

CYBER GUIDANCE

SPECIAL EDITION

CHANGES TO NEW ZEALAND'S PRIVACY LAWS

DATE ISSUED: 1st October 2020

Changes to New Zealand's Privacy Act come into effect on 1st December 2020. This means that all businesses need to understand these changes, how they relate to their business and what are the mandatory requirements under the new laws. Replacing the Privacy Act 1993, this new privacy acts serves to strengthen protections around information management.

The following section will be divided into a breakdown of the new requirements, followed by acceptable remediation steps that may be taken in order to ensure compliance where applicable.

WHAT DOES THIS MEAN FOR YOU?

Reporting Privacy Breaches

Responsibility for the reporting of any breach of privacy now rests directly with the organization and those they engage with in respect to personal data collection, storage, and disclosure. Should your business become aware of a security breach that will or is likely to cause serious harm, those affected must be notified, along with the Office of the Privacy Commissioner.

What can you do?

Create and implement an in-house process to handle privacy breaches in a timely manner. This guide should contain step-by-step instructions for how to contain the breach, a metric of how to determine whether the breach must be reported to the Commissioner and those affected and a review phase to determine future protections against a similar occurrence. To determine what constitutes 'serious harm' as mentioned in the Act, considerations such as sensitivity of information, mitigation actions taken to reduce the risk of harm and what the nature of the repercussions for individuals may be.

Reach out to any partners, service providers or contractors to make sure they understand their obligations under the new privacy laws so that you are notified immediately of any breach, enabling you to undertake your containment and mitigation process as above.

Compliance Notices & Access Requests

In the event that a business is found to be non-compliant with the Act, the Privacy Commissioner has the ability to issue notices requiring any business to commence certain operations to obtain compliance, or cease certain operations if they are found to be non-compliant. The Privacy Commissioner will also assume the responsibility of making legally binding decisions surrounding complaints regarding access to information, such as requests of an individual to access their personal information, that would have previously fallen under the Human Rights Review Tribunal. However, the Commissioner's decisions may still be appealed through the Tribunal.

What can you do?

Appoint a Privacy Officer within your business whose responsibility it is to ensure your organization is meeting the mandatory privacy requirements.

Create and implement privacy management processes which will detail how the business will handle all personal information, including its collection, storage, how it is used and when it may be disclosed. Making sure you have a process in place to action requests to information within a reasonable timeframe is also essential. Engage with any service providers that assist with any of the above and ensure your expectations, processes and controls are aligned. This is particularly important in the event that the service provider is based offshore.

Cross-Border Protections

Any personal information being sent overseas is still subject to New Zealand's privacy laws. This also applies to any offshore provider wishing to engage with New Zealand businesses, as their compliance with the Act is also compulsory.

What can you do?

You must obtain permission from your customers before sharing any of their personal information with a third party. This include suppliers, service providers and advertisers. This is most easily done by updating your company's privacy policy and terms and conditions of service.

When using any overseas providers, making sure their understanding and compliance with New Zealand's privacy laws is crucial and take into consideration their history around privacy and data breaches. Make sure all current contracts are updated and amended to fit with the new requirements.

In any instance that an overseas provider does not comply with the New Zealand Privacy Act, full disclosure must be given to all parties and individual involved and their permission to continue service must be obtained.

WHAT ARE THE RISKS?

Criminal Liability

Failure to report a data breach, destruction of requested personal information if a request has been made to release it and misleading an agency in a manner that may affect another person's information (including impersonation) could all result in a fine of up to NZD\$10,000.

The Privacy Commissioner is also able to dictate a reasonable timeframe in which an agency must comply with any investigations and non-compliance may result in fines from NZD\$2,000 – NZD\$10,000

Class Action

Anyone other than the Director of Human Rights Proceedings may undertake class action through the Human Rights Review Tribunal relating to privacy breaches. These proceedings may result in the complainant being awarded up to NZD\$350,000.

Your Reputation

Under the new Act, the Privacy Commissioner has the right to publicly identify any business that is found to be in breach of the Privacy Act 2020

REFERENCES & RESOURCES

For more information surrounding the Act and the Act itself, please visit the links below:

Privacy Commissioner: <https://www.privacy.org.nz/blog/key-changes-in-the-privacy-act-2020/>

Ministry of Justice: <https://www.justice.govt.nz/justice-sector-policy/key-initiatives/privacy/>

New Zealand Legislation: <http://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html>