MARSH

May 2018

CLIENT ALERT

IMPLICATIONS OF THE PRIVACY BILL

The Privacy Bill has just passed its first reading in the House of Representatives. It has been introduced to update New Zealand's privacy laws, bringing them in line with recent international developments and regulations. Australia implemented similar laws in late February this year and by mid-May there have been 108 breaches reported to the Privacy Commission, proving a growing importance of privacy concerns to an increasingly connected world.

The introduction of the EU GDPR (Global Data Protection Regulation) on 25 May 2018 will also mark the biggest overhaul of privacy regulations in Europe for two decades, putting much more onus on businesses to protect the personal data of EU citizens.

The updated Privacy Act is an attempt to develop more accountability and responsibility with respect to cyber security and protecting personal information. The main impact of the Bill will be the introduction of mandatory notification to the Privacy Commissioner (Commissioner) and affected individuals following a privacy breach.

The insurance market is responding to the increased risk by developing more comprehensive cyber insurance plans, tailored to the different risk profiles of companies.

BACKGROUND ON LEGISLATIVE CHANGES

The Privacy Bill requires an agency (any person or body of persons) to report to the Commissioner any notifiable privacy breach as soon as practicable after becoming aware of the breach. Agencies must additionally notify the affected individuals of a breach, or make a public notice.

The Bill seeks to strengthen cross-border data protection by ensuring the international disclosure of personal information is done within a jurisdiction with comparable privacy laws to New Zealand, ensuring acceptable privacy standards are maintained worldwide.

Failure to comply with the above could result in a fine of up to $10,000.

Furthermore, the statutory power of the Commissioner has been significantly extended. The Commissioner can issue compliance notices to agencies that breach the Act, enforce binding decisions resulting from complaints and publish an agency's identity without consent, if they deem it within the public interest to do so.

WHAT IS A 'NOTIFIABLE' PRIVACY BREACH?

A notifiable privacy breach is the unauthorised exposure or withholding of personal information, either caused by a person inside or outside an agency, that could cause harm to an individual.

Examples of personal information include health information, employee records, tax file numbers and credit information.

WHAT IS THE NOTIFICATION PROCESS?

1) Notify the Commissioner:

- Describe the nature of the privacy breach, the affected individuals and suspected cause of the breach.
- State the intended response to the breach and what relevant parties will be contacted.

2) Notifying the affected individuals:

- Describe the privacy breach, the intended response and state any initial steps the individual can take to avoid/mitigate further harm.
- Confirm the Commissioner has been notified and inform the individual of their right to make a complaint to the Commissioner.

CRIMINAL OFFENCES

Additionally, several new criminal offences have been introduced by the Privacy Bill:

- Providing false information to anyone exercising power under the Privacy Act.
- Falsely representing an authority under the Privacy Act.
- Impersonation or false pretense for the purpose of gaining access to an individual's personal information.
- Knowingly destroying personal information that is subject to a request.

Any person who commits one of the above offences will be liable for a fine of up to **$10,000**.

It must be noted that the Privacy Bill is still in the House and is by no means finalised. The Commissioner is expected to push for further reform in the Select Committee, before the second reading.

THIRD PARTY SERVICE AGREEMENTS

In preparing for the Privacy Act update, it is critical for an organisation to review its third party supplier relationships to establish where notification responsibilities would lie in the event of an eligible data breach. Personal information will still be considered held by 'agency A' if another agency (B) holds the information as an agent, for the purpose of safe guarding or processing the information, on behalf of agency A.

When entering into new contractual arrangements or reviewing existing ones, a business should ensure clear procedures are established for complying with the Privacy Act. Generally speaking, it is recommended that the agency with the most direct relationship with the individuals at risk of serious harm, be the one to notify.

REGULATION RISKS

In addition to the regulatory implications following a data breach, a business may also face legal liability arising from third party litigation. This may result from a breach of confidentiality obligations that are owed to customers, who can pursue the agency for financial compensation following loss or theft of their personal information.

INSURANCE RESPONSE

The update in Privacy regulations and legislation around the world recently has no doubt been encouraged by rapid technological developments and subsequently cyber security over the past few decades. A cyber insurance policy can address these issues, including the increased onus on privacy protection, but should not act as the only solution for managing a company's exposure to cyber-attacks or data breaches.

Mitigating cyber risk through insurance plays an important role in the overall risk management framework of a business, though it should be treated as a last resort. There are many costs that may impact a company in the event of a privacy breach and insurance can assist in providing support for these costs. Some examples are shown in the following table:

DATA BREACH CONSEQUENCE	FINANCIAL COST / LOSS	CYBER INSURANCE PROTECTION
IT forensic costs to assess and remediate the data breach	Expected	Yes
Notification costs incurred in advising affected individuals	Expected	Yes
Legal costs to notify regulators (breach coach)	Expected	Yes
Ongoing credit monitoring services to affected individuals	Expected	Yes
PR costs to assist in reducing damage to brand	Expected	Yes
Legal defence costs and damages for liability claims arising from affected individuals	Possible	Yes
Payment Card Industry (PCI) fines or assessments	Possible if breached data includes credit card information	Yes
Extortion demands	Possible	Yes

** the above summary represents a general overview of available insurance coverage and should not be relied upon in the event of a claim. Please refer to the specific terms and conditions of your insurance policy for full terms and conditions.*

WHAT NEXT?

In summary, the upcoming changes to the Privacy Act will strengthen NZ legislation to make it more 'in-line' with its international counterparts as the world progresses further into the digital age. However, we feel the proposal after the first reading is currently light on penalties, and should be as close to the GDPR with its strict requirements in order to harmonise the compliance measures that businesses will need to put in place worldwide. Working towards an agreed global standard would be the logical next goal.

Marsh prides itself facilitating the stability and growth of New Zealand business by providing well-tailored insurance programmes to suit different requirements. Where Marsh excels is in providing additional risk-led advice and to fully understand your level of cyber resiliency. Please contact your Marsh broker on **0800 627 744** to discuss where you stand in the world of cyber risk, how you can work to mitigate it, or to discuss insurance options.