between 1 December 2020 and 31 March this year. This was a 97% increase in the number of breaches reported in comparison to the preceding six months. The OPC says that breaches can occur in any sector – public, private, or non-profit. Breaches were reported from the social assistance sectors, financial and insurance services, education and training, retail trade and accommodation, and even mining.

It is an offence to fail to notify the OPC of a notifiable privacy breach. Failure to notify could incur a fine of up to $10,000.

More useful information on notifying a breach to the OPC including access to the notification tool is available here.

Notifying affected individuals if a breach occurs

If a notifiable privacy breach occurs, the business or organisation must also notify the affected people (with some exceptions). This should happen as soon as possible after becoming aware of the breach. Failure to do so may be an interference with a person's privacy under the Privacy Act 2020. Notifying people also lets them take action to protect themselves and their information.

There may be some valid reasons why an agency would not notify affected individuals. The OPC's NotifyUs tool assists with the notification and decisions about notifying affected people.

The Privacy Commissioner now has greater powers

The Privacy Act 2020 gives the Privacy Commissioner (the Commissioner) greater powers to ensure agencies comply with their obligations. The two key new powers are access directions and compliance notices.

If an agency refuses or fails to provide access to personal information in response to a request without a proper basis, the Commissioner may now compel the agency to give this information to the individual concerned through an access direction. An access direction is a binding written notice issued to an agency by the Commissioner directing it to release personal information to an individual. Access directions may be appealed to the Human Rights Review Tribunal.

The Privacy Act 2020 also allows the Commissioner to issue compliance notices to agencies that are not meeting their obligations. A compliance notice will require an agency to do something, or stop doing something, in order to comply with the Privacy Act 2020. Compliance notices may also be appealed to the Human Rights Review Tribunal

A business or organisation that has been issued a compliance notice and fails to change its behaviour can be fined up to $10,000.

The OPC says that in the first six months of the Privacy Act 2020, it focussed on education to help agencies understand their new legal responsibilities. However, it has signalled that it is prepared to use enforcement action to support behaviour changes in those agencies that repeatedly fail to meet their obligations or should know better. For example, this might be if breaches generated by email errors persist in organisations that are not taking the necessary precautions.

"Just go ahead and enter your email for us."

New offences and greater potential fines for those who commit them

There are new criminal offences in the Privacy Act. It will now be a criminal offence to:

- 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.
- destroy a document containing personal information, knowing that a request has been made for that information.

As mentioned above, it is also an offence not to notify a notifiable breach. The penalty in all cases is a fine up to $10,000.

© Vero Liability Insurance Limited 2021

New obligations apply when transferring privacy information overseas

Agencies will now be responsible for ensuring that any personal information they disclose to organisations outside New Zealand is adequately protected. 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. The OPC has model contract clauses covering the protection of information that New Zealand agencies can use to assist with meeting their obligations.

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 cross-border disclosure under the Privacy Act 2020. A typical example of this is an overseas company providing cloud-based services for a New Zealand organisation. The New Zealand organisation will, however, be responsible for ensuring that their agent – the overseas company – handles the information in accordance with the Privacy Act.

A business or organisation is permitted to make a cross-border disclosure in certain, urgent circumstances where it would not otherwise be allowed. This might be 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.

An overseas businesses or organisation may be treated as a New Zealand business for the purposes of its privacy obligations

The Privacy Act 2020 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.

Class actions for privacy and data breaches – an emerging risk

Where a group of people are harmed by a privacy breach, there is provision in the Privacy Act 2020 for a representative acting on behalf of the aggrieved individuals to make a claim in the Human Rights Review Tribunal. An award of up to $350,000 may be made to each member of the class. Obviously, the totals involved could be substantial if the harm is particularly serious and/or if there are many people impacted.

When it all goes wrong – responding to a privacy breach

The OPC advises that agencies should respond as quickly as possible to a privacy breach to minimise the harm. This response should involve:

- containing the breach and finding out what went wrong. This includes trying to get the lost information back, disabling the breached system and cancelling or changing access codes. It also involves immediately notifying their insurer, other parties like internal auditors and risk managers and Police if the breach appears to involve a theft or criminal activity.
- assessing the risks of the privacy breach including the types of personal information involved, the cause and extent of the breach; and the harm that may result.
- notifying the people whose personal information is handled if they could suffer serious harm (unless an exception applies). If the consequences from the breach are minimal or minor, or if telling people would cause more worry and harm than not telling them, it may be acceptable not to tell the affected individuals. Also notify the Privacy Commissioner if obliged to do so.
- preventing future breaches with a well-thought-out security plan for all personal information. The OPC suggests the International Organisation for Standardisation as a strong starting point: Information security management systems (ISO/IEC 27001:2013).

The OPC has more information on responding to a privacy breach here. They also have very useful Privacy Breach Guidelines.

Privacy breach insurance

The OPC says that if an organisation handles significant quantities of personal information, it may wish to consider cyber or privacy breach insurance. VL has a range of Statutory Liability and Directors & Officers Liability insurance policies for businesses and organisations; as well as a Cyber insurance offering. Talk to your broker for more information.

Want more information?

Most of the information in this issue of VL's *Undercover* is sourced from the very useful Office of the Privacy Commissioner website.

You can also find information on security and privacy for websites here.

© Vero Liability Insurance Limited 2021