Australia introduces mandatory data breach notification regime

14 February 2017

In brief

On 13 February 2017, with bipartisan support, the Senate passed the *Privacy Amendment (Notifiable Data Breaches) Bill 2016* (**Bill**). The Bill will now be presented to the Governor-General and its key provisions will come into operation on a date fixed by proclamation or 12 months after assent. Once enacted, the *Privacy Amendment (Notifiable Data Breaches) Act 2016* will introduce into Australia a mandatory data breach notification regime.

This new law will apply to all APP entities that are currently subject to the Australian Privacy Principles under the *Privacy Act 1988* (Cth) (e.g. many Australian Government agencies and private sector organisations with an annual turnover of more than $3 million). It will also apply to certain credit providers, credit reporting bodies, and holders of tax file number information.

Under the new law, unless an exception applies, APP entities along with credit providers, credit reporting bodies and tax file number recipients (each an **entity**), must notify eligible data breaches to the Office of the Australian Information Commissioner (**OAIC**) and affected individuals as soon as practicable after the applicable entity becomes aware that *"there are reasonable grounds to believe that there has been an eligible data breach of the entity"* (section 26WK of the Bill).

In summary, an ***'eligible data breach'*** occurs where there has been:

(a) unauthorised access or disclosure, or loss of information where unauthorised access or disclosure is likely; and

(b) a reasonable person would conclude that the access or disclosure would likely result in serious harm to the individuals to whom the information relates.

Who is subject to the new regime?

APP entities, credit reporting bodies, tax file number recipients holding information subject to the information security requirements under the Privacy Act.

↓

When is the requirement to notify triggered?

When an entity is aware that there are reasonable grounds to believe that there has been an '***eligible data breach***' of the entity.

↓

Do any exceptions apply to the notification requirement?

Yes, there are a range of exceptions, including where the affected entity takes sufficient remedial action in response to the eligible data breach before it causes serious harm.

↓

pwc

What does notification involve?

The entity must notify the OAIC and all individuals affected by the breach. If impractical to notify all affected individuals, the entity must publish a statement on its website and publicise the content of the statement. The notification must set out certain matters about the eligible data breach.

What are the possible sanctions?

Serious or repeated failure to comply could expose the affected entity to the risk of material civil penalties. There is also the risk of reputational and associated commercial damage.

The Bill is the third iteration in a series privacy reforms flowing from the recommendations of the Australian Law Reform Commission in 2008. First introduced to Parliament in 2013, and then again in 2015 as the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015,* the current Bill was introduced on 19 October 2016. Its passage has not been without controversy and many were concerned about the low applicability thresholds, unreasonable compliance burden and notification fatigue. Many of these concerns were considered and addressed as part of an industry consultation process and the development of the Bill.

Objectives of the new regime

The growth of the digital economy, advances in technology and the 'internet of things' have led to vast amounts of personal information being collected and stored by numerous organisations. With greater volumes of data comes greater risk of damage through disclosure or misuse. This is particularly so with personal information. Not only is there potential damage to the individuals concerned (whether that damage is financial, reputational, emotional or otherwise), but the digital economy necessarily relies on trust. Accordingly, various governments favour mandatory data breach reporting, amongst a suite of other initiatives, to bring accountability and transparency to organisations holding personal information. As explained in the Explanatory Memorandum to the Bill, the Bill is intended to:

- give individuals the opportunity to change or otherwise 're-secure' the information that has been accessed, disclosed or lost (i.e. the **mitigation objective**); and
- encourage businesses to improve their information security practices (i.e. the **deterrent objective**).

The Bill also endeavours to strike the right balance between promoting these objectives and the risk of placing an unreasonable compliance burden on regulated entities.

The takeaways

It is important to ensure compliance with the new law, including by implementing processes to meet the various assessment / notification requirements. In response to the passing of the Bill, the Australian Privacy and Information Commission has said the OAIC will release additional guidance over the next 12 months to help agencies and businesses prepare for the new law.

