GILBERT +TOBIN

# MANDATORY DATA BREACH NOTIFICATION ARRIVES IN AUSTRALIA: A REVIEW OF THE AUSTRALIAN PRIVACY AMENDMENT (NOTIFIABLE DATA BREACHES) ACT 2017

17 FEBRUARY 2017

PETER G LEONARD, PARTNER, GILBERT + TOBIN LAWYERS

*On 13 February 2017 the Federal Parliament enacted the Privacy Amendment (Notifiable Data Breaches) Act 2017, inserting mandatory data breach notification requirements into the Privacy Act 1988. These provisions will replace the voluntary data breach notification guidelines as currently administered by the Privacy Commissioner and require entities subject to the Privacy Act to notify the Privacy Commissioner and affected individuals if the entity experiences a data breach of a kind covered by the Act. We review the new requirements below.*

The Australian Privacy Principles (**APPs**) in the Australian federal Privacy Act 1988 (**Privacy Act**) apply to APP entities, relevantly including businesses carried on in Australia that collect or hold personal information In Australia (whether or not collected from Australian residents), Australian corporations wherever they do business and most Australian Government agencies. An entity may carry on business in Australia without necessarily having a point of physical presence in Australia and may be taken to collect information in Australia where the solicitation for collection is made from outside Australia and the information is provided pursuant to this solicitation from within Australia. As Australian privacy professionals will know, there is a small business exception to the general operation of the Privacy Act for private sector organisations in corporate groups with less than AU$3 million consolidated group annual revenue, although this small business exception is itself subject to a number of exceptions, bringing within the Act smaller businesses that are private health service providers, that sell or purchase personal information or that are operating under Australian Government agency contracts.

Australian privacy professionals will also be familiar with the APPs unusual 'accountability principle'. The combined operation of APP 8.1 and section 16C of the Privacy Act has the effect that generally (some limited exceptions are available in APP 8.2) an APP entity that discloses personal information to an entity outside Australia that is not itself an APP entity remains responsible for ensuring that the recipient entity complies with privacy standards equivalent to the APPs, and that APP entity is liable (accountable) to affected individuals if the recipient organisation does not. This concept had been picked up in the mandatory data breach notification provisions, such that the APP entity must make relevant notifications if the recipient entity is subject to data breach of a kind covered by the Act: in such a circumstance the APP entity is deemed to hold the information that was subject to the data breach: new section 26WC.

The core obligation as to information security arises under APP 11 - security of personal information requires APP entities to take such steps as are reasonable in the circumstances to protect personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. Other provisions of the Privacy Act create equivalent obligations in relation to credit reporting information, credit eligibility information and tax file number information.

The new Act supplements the operation of APP 11 by inserting a new Part IIIC in the Privacy Act as a new mandatory data breach notification scheme for APP entities, including credit reporting bodies, credit providers and tax file number recipients. The relevant provisions are to be subject to a transitional regime and some requirements may not fully commence for 12 months after the Act commences operation: it is not yet clear just when the transition will be proclaimed as completed.

Where relevant entities experience an 'eligible data breach' that satisfies certain conditions, the data breach is 'notifiable'. Only very limited exceptions will be available. These exceptions include a public interest exception of avoiding prejudicing the activities of law enforcement agencies or disclosing information where that disclosure would be inconsistent with a secrecy provision in another law.

Entities may also apply to the Privacy Commissioner for an exception from the notification requirement, either altogether or for a specific period of time. The Commissioner has an additional power to direct an entity to notify an eligible data breach.

Note that an APP entity may have fully complied with its obligation under APP 11.1 to take reasonable steps to secure personal information it holds and nonetheless be subject to a notification requirement in relation to an eligible data breach. For example, an entity may experience a eligible data breach due to human error or other circumstances that are not reasonably foreseeable. In such cases notification must be given.

An eligible data breach is where there is unauthorised access, unauthorised disclosure or loss of personal information, credit eligibility information or tax file number information, that a reasonable person would conclude is likely to result in serious harm to any of the individuals to whom the information relates: new section 26WE(2).

Where an entity has reason to suspect that an eligible data breach may have occurred, the entity is required to undertake a reasonable and expeditious assessment of the circumstances and in any event take all reasonable steps to complete that assessment within 30 days: new section 26WH.

If an entity complies with this assessment requirement in relation to an eligible data breach of the entity and the access, disclosure or loss that constituted the eligible data breach of the entity is also an eligible data breach of one or more other entities: section 26WJ. This somewhat complex exception is intended to apply in cases where more than one entity jointly and simultaneously holds the same particular record of personal information, for example, due to outsourcing, joint venture or shared services arrangements between entities. The intended effect is that only one assessment under section 26WH needs to be undertaken into a single eligible data breach, regardless of how many entities hold the record of information. A corresponding overlap provision addresses the notification requirements and ensures that only one of the multiple entities must give notification to the Commissioner and affected individuals: new section 26WM.

In determining whether a reasonable person would conclude that an access or disclosure would or would not be likely to result in serious harm to any of the individuals to whom the information relates, specified factors to which regard should be had include the kind or kinds of information; the sensitivity of the information; whether the information is protected by one or more security measures and if so the likelihood that any of those security measures could be overcome; the persons, or the kinds of persons, who have obtained, or who could obtain, the information; if a security technology or methodology was used in relation to the information and was designed to make

the information unintelligible or meaningless to persons who are not authorised to obtain the information, the likelihood that the recipients have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology; and the nature of the harm: new section 26WG.

