ON 13 FEBRUARY 2017 THE AUSTRALIAN GOVERNMENT PASSED THE PRIVACY AMENDMENT (NOTIFIABLE DATA BREACHES) BILL 2017.

Date: 15 February 2017

By: Cameron Abbott, Rob Pulham, Allison Wallace

WHO DOES THIS AFFECT?

The new requirements affect all APP entities i.e. any entity that is currently bound to comply with the Australian Privacy Principles under the *Privacy Act 1988* (Cth), including Commonwealth Government Agencies and private organisations with an annual turnover of more than AUD3 million, as well as a limited number of other entities including credit reporting bodies, credit providers, and file number recipients (together, **Entities**).

WHAT ARE THE 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.

An ***eligible data breach*** is either:

- unauthorised access to or disclosure of the relevant information, where the access or disclosure would ***reasonably be likely*** to result in ***serious harm*** to any of the individuals to whom the information relates, or
- loss of information in circumstances where unauthorised access to or disclosure of the information is likely to occur, and assuming that it were to occur, that access or disclosure would ***reasonably be likely*** to result in ***serious harm*** to any of the individuals to whom the information relates.

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.

If an Entity is aware that there are reasonable grounds to believe that an eligible data breach has occurred, the Entity must prepare a statement setting out specified details and notify both the Privacy Commissioner and the affected individual(s). If it is not practicable to notify affected (or at risk) individuals, the Entity is required to publish the statement on its website.

If an Entity suspects an eligible data breach may have occurred, but is not aware of reasonable grounds to believe the relevant circumstances amount to an eligible data breach, the Entity must investigate and within 30 days determine whether there are reasonable grounds to believe that an eligible data breach has occurred, and therefore, whether notification is necessary.

WHAT ABOUT 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.

This obviously makes it important for Entities to understand what information is held on their behalf by overseas service providers, and to ensure that there are appropriate contractual arrangements in place to enable them to comply with these new requirements.

However, it is not yet clear whether an overseas recipient's awareness of a breach will be imputed to the Entity, and therefore whether the requirement to notify of eligible data breaches applies in circumstances where the overseas recipient is aware of the breach, but the Entity is not. Depending on the types of information an overseas recipient holds on its behalf, an Entity may be justified in taking a conservative approach to this issue when contracting with overseas recipients, at least until the Privacy Commissioner's approach to the enforcement of this issue becomes clearer.

ARE THERE ANY EXCEPTIONS?

If an Entity takes action in relation to unauthorised access or disclosure before that access or disclosure results in serious harm to the individuals to whom that information relates, and a reasonable person would conclude that as a result of the action the access or disclosure would not be likely to result in serious harm to any of those individuals, then an eligible data breach will be deemed not to have occurred.

ARE THERE ANY PENALTIES?

A failure to comply with the new laws could result in monetary fines of up to AUD360,000 for individuals, and AUD1.8 million for businesses.

At the time of passing the legislation no specific date has been set for when the new requirements will come into effect, but we expect them to come into effect within the next 12 months.

KEY CONTACTS

CAMERON ABBOTT
PARTNER
MELBOURNE
+61.3.9640.4261
CAMERON.ABBOTT@KLGATES.COM

ROB PULHAM
SPECIAL COUNSEL
MELBOURNE
+61.3.9640.4414
ROB.PULHAM@KLGATES.COM

ALLISON WALLACE
LAWYER
MELBOURNE
+61.3.9205.2095
ALLISON.WALLACE@KLGATES.COM

