

Market Update

SEPTEMBER 2019

New Zealand's new Privacy Act edges closer

WHAT'S CHANGING?

The long-awaited legislative overhaul to New Zealand's privacy framework contained in the Privacy Act 1993 is on track for commencement on 1 March 2020. The Privacy Bill, which contains a comprehensive suite of reforms, has recently passed its second legislative reading.

New Zealand's new privacy framework will be based on the same OECD principles that underpin the likes of the EU's General Data Protection Regulation and Australia's Privacy Act 1988.



Mandatory notification of privacy breaches

Agencies (which the Bill defines widely to include any person or corporation, whether public or private) will need to notify privacy breaches that cause, or are likely to cause, "serious harm" to affected individuals. The Bill includes guidance on the factors agencies may consider when determining the likelihood of serious harm (clause 117A). Factors include the sensitivity of the personal information, the nature of any recipients and any actions taken by the agency to reduce the risk of harm. The timeframe for notification is "as soon as practicable".



Extra-territorial implications

The Bill has an extra-territorial effect, meaning it will apply to any action taken by an overseas agency "in the course of carrying on business in New Zealand". This is similar to the obligations of overseas agencies carrying on business in the EU's GDPR. Furthermore, for New Zealand agencies, the Bill proposes to apply to information collected and held both inside and outside New Zealand.



Increased powers for the Privacy Commissioner

The Bill grants stronger powers to the Privacy Commissioner to include the ability to issue binding decisions on access requests, conduct investigations, and to issue compliance notices to agencies who breach the Act or interfere with any of the Information Privacy Principles.



Confirmation of the existing privacy principles

The Bill reaffirms the 12 existing privacy principles. These include requirements that personal information is only collected for lawful purposes, is stored securely, and is not held for longer than required. The existing principles also include rights to access and correct personal information, as well as the right to receive information about processing of personal information. The new privacy principle (now principle 12 of 13) puts restrictions on the circumstances where personal information may be disclosed to persons or entities outside of New Zealand.

WHAT'S MISSING COMPARED TO OTHER JURISDICTIONS

The Privacy Commissioner had asked for wider enforcement powers, including the ability to fine organisations up to NZD1 million. At this stage fines are limited to NZD10,000 for particular infringements, including failure to notify privacy breaches.

While fines will be modest compared to other jurisdictions, if the Privacy Commissioner believes a further monetary penalty is appropriate, he or she will have the power to bring proceedings in the Human Right Review Tribunal against the agency in question. Affected individuals are also able to bring proceedings in the Tribunal for breach of privacy. Awards are available for both financial loss and distress (with damages up to \$350,000 available).

As well as increased fines, the Privacy Commissioner also sought a range of amendments that would bring the proposed regime closer to that seen in the EU. For example, the introduction of the right to data portability and the right to be forgotten. While these have not been included in the Privacy Bill, the Government has alluded to the fact that these rights and powers represent data privacy best practice and could be introduced in an update to the privacy regime in the coming years.

WHAT'S NEXT?

The Bill will now move on to the Committee of the whole house and then the third reading, where yet further changes could be made. At this stage the Bill contains a commencement date of 1 March 2020 and a timeframe for the introduction of mandatory reporting of privacy breaches will follow but is yet to be announced.

We recommend that agencies brace themselves for these changes by:

- 1) **Reviewing their privacy policies** to ensure compliance with the privacy principles;
- 2) **Preparing for mandatory notifications**, in particular making sure they have a cyber and data incident plan in place; and
- 3) **Considering the value cyber insurance could add** to their business. Civil Enforcement Awards and Pecuniary Penalties could result from breaches.

Need to know more?

For more information please contact us.



Mark Anderson

Partner & NZ Cyber Team Leader

T: +64 9 280 0524

mark.anderson@wottonkearney.com



Sierra Ryland

Senior Associate, Wellington

T: + 64 4 974 9280

sierra.ryland@wottonkearney.com



Joseph Fitzgerald

Senior Associate, Wellington

T: +64 4 499 5589

joseph.fitzgerald@wottonkearney.com

© Wotton + Kearney 2019

This publication is intended to provide commentary and general information. It should not be relied upon as legal advice. Formal legal advice should be sought in particular transactions or on matters of interest arising from this publication.