However, this is a business imperative and legal compliance is only part of your company's data protection program. The new laws present companies with an opportunity to engage with their customers on privacy protection and to build / maintain trust in an increasingly digital world. This is an ideal time to review how your company manages its information (and manages itself) to take stock of its information assets, its data protection measures (including response activities) and to ensure it minimises the risk of a breach in the first place.

For a detailed discussion of the key features of the mandatory data breach notification regime and an overview of the key issues facing entities bound by the new regime, please see below.

The new mandatory data breach notification regime

In further detail

Who is affected and how?

The Bill primarily supplements the existing obligations under APP 11.1, which requires an APP entity holding personal information to take reasonable steps to protect information from unauthorised disclosure, misuse, interference and loss.

What are the key features?

- Under the Bill, where an entity is aware that there are reasonable grounds to believe that there has been an 'eligible data breach' of the entity, then it must comply with the notification obligations.
- Specifically, as soon as practicable after the entity becomes aware, it must prepare a statement that addresses certain matters in relation to the eligible data breach and provide a copy of the statement to the OAIC and any affected individuals.
- Where it is not practical for the entity to notify all affected individuals, the entity must publish a copy of the statement on its website and take reasonable steps to publicise the content of the statement.
- The statement must include the identity and contact details of the entity, a description of the 'eligible data breach', the kind or kinds of information concerned and the recommended steps for individuals to take in response to the breach.
- If an entity suspects an 'eligible data breach', the Bill also requires that entity to carry out an assessment of whether there are reasonable grounds to believe an 'eligible data breach' has occurred.
- A failure to notify an 'eligible data breach' is an "*interference with the privacy of an individual*" under the Privacy Act. Serious or repeated interferences with the privacy of an individual can give rise to civil penalties.
- There are also a number of exceptions to the notification obligation (or ways in which an entity can avoid a breach being classified as an "eligible data breach"). Relevantly, these include:
    - where the entity is already required to disclose the breach pursuant to the My Health Records Act 2012 (Cth);
    - if the notification is inconsistent with a secrecy provision in another law;
    - if the entity has taken effective remedial action in respect of the 'eligible data breach' before it cases serious harm; or
    - if an 'eligible data breach' affects multiple entities and one of the other affected entities has already given notice of the eligible data breach in accordance with the notification requirements.
- Where (a) an entity has disclosed personal information to an overseas recipient; (b) APP 8.1 applies to the disclosure and (c) the overseas recipient holds the personal information, the mandatory notification requirements will still apply as if the entity held the information itself. This ensures that an entity will remain responsible and accountable for personal information, even where the 'eligible data breach' occurs offshore.

These key features of the new regime are summarised in the diagram on the next page.

Mandatory Data Breach Notification Regime

Who is subject to the new regime?

- New regime applies to:
  - **APP entities** (holding personal information);
  - **Credit reporting bodies** (holding credit reporting information);
  - **Credit providers** (holding credit eligibility information); and
  - **Tax file number recipients** (holding TFN information),

  where each of these entities is required to comply with the information security requirements under the Privacy Act in relation to the relevant information.

When is the requirement to notify triggered?

- When an entity is aware that there are reasonable grounds to believe that there has been an '***eligible data breach***' of the entity (whether after conducting an assessment of a suspected eligible data breach or otherwise).

What is an 'eligible data breach'?

Eligible data breach occurs if:

- there is unauthorised access to / disclosure of, the relevant personal, credit or TFN information; and
- a ***reasonable person*** would conclude the access/disclosure is ***likely to result in serious harm*** to any of the individuals to whom the information relates.

OR

- where the relevant information ***is lost*** (assuming that unauthorised access / disclosure were to occur), a ***reasonable person*** would conclude it is ***likely to result in serious harm*** to any of the individuals to whom the information relates.

What if there is only a suspected eligible data breach?

