One year on – a look at the Privacy Act 2020

One year on we look at the implementation of the new tools created under the Privacy Act 2020 and how businesses are adapting.

On 1 December 2020, the Privacy Act 2020 (**Privacy Act**) came into force repealing and replacing the 27-year-old Privacy Act 1993. The implementation of the new Act followed a long period of review which coincided with significant developments in the use of data-centric technologies and strengthening of international data protection regulation.

The Privacy Act retained the former Act's principle-based approach to regulation while strengthening its privacy protections, promoting early intervention by agencies and enhancing the role of the Office of the Privacy Commissioner (**OPC**).

The key changes under the new Act included:

- increased OPC powers, including:
    - the ability to issue and enforce compliance notices; and
    - increased information gathering authority;
- the introduction of mandatory privacy breach reporting;
- strengthened requirements on cross-border disclosures of personal information;
- the introduction of new criminal offences; and
- permitting class actions in the Human Rights Review Tribunal by persons other than the Director of Human Rights Proceedings.

First use of compliance notice

The Privacy Commissioner may now issue a compliance notice to organisations or businesses that are not meeting their obligations under the Privacy Act. A compliance notice may require an organisation to do something, or to stop doing something, in order to comply with the Privacy Act.

On 15 September the OPC issued a compliance notice to the Reserve Bank, marking the first use of the new statutory power created under the Privacy Act.

In late December 2020, the Bank suffered a cyber-attack which impacted a third-party file sharing software used by the agency. The breach, which was reported to the OPC in January 2021, was said by the OPC to suggest there were systemic weaknesses in the Bank's systems and processes for protecting personal information.

Following the OPC's investigation, the Privacy Commissioner determined that the Bank had failed to adequately protect a subset of personal information held by the Bank.

The compliance notice issued to the Reserve Bank set out the steps the Bank must take within identified timeframes in order to address weaknesses in the Bank's systems and to comply with information privacy principle (**IPP**) 5, which relates to the storage and security of personal information.

This compliance notice indicates the OPC's desire to use the new tools available to it to deliver better privacy outcomes, the outgoing Privacy Commissioner John Edwards stating that the compliance notice "*provides a learning opportunity for the Bank, and for other agencies*".

The incident also highlights to businesses the importance of early engagement and having in place a clear road map to follow when faced with such an event. The Reserve Bank was commended by the OPC for promptly responding to the incident and working

One year on – a look at the Privacy Act 2020
(Continued)

collaboratively with the OPC, thereby potentially softening the possible PR fall out following the incident.

Businesses should ensure they prepare, implement and regularly test a privacy breach response plan which includes processes for managing and ensuring pro-active engagement with the OPC (including identification of those key individuals who will lead this engagement).

For further information, the OPC has published guidelines on compliance notices which can be viewed here.

Mandatory privacy breach reporting

As of 1 December 2020, an agency must notify the Privacy Commissioner and affected individuals if it is aware a notifiable privacy breach has occurred – a privacy breach being notifiable where is it is reasonable to believe the breach has caused serious harm or is likely to do so.

It is clear that during the first six months of the notification regime, the OPC's focus has been educating organisations to ensure they understand their new legal responsibilities. We are now seeing a greater use of the Privacy Commissioner's powers under the Privacy Act to investigate or enforce compliance where organisations repeatedly fail to meet their obligations or simply should have known better.

On 1 December, the OPC published a report which considered the impact of mandatory privacy breach reporting one year after the new Act came into effect.

Some key findings were:

- the OPC received a total of 697 privacy breach notifications between 1 December 2020 and 31 October 2020. This was four times the number of notifications dating 1 December 2019 to 31 October 2020;
- a third of all privacy breaches reported between 1 December 2020 and 31 October 2021 met the threshold for serious harm, suggesting organisations have been taking a predictably cautious approach to reporting in the new Act's early stages;
- over a third (35%) of serious breaches reported involved emotional harm; and
- the majority of serious breaches resulted from human error (mostly email error).

