MARSH

Client Briefing

NOVEMBER 2019

#Cyber2020 – New Zealand's Privacy Fightback

New Zealand's Privacy Bill, which is on track for commencement on 1 March 2020, ushers in a new era for privacy in New Zealand that will promote data transparency and accountability across the whole economy. This is a long-awaited legislative overhaul to New Zealand's current Privacy Act 1993.

The new privacy framework intends to set the required standards and expectations on data handling fit for a digital economy, with the long term goal being a positive change in behavioural norms. Knowing that these changes are on the horizon, New Zealand businesses should start preparing now.

Key Changes in the Privacy Bill

- **Mandatory Notifications** – Moving away from our current voluntary notification framework, any public or private entity that holds personal information (defined as 'Agency' in the new bill), will be required to notify affected individuals of a data or privacy breach which may likely cause them serious harm – this may be 'harm' beyond just financial loss, such as humiliation or loss of dignity. Agencies will also be required to notify the Office of the Privacy Commissioner (OPC) as soon as practicable to engage with any further regulatory conversations.
- **Increased Power for the Privacy Commissioner** – The Bill will grant stronger powers to the OPC which include the ability to issue binding decisions on data access requests, conduct investigations, and to issue compliance notices to agencies who breach the Act (such as non-notification) or interfere with any of the Privacy Principles in the Act.
- **Extra-Territorial Implications** – To fit the global data economy of the 21st century, the Bill carries an extra-territorial effect, which means it will also apply to any action taken by an overseas agency 'in the course of carrying on business in New Zealand.' Additionally, for New Zealand agencies, the Bill proposes to apply to data collected and held both inside and outside New Zealand, meaning that storing data offshore will not be a defence for non-compliance. There will also be guidelines on the circumstances where personal information may be disclosed to persons or entities outside of New Zealand.

Practical Implications for New Zealand Businesses

- Businesses will need to regularly review and assess the data they collect on individuals; where and how securely it is being stored; and how individuals could be impacted in the event of a breach. Managing privacy risk may demand time, attention and potentially more expenses depending on the size and scale of an organisation.
- The introduction of mandatory notifications will result in a significant increase of forensic investigation and determination costs, even when a data breach may appear 'minor' at face value. For example, a business email compromise where data does not appear to be exfiltrated on the dark web (and therefore unlikely to cause 'serious harm') may require lengthy and thorough forensic work under the new regulatory framework to have full assurance that the breach falls does in fact fall under the notification threshold.
- For breaches that do require notification, the notification process can be costly – especially if ongoing identity monitoring for affected individuals is required.
- The Bill will empower individuals to value the data they are providing organisations and demand transparency and accountability. Changing attitudes towards privacy and public awareness of the potential consequences of a privacy breach may also result in third-party liability claims and class-actions lawsuits – despite New Zealand still being less litigious than other jurisdictions.

Quick tips to be ready

- **Engage with the OPC** to find out what may be expected of you and your organisation going forward – they are very willing to assist businesses in preparation for the new standards. The OPC website also contains a wealth of resources to keep you up-to-date on the law reforms.
- **Review and test your incident response plan**s so that you have clarity over what to do when a privacy breach is discovered. This may include having external vendors readily available or knowing how to trigger your cyber insurance policy if you have one in place.
- **Consider transferring some of your risk to a cyber-insurance policy** if you are currently uninsured in this regard. Cyber insurance policies widely respond to the fallout from privacy breaches and are built for the modern digital risk landscape. It can greatly reduce your financial burden to determine the extent of, and recover from, a notifiable breach.

Your Marsh broker can provide more information regarding how Cyber insurance can play a valuable role in offsetting the upcoming shift in New Zealand's privacy landscape.

JONO SOO
Head of Cyber Specialty – New Zealand
jono.soo@marsh.com