If there are ***reasonable grounds to suspect*** that there may have been an 'eligible data breach', the entity must:

- carry out a ***reasonable and expeditious assessment*** of whether there are reasonable grounds to believe that the relevant circumstances amount to an 'eligible data breach'; and
- take all reasonable steps to ensure that such assessment is carried out within ***30 days*** of becoming aware of the reasonable grounds for suspicion.

Do any exceptions apply to the notification requirement?

- There are a range of exceptions to the notification requirement, including:
  - ***Remedial action:*** Where the affected entity takes sufficient remedial action in response to the 'eligible data breach' before it causes serious harm to any affected individual; and
  - ***Single notice:*** If the 'eligible data breach' affects more than one entity, only one of the affected entities needs to undertake notification.

What does notification involve?

- Where an entity becomes aware of an eligible data breach, the entity must notify the OAIC and all individuals affected by the breach ***as soon as practicable.***
- If impractical to notify all affected individuals, the entity must publish a statement on its website and publicise the content of the statement.
- The notification must include:
  - the identity and contact details of the entity;
  - a description of the 'eligible data breach';
  - the kind(s) of information concerned; and
  - recommendation(s) of what the individual should do in response to the breach.

What are the possible sanctions?

- Serious or repeated failure to comply with the Privacy Act risks civil penalties of 2,000 / 10,000 penalty units for individuals / corporations respectively (approx. $360,000 / $1.8 million).
- Risk of reputational and commercial damage.

Key issues

The threshold test for an eligible data breach

Under the Bill, an "*eligible data breach*" occurs where:

- there is unauthorised access to or disclosure of the relevant information, which a "*reasonable person"* would conclude is "*likely to result in serious harm*" to any of the individuals to whom the information relates; or
- the relevant information is lost in circumstances where unauthorised access to or disclosure of personal information is likely to occur, and if it were to occur a "*reasonable person*" would conclude that it is "*likely to result in serious harm*" to any of the individuals to whom the information relates.

The Bill essentially requires eligible data breaches to be notified where a reasonable person would conclude that the access, disclosure or loss would be "*likely to result in serious harm*" to the affected individual. The Explanatory Memorandum notes that the phrase '*likely*' is intended to mean '*more probable than not*'.

This threshold test is arguably higher than the test set out in the 2015 Bill which required data breach notification where there was a "*real risk of serious harm*", with '*real risk*' being defined as '*a risk that is not a remote risk*'. By raising the threshold (i.e. so that notification will be required where the data breach is "*likely*" to result in serious harm), it is expected that fewer data breaches will need to be reported. As noted in the Explanatory Memorandum: "*It is not intended that every data breach be subject to a notification requirement*."

Reasonable person test to determine what is 'serious harm'

The determination as to what is '*serious harm*' is an objective '*reasonable person*' test. That is, whether a reasonable person would conclude that access to or disclosure of the personal information would be likely to result in serious harm to *any* of the individuals to whom the information relates. The Explanatory Memorandum notes that "*serious harm*" is to be broadly construed and may include physical, emotional, economic and financial harm as well as reputational damage.

While the Bill does not expressly define '*harm*', it does set out a non-exhaustive list of relevant factors to be taken into account in determining whether or not the breach is likely to result in serious harm. These include:

- the kind and sensitivity of the information;
- whether the information is protected by security measures and if so, the likelihood that such measures could be overcome;
- the persons or kinds of persons who have or could obtain access to the information; and
- the nature of the harm.

Importantly, the test for '*serious harm*' does not require that harm to be attributed to all affected individuals. It is satisfied if the harm would be caused to *any* individual whose relevant information has been breached.

Importance of security measures in reducing the risk of an "eligible data breach"

The Bill also confirms when determining whether or not the breach is likely to result in serious harm (and is therefore an '*eligible data breach*'), a relevant factor is the likelihood that persons who have the intention of causing harm, have or could obtain the information or knowledge required to circumvent a security technology or methodology (including encryption).

