

NZ Privacy Act 2020 – Update 1

JULY 2020

AT A GLANCE:

- New Zealand's *Privacy Act 2020* will come into effect on 1 December 2020.
- The new legislation updates New Zealand's 27-year-old privacy framework.
- Insurers and insureds need to act now to get ready for these changes, which include mandatory notification requirements and extra-territorial jurisdictional scope.
- The risks of non-compliance include regulatory investigations, fines and exposure to compensation claims.

These significant reforms will change the way organisations in New Zealand manage privacy issues and data security.

What the new law means for insurers and their insureds

REFORM AT LAST

New Zealand's *Privacy Act 2020* passed its final parliamentary hurdle with unanimous support and received royal assent on 30 June 2020. The new law will be in force from 1 December 2020, creating new responsibilities for organisations in New Zealand.

The Privacy Act replaces 27-year-old legislation and implements a number of the changes adopted in comparable jurisdictions, such as the EU, Australia, and various US states.

THE KEY AREAS OF REFORM

The Privacy Act 2020 operates around the existing fulcrum of the information privacy principles, with the addition of one new principle addressing disclosures of information outside of New Zealand. The principles address how personal information may be gathered, stored, used and disclosed. While the new Act retains the principles, it makes a number of changes concerning how these principles are enforced and regulated.

1. *Mandatory notifications for privacy breaches*

If a privacy breach poses a risk of “serious harm” to affected individuals, agencies will have to notify the Privacy Commissioner and affected individuals. In assessing what constitutes “serious harm”, agencies need to consider factors such as the sensitivity of the personal information, the nature of any recipients, and any actions taken by the agency to reduce the risk of harm.

Guidance and further information on the factors to consider is provided in section 113 of the Act.

2. *Increased powers for the Privacy Commissioner*

The Act now gives the Privacy Commissioner the power to make:

- Compliance notices – these require agencies to comply with the new legislation, and carry non-compliance penalties of up to \$10,000, and
- Access directions – the Privacy Commissioner may direct an agency to provide an individual with access to their information. If an agency fails to comply, the individual in question can apply to the HRRT for an access order, which also carries a non-compliance penalty of \$10,000.

3. *Controls on disclosure of information overseas*

The new Privacy Act introduces a new information privacy principle concerning disclosure of personal information outside of New Zealand. This reform requires New Zealand organisations engaged in cross-border information transfers to ensure the overseas entities they are dealing with have similar levels of privacy protection to those in New Zealand. The obligations associated with this reform are similar to those imposed in other jurisdictions, including the EU's GDPR regime.

4. Criminal offences

There are new criminal offences in this space, which carry a maximum fine of \$10,0000, including offences for agencies that:

- fail to notify a privacy breach appropriately
- destroy personal information that has been requested, and
- otherwise obstruct, hinder or resist the Privacy Commissioner when they exercise powers under the new legislation.

5. Extra-territorial scope

The new Act also has extra-territorial jurisdictional scope, which applies to agencies that do not have a physical presence in New Zealand but carry on business within New Zealand. This means businesses now have an obligation to comply with the new legislation regardless of where they, or their servers, are based.

WHAT THIS MEANS FOR INSURERS AND THEIR INSURED

These significant reforms will change the way organisations doing business in New Zealand manage privacy issues and data security.

As has occurred in other jurisdictions with similar regimes, the reforms may also lead to a spate of privacy and data security related claims, including representative actions.

Before the law comes into effect, insureds and insurers – including overseas insurers with New Zealand insureds – should consider how these new obligations will affect the way they operate, and the potential exposure or liability they may cause.

Key steps insureds can take in preparing for the new regime include:

- reviewing privacy policies to ensure compliance with the privacy principles
- preparing for mandatory notifications, including ensuring there is a cyber and data incident response plan in place, and
- assessing whether the business would benefit from cyber insurance.

KEEPING YOU ACROSS THE ISSUES

Over the next few months, Wotton + Kearney will publish a series of updates about the Privacy Act and associated issues.

If you have any questions about the new legislation, require advice, or need help preparing a cyber and data incident response plan, please contact our team.

Need to know more?

For more information please contact our authors.



Mark Anderson

Partner & NZ Cyber Leader

T: +64 9 280 0524

mark.anderson@wottonkearney.com



Joseph Fitzgerald

Senior Associate

T: +64 4 260 4796

joseph.fitzgerald@wottonkearney.com



Sierra Ryland

Senior Associate

T: +64 4 974 9280

sierra.ryland@wottonkearney.com



Johnson Zhuang

Solicitor

T: +64 9 280 1499

johnson.zhuang@wottonkearney.com

© Wotton + Kearney 2020

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. Company no 3179310. Regulated by the New Zealand Law Society.