To date, organisations are generally notifying the OPC too late. While the Privacy Act is silent on the specific timeframe for notification, the OPC released guidance in June 2021 stating that, unless there are extenuating circumstances, notification to the OPC should be within 72 hours. The OPC's recent report found that currently less than half of all serious breach notifications are being made within that expected timeframe. Furthermore, by the time that the OPC had been notified, only 61% of agencies had contacted the affected individual. It is understandable that notification to affected individuals will often take longer than notification to the OPC, however, it is still a requirement under the Privacy Act. We are reminded that while there are exceptions for not notifying affected people, these are limited.

The OPC has released helpful online tools and practice guidance for organisations on dealing with privacy breaches, including:

- "NotifyUs", an online tool for organisations and businesses to work out if privacy breaches are notifiable and if so, to report the breach to the OPC; and
- blog posts on how the OPC has dealt with certain organisations to date who have suffered privacy breaches under the new regime.

One year on – a look at the Privacy Act 2020
(Continued)

Overseas disclosures

The inclusion of the new IPP12 in the Privacy Act introduced stronger protections relating to the transfer of personal information to entities or persons outside of New Zealand.

Generally speaking, under the new regime, an agency can disclose personal information to a foreign entity if:

- the individual concerned authorises the disclosure (after being informed that the destination does not have comparable privacy safeguards); or
- comparable privacy safeguards will apply (i.e. if the foreign entity is in a prescribed country (which will be set out in subsequent regulations) or is otherwise subject to contractual obligations that are comparable those under the Privacy Act).

An important clarification made under the Privacy Act is that the protections regarding overseas disclosures will not apply where information is transferred to a service provider solely for the purpose of safe custody or processing on behalf of the agency (i.e. to an overseas-based cloud storage provider). Accordingly, if a service provider is not using the transferred personal information for its own purposes, the transfer of personal information outside of New Zealand from an agency to the service provider will not constitute a disclosure of personal information for the purposes of IPP12.

Since the Privacy Act came into force, the OPC has created an online Principle 12 Decision Tree which takes users of the tool through a series of questions to help work out whether the protections regarding overseas disclosures apply to the information the user is disclosing and if so, whether the user is complaint with the regime.

The OPC has also released template model clauses and a Model Clause Agreement Builder which can be used if an agency is seeking to make an overseas disclosure on the basis that the foreign entity is contractually bound to protect the information by safeguards comparable to those provided under the Privacy Act.

The Model Clause Agreement Builder is a useful resource to assist small-to-medium size businesses navigate the intricacies of overseas transfers under the Privacy Act.

Human Right Review Tribunal decisions

Complaints received by the Privacy Commissioner under the Privacy Act may be escalated to the Human Rights Review Tribunal. The Tribunal has the same powers as a district court and can make binding decisions, award damages up to a maximum of $350,000 and order parties to pay costs.

The OPC has released a helpful blog post providing guidance on the approach the Tribunal has taken to date in awarding damages for emotional harm caused by a privacy breach. As damages are intended to be compensatory rather than punitive, complainants are less likely to be awarded damages if they cannot show that the harm was a direct result of the relevant privacy breach.

Where to from here?

While the Privacy Act introduced a number of new tools to encourage improved privacy practices, the Privacy Act did not materially increase penalties for non-compliance.

When discussing the Privacy Bill, the Privacy Commissioner commented that "*without real and meaningful consequences for non-compliance, rogue agencies will continue to thumb their nose at the regulation, meaning responsible organisations will disproportionately bear the cost of compliance, while cowboys will ignore their obligations*."

While monetary penalties under the Privacy Act remain comparatively low, privacy concerns remain front of mind for consumers and so the reputational impact of

One year on – a look at the Privacy Act 2020
(Continued)

suffering a privacy breach or receiving a compliance notice is likely to drive many businesses to ensure data protection remains a key focus point at the board level.

As public pressure to ensure the Privacy Act has sufficient teeth continues to rise, we will keep a close watching brief on developments in this space.

Want to know more?

If you have any questions, the Anderson Lloyd Team are available to assist and can be contacted here.