GALLAWAY COOK ALLAN LAWYERS

New Privacy Act now in force

Jenna Riddle, Diccon Sim, Geoff Bevan and Gerrad Brimble

The Privacy Act 2000 (Act) came into force on 1 December 2020, replacing the previous Privacy Act 1993.

The new Act makes several changes to New Zealand's privacy legislation, including extending agencies' obligations when dealing with personal information, and conferring new compliance powers on the Privacy Commissioner.

Existing obligations under the previous Privacy Act 1993 continue to apply. The key changes introduced by the new Act are as follows:

Changes to the Information Privacy Principles

The information privacy principles are principles under the Act that set out how agencies are expected to deal with personal information. They can be found here. These have been updated to:

- Prevent identifying information being collected if it is not necessary;
- Require agencies that collect personal information from children and young people to do so in a way that is fair and does not unreasonably intrude on the individual's personal affairs; and
- Impose obligations on agencies that send personal information outside of New Zealand, to ensure that this information remains secure (see below for more details).

The Act also empowers the Privacy Commissioner to issue codes of practice that may affect how information privacy principles are applied.

Clarifying agencies responsibility

The new Act makes it clear that agencies are responsible for how their workers collect and deal with individuals' personal information, whether or not the agency knows about or has authorised the workers actions. The onus is therefore on agencies to make sure their workers know about and understand the information privacy principles, and that they have systems in place to monitor compliance.

Notifiable privacy breaches

The Act will require agencies to notify the Office of the Privacy Commissioner and affected individuals, as soon as possible if they have a privacy breach that they believe has caused or is likely to cause serious harm.

Not all privacy breaches need to be reported to the Privacy Commissioner, only those that cause or are likely to cause serious harm.

The Act establishes a number of tests to help agencies to assess whether a breach reaches the serious harm threshold and needs to be notified to the Privacy Commissioner. These include:

- the nature of the personal information;
- the nature of the harm that could be caused to affected individuals;
- who has obtained or may obtain the personal information;
- any action taken by the agency to reduce the risk of harm following the breach;
- whether the personal information is protected by security measures.

Failure to report a notifiable breach to the Privacy Commissioner is an offence under the Act liable to a fine of up to $10,000. The Privacy Commissioner has information here to help agencies through the process of responding to privacy breaches, including assessing the nature of the breach and whether it should be notified. The Commissioner has also developed an online tool, NotifyUs (here) that agencies can use to help decide if a privacy breach needs to be notified.

Given the potential fines that may be imposed for failing to properly report a breach, we anticipate agencies will initially take a cautious approach to reporting. Agencies in any doubt about whether a breach is serious are best to err on the side of "better safe than sorry" and report it.

Enforceable access directions

If an agency declines to give an individual access to their personal information, Individuals can ask the Privacy Commissioner to direct the agency to give them access. These directions will also be enforceable in the Human Rights Review Tribunal (Tribunal). Failure to comply with an order by the Tribunal will be liable to a fine of up to $10,000.

Compliance notices

The Privacy Commissioner is now able to issue an agency with a compliance notice. Compliance notices will notify an agency that they are not complying with the Act, and require the agency to remedy the breach. Compliance notices may also tell the

agency what steps it needs to take to remedy the breach, and the date by which the breach must be remedied.

If an agency fails to comply with a compliance notice, the Privacy Commissioner can seek enforcement in the Tribunal. Non-compliance with an enforcement order issued by the Tribunal is liable to a fine of up to $10,000.

Disclosing information overseas

The Act introduces a new privacy principle to deal with how information can be sent overseas. An agency will only be able to disclose information to an agency outside of New Zealand if that agency is subject to similar safeguards to those provided for in the Act. Agencies will therefore need to take appropriate steps to satisfy themselves information will be protected if it is sent outside of New Zealand.

The European Union's General Data Protection Regulations (GDPR) impose stringent data protection obligations on agencies operating in the EU, so New Zealand agencies may be able to send personal information to the EU with some comfort about its safety and security. However, other jurisdictions may have less robust data protection regimes in place. Agencies will need to ensure they understand where the personal information they send overseas is going, and satisfy themselves it is being dealt with appropriately.

If the agency knows personal information will not be adequately protected, or is not able to confirm that the personal information will be protected when it is sent overseas, it must tell the individual their personal information may not be protected, and get the individual's express authorisation to send their information outside of New Zealand.

Extraterritorial effect

The Act will also apply to agencies that operate in New Zealand, even if they are not physically located here. So online agencies like Facebook, Google, Amazon, Netflix or The Iconic will have obligations under the Act and will be liable if they fail to meet those obligations.

Gallaway Cook Allan can assist agencies with advice about their obligations under the Privacy Act 2020. Please contact our team to discuss your situation.