Carter Newell LAWYERS

Cyber Risk Newsletter

February 2017

Need to Know – Australia's New Data Breach Notification Laws

Katherine Hayes , Senior Associate

Greg Stirling, Associate

The Privacy Amendment (Notifiable Data Breaches) Bill 2017 (**bill**) amends the *Privacy Act 1988* (Cth) (**Privacy Act**) and imposes an obligation on businesses to notify individuals and the Information Commissioner of data breaches. While the introduction of a mandatory data breach notification regime is significant, the threshold for notification is quite high.

When will it take effect?

The notification laws are expected to come into effect within the next 12 months. The bill was passed by both houses of parliament on 13 February 2017 and is currently awaiting Royal Assent.

Who is affected?

All entities that are currently subject to the Australian Privacy Principles (**APP entity**) in the Privacy Act, which includes:

- Australian Government agencies;
- all businesses and not-for-profit organisations with an annual turnover for the previous year of more than $3 million;
- health service providers, or holders of health information (subject to the operation of the *My Health Records Act 2012* (Cth));
- credit reporting bodies; and
- holders of one or more individuals' tax file numbers.

Also, if an APP entity has provided personal information to an overseas entity, these notification obligations may still apply as if the APP entity itself held the information.

What are the notification requirements?

An *'eligible data breach'* is central to this legislation. An eligible data breach happens if:

- there is unauthorised access, disclosure or loss of, **personal information** held by an APP entity; and
- a reasonable person would conclude that the access, disclosure or loss is likely to result in **serious harm** to any of the individuals to whom the information relates.

'Personal information' means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not. Common examples may include individuals' dates of birth, addresses and credit card details.

'Serious harm' imposes a fairly high threshold, and is where a reasonable person would conclude that access to, or disclosure of, personal information would be likely

to result in serious harm, taking into account a range of specified matters[1] including:

- the kind of information and its sensitivity;
- the persons who have obtained the information through the breach;
- whether the information was encrypted; and
- the nature of the harm.

The Office of the Australian Information Commissioner has previously considered *'serious harm'* to include identify theft and financial fraud.[2]

There are three categories of obligation surrounding an eligible data breach.

Suspected breach

Within 30 days of an APP entity suspecting that there may have been an eligible data breach it is obliged to carry out a reasonable and expeditious assessment of whether there in fact has been such a breach.

Actual breach

If an APP entity has reasonable grounds to believe that an eligible data breach has happened, it must notify:

- affected individuals; and
- the Information Commissioner.

An APP entity is also required to provide such notification if directed to do so by the Information Commissioner.

Remedial action

If an eligible data breach occurs, and the APP entity takes action before the breach results in serious harm to any of the affected individuals, then the breach is deemed to have not been an *'eligible data breach'* and no notification steps are required.

The notification

The APP entity's notification to the Information Commissioner and the affected individuals must be provided as soon as practicable after the APP entity becomes aware of the breach, and must contain:

- the identity and contact details of the APP entity;
- a description of the eligible data breach;
- the kinds of information concerned; and
- recommendations of the actions that the affected individuals should take in response to the eligible data breach.

What are the consequences of non-compliance?

If an entity or individual does not comply with the requirements of the legislation, they risk facing civil penalties of up to $1.8 million or $360,000 respectively or compensation orders to individuals who have suffered loss or damage as a result of the non-compliance.

What do I need to do?

If these amendments are likely to impact your organisation, we recommend action be taken now to prepare for the commencement of the bill. Such action may include implementing:

- the Australian Signals Directorate's recently introduced ***'Essential Eight'*** strategies to mitigate cyber security incidents; and
- a data breach response plan, such as the example plan on the website of the **OAIC**.

We also recommend a whole-of-business approach towards minimising cyber risks and the associated fall-out from a cyber event should be taken. As part of this, companies should consider how their present insurance coverage responds to cyber events and whether obtaining specialised cyber risk insurance coverage is necessary, particularly in light of the impending commencement of the bill.

.....

[1] See s 26WG of the bill.
[2] See, for example, the **Data Breach Notification Guide,** published on the OAIC's website in August 2014.

Authors

Katherine Hayes
Senior Associate

P: (07) 3000 8349
E: khayes@carternewell.com

Greg Stirling
Associate

P: (07) 3000 8366
E: gstirling@carternewell.com