New data breach notification laws are on the way

WORDS BY CARTER NEWELL PARTNER, MICHAEL GAPES

*On 13 February 2017, the **Privacy Amendment (Notifiable Data Breaches) Bill 2016** was passed. It is currently awaiting Royal Assent, but is expected to come into effect within the next 12 months.*

In this article, we will briefly address some key aspects of the new legislation. More detailed information, including our best practice recommendations as to how to ensure that your agency complies with the new legislation, will be provided once a commencement date is known. In addition, training will also be offered to REIQ members.

Who does the new legislation apply to?

The new legislation will apply to entities that are currently subject to the *Australian Privacy Principles* (**APP entity**) in the *Privacy Act*, which includes:

- Australian government agencies (excluding state and local government);
- all businesses and not-for-profit organisations with an annual turnover in excess of $3 million;
- health service providers or holders of health information;
- credit reporting agencies; and
- holders of one or more individuals' tax file numbers.

So what is a data breach?

An "*eligible data breach*" happens if:

- there is unauthorised access to, or unauthorised disclosure 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*" is defined as meaning information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not. Some examples may include individuals' dates of birth, addresses and credit card details.

"*Serious harm*" is not specifically defined in the new legislation, but is likely to capture a broad range of physical, psychological, emotional, economic and financial harm. However, the new legislation sets out a number of considerations in determining whether access to, or disclosure of, personal information would be likely to result in serious harm. These factors include the kinds of information involved in the breach and its sensitivity, the individuals who have obtained the information through the breach, whether the information is protected by one or more security measures and the nature of the harm.

So what action is necessary in the event of a breach?

There are varying obligations surrounding an eligible data breach.

For instance, an APP entity which suspects that there *may* have been an eligible data breach is required, within 30 days, to carry out a reasonable and expeditious assessment of whether in fact there has been such a breach.

However, if an APP entity has reasonable grounds to believe that an eligible data breach has in fact already occurred, it is required to notify:

- the affected individuals; and
- the Information Commissioner.

Note, however, that if an eligible data breach has occurred, and the APP entity has taken action before the breach results in serious harm, then the breach is deemed to have not been an "*eligible data breach*" and no notification is required.

Notification to the Information Commissioner of a data breach

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 a breach. The notification statement must include:

- the identity and contact details of the APP entity;
- a description of the breach;
- the kinds of information concerned; and
- recommendations about what affected individuals should do in response to the breach.

Penalties

If an APP entity or individual does not comply with the legislation, they could be faced with 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.

Next steps

As indicated above, the legislation is likely to come into force within the next 12 months. When a commencement date is known, further information and training will be provided to REIQ members.