Teddington
The Law of Business

Privacy Act changes on the way!

Unlike many other jurisdictions, Australia does not currently have a mandatory data breach notification regime (ie legal requirements imposed on organisations to notify impacted individuals and/or relevant regulators where personal information an organisation holds about an individual is subject to a data breach or other similar incident).

In February this year, the Privacy Amendment (Notifiable Data Breaches) Bill 2016 was passed by the Parliament.

The Bill amends the Privacy Act and establishes a regime requiring organisations to notify he Australian Information Commissioner and affected individuals about 'eligible data breaches'. This regime will commence on 22 February 2018 unless brought forward by the Parliament.

The requirements affect all entities that are currently required to comply with the Australian Privacy Principles under the Privacy Act 1988 (Cth); private organisations with an annual turnover of more than $3 million, Commonwealth Government Agencies and, a number of other entities including credit reporting bodies, credit providers, and file number recipients.

NEW REQUIREMENTS

Entities must notify affected individuals, as well as the Privacy Commissioner, when Entities become aware that there are reasonable grounds to believe that an '***Eligible Data Breach***' has occurred in relation to that Entity.

Under the Act an ***Eligible Data Breach*** occurs where:

- there has been unauthorised access to, or disclosure of, personal information and a reasonable person would conclude that there is a likely risk of serious harm to any of the affected individuals as a result of the access or disclosure; or
- personal information is lost in circumstances that are likely to give rise to unauthorised access to, or disclosure of, the information and a reasonable person would conclude that there is a likely risk of serious harm to any of the affected individuals.

In determining whether access to or disclosure of information would ***reasonably be likely*** to result in ***serious harm***, various matters are taken into account, including:

- the kind or kinds, and sensitivity, of the information
- whether the information is protected by one or more security measures, and the likelihood that those measures could be overcome
- the person or the kinds of persons who have obtained or could obtain the information
- the likelihood that any persons who could obtain information that has been secured by making it unintelligible or meaningless to unauthorised persons may also have the means to circumvent that security, and
- the nature of the harm.

Teddington Pty Ltd
Suite 415, 410 Elizabeth Street, Surry Hills NSW 2010
teddingtonlegal.com.au

Teddington
The Law of Business

NOTIFICATION

Under the notification regime:

- entities that have reasonable grounds to suspect that an eligible data breach has occurred will be required to carry out a reasonable and expeditious assessment of the suspected data breach.
- The Entity will need to take reasonable steps to ensure the assessment is completed within 30 days of the organisation becoming aware of the suspected data breach; and
- following such assessment organisations will (subject to any exceptions) be required to notify the Commissioner and affected individuals where the organisation has, or suspects there are, reasonable grounds to suspect that an 'eligible data breach' has in fact occurred. This would require the organisation to:
    - prepare a statement setting out the organisation's identity and contact details, a description of the breach, the kind of information concerned, and recommendations about what individuals should do in response to the breach;
    - give a copy of the statement to the Commissioner;
    - if practicable, take reasonable steps to notify the contents of the statement to each of the individuals to whom the relevant information relates or are at risk from the breach; and
    - if not practicable to notify affected individuals, publish a copy of the statement on the organisation's website (if any) and take reasonable steps to publicise the contents of the statement.

Where an organisation has taken remedial action to address potential harm to individuals that may arise due to a relevant data breach before any serious harm is caused to individuals to whom the information relates, the mandatory notification obligations will not apply.

INFORMATION HELD BY OVERSEAS RECIPIENTS

The new requirements apply to information held on behalf of an Entity by an overseas recipient, as though the information was directly held by the Entity. Therefore, an eligible data breach that occurs in relation to the overseas recipient will be deemed to have occurred in relation to the Entity.

PENALTIES

A failure to comply with the new laws could result in fines of up to $360,000 for individuals, and $1.8 million for businesses.

RECOMMENDATIONS

Entities that are required to comply with the Privacy Act should start preparing for the commencement of the notification regime;

APP entities should develop processes for detecting, containing and managing data breaches and all entities should prepare a **Data Breach Response Plan**.

Mark Gardiner, of Teddington Legal has assisted many companies with their Privacy Act requirements and is well placed to advise and assist companies to be ready for this significant legislative change.

Mark Gardiner
LEGAL DIRECTOR
02 8096 8143
mark@tt.legal

Teddington Pty Ltd
Suite 415, 410 Elizabeth Street, Surry Hills NSW 2010
teddingtonlegal.com.au