If an entity has reasonable grounds to believe they have experienced an eligible data breach, after an assessment or otherwise, the entity must notify the Information Commissioner and affected individuals. Reasonable grounds may be either direct evidence or indirect inference: for example, a pattern of complaints may provide the entity reasonable grounds to believe that an eligible data breach of the entity has occurred.

An exception applies where an entity can determine with a high degree of confidence that it has taken action to remediate the harm arising from an eligible data breach before that harm has occurred, such that a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to any of the individuals to whom the information relates: new section 26WF.

The form of notification to the Privacy Commissioner will be a 'subparagraph 26WK(2)(a)(i) statement'. Required information includes the identity and contact details of the entity; a description of the eligible data breach that the entity has reasonable grounds to believe has happened; the kind or kinds of information concerned; and recommendations about the steps that individuals should take in response to the data breach. The recommendations are intended to provide individuals whose information has been compromised in an eligible data breach with general advice about steps they should take to mitigate the harm that may arise to them as a result: for example, recommending that individuals request a copy of their credit report if an eligible data breach might result in credit fraud.

Notification of the contents of the subparagraph 26WK(2)(a)(i) statement must also be given to affected individuals. There are three alternative requirements or options, subject to 'practicability'. Practicability involves consideration as to the time, effort or cost of a particular form of notification, when considered in all the circumstances of the entity and the data breach. An entity must either:

+ if it is practicable to do so, take such steps as are reasonable in the circumstances to notify each of the individuals to whom the relevant information compromised in an eligible data breach relates, or
+ if it is practicable to do so, take such steps as are reasonable in the circumstances to notify those individuals who are considered to be 'at risk' of serious harm from the eligible data breach, or
+ if it is not practicable to notify via either of the above two methods, notify the statement by publishing the statement on the entity's website and taking reasonable steps to publicise the statement. For example, if it is reasonable to do so, an entity could take out multiple print or online advertisements (which could include paid advertisements on social media channels), publish posts on multiple social media channels, or use both traditional media and online channels.

An entity might choose to notify a statement under the first option if it would require an unreasonable volume of resources for the entity to assess which affected individuals are 'at risk' from an eligible data breach and which are not. An example might be an eligible data breach involving unauthorised access to a customer database containing varying amounts of personal information about a large number of individuals, where only some of those individuals might be 'at risk' due to the eligible data breach. Notification to the entire cohort of individuals may reduce the cost of compliance for the entity, and would also allow each individual who is notified of the contents of the statement to consider whether they need to take any action in response to the eligible data breach.

An entity might choose to notify a statement under the second option when the entity is able to ascertain with a high degree of confidence that only some particular individuals are 'at risk' from the eligible data breach. For example, if the entity was able to determine that the only likely result of serious harm from the eligible data breach would involve payment information stored in relation to a specific subset

of the broader 'cohort' of individuals such that only that subset is 'at risk' from the eligible data breach, the entity might choose to notify the contents of the statement to those individuals only.

Entities must comply with the obligation to notify individuals as soon as practicable after preparing the subparagraph 26WK(2)(a)(i) statement and providing it to the Privacy Commissioner. Where an entity normally communicates with an individual using a particular method, any notifications provided to the individual may use that method. Where there is no normal mode of communication with the particular individual the entity must take reasonable steps to communicate with him or her. Reasonable steps could include contact by email, telephone or post.

The Commissioner has a constrained power to grant an exemptions in the public interest from the requirement to provide notification to affected individuals: new section 26WQ. Examples of such public interest are where there is a law enforcement investigation being undertaken into a data breach and notification would impede that investigation, or where the information concerns matters of national security.

The mandatory data breach notification scheme is connected to the existing enforcement framework under the Privacy Act. This means that the Privacy Commissioner's existing investigatory powers will apply in the event that an entity breaches a requirement of the scheme. The Commissioner may investigate possible noncompliance with the mandatory data breach notification scheme and potentially make a determination requiring the entity to remedy such noncompliance. In the case of serious or repeated noncompliance, the Commissioner may also apply to a court to impose a civil penalty.

The Privacy Amendment (Notifiable Data Breaches) Act 2017 was significantly amended from earlier draft bills following criticism of drafting deficiencies and ambiguities in these earlier drafts. The mandatory data notification scheme as enacted is easier to understand and apply. Australian privacy professionals will know that the Office of the Australian Information Commissioner already receives voluntary data breach notifications and has extensive experience in assessing such notifications. The Commissioner has issued a Guide as to the Commissioner's expectations as to such notifications: OAIC, Data breach notification — A guide to handling personal information security breaches, August 2014. That Guide also sets out a data breach response process which can be expected to continue to be the Commissioner's view as to the process of triaging data breaches, as now supplemented by these additional mandatory requirements. Although the Commissioner's Guide was based upon a different threshold ('real risk of serious harm to an individual'), it should be readily capable of adaptation to this new scheme. We may expect to see new guidance from the Commissioner over forthcoming months.

**PETER LEONARD**
**Partner**
Gilbert + Tobin Lawyers, Sydney
T:+61 2 9263 4003
E: pleonard@gtlaw.com.au