This highlights the importance of implementing robust security technology and solutions. Where entities have implemented such measures, this will significantly lessen the risk of a data breach (both in practice and when assessing whether an 'eligible data breach' has occurred).

Assessment of suspected 'eligible data breaches'

The trigger for undertaking an assessment of a suspected eligible breach is when an entity that becomes aware that there are reasonable grounds to suspect that an eligible data breach has occurred. An entity that is aware that there are *reasonable grounds to suspect* that there has been an eligible data breach, but does not have reasonable grounds to believe that there has been an 'eligible data breach', must carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that there has been an 'eligible data breach'.

The entity must take all reasonable steps to ensure that the assessment is completed within 30 days of the entity becoming aware of the reasonable grounds for the suspicion.

The assessment process is intended to apply where an entity becomes aware of circumstances that may constitute an eligible data breach, but the entity needs to complete a further assessment in order to determine whether the relevant circumstances actually amount to an eligible data breach.

The obligation to assess a suspected eligible breach is triggered when an entity that becomes aware that there are *reasonable grounds to suspect* that an eligible data breach has occurred. This is in contrast to the 2015 Bill which included a requirement for an entity to investigate the data breach within 30 days of the date that it "*ought reasonably to have been aware*" that there were reasonable ground to believe that there had been a serious data breach.

The removal of the requirement for an entity to consider when it ought reasonably to have been aware of the data breach, will alleviate many of the concerns raised during the consultation process about the practical difficulties of complying with this requirement. In any event, entities will still need to ensure that they have security incident management frameworks in place so that when they become aware of a suspected eligible data breach, they can undertake the appropriate response measures.

Be proactive about information security

It is essential that entities are proactive in responding to a data breach incident and that they take such preventative action necessary before any serious harm occurs to the affected individuals. This is reflected by the '*remedial action'* exception to the notification requirement in the Bill. Under this exception, where:

- there is unauthorised access to, disclosure or loss of information but the entity takes action before it results in any serious harm to the affected individual; and
- as a result of the action a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to the individual,

then the unauthorised access or disclosure is deemed to have never been an eligible data breach.

Responsibilities for notification

If an entity complies with the relevant notification requirements in relation to an eligible data breach, and that eligible data breach has also occurred in relation to other entities, then those other entities do not need to comply with the notification requirements in respect of that eligible data breach. This exception ensures that where multiple entities are affected by a single incident, only a single notice by one of the affected entities will be required.

Unlike other jurisdictions, the Bill does not introduce the concept of '*data controller*' or "*data processor*", nor does it specify a particular entity who will be responsible for complying with the notification requirement. Accordingly, entities will need to ensure that their arrangements with contracted services providers articulate each party's responsibility in responding to a data breach.

Entities will also need to liaise with their contracted service providers in the event of an eligible data breach to ensure that the relevant notification requirements are complied with by at least one of the affected entities.

Our final thoughts…

The mandatory notification requirements aim to ensure greater accountability and transparency in the information-handling practices of organisations and agencies. The Bill was passed in an environment of increasing international regulation of privacy (including, for example, the European Union GDPR).

The new law caps off an active time in the data protection space, with the Full Federal Court handing down a key decision narrowing the definition of '*personal information*' under the Privacy Act in *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4.

The Bill will require relevant entities to put in place effective data breach response and notification processes. Importantly, the new law seeks to protect organisations that are proactive and respond quickly and effectively to data breaches and suspected data breaches.

It is important to ensure compliance with the new law, including by implementing processes to meet the various assessment and notification requirements. In large organisations, this will become a particularly challenging requirement. In response to the passing of the Bill, the Australian Privacy and Information Commission has said the OAIC will release additional guidance over the next 12 months to help agencies and businesses prepare for the commencement of the new law.

This is a business imperative and legal compliance is only part of your company's data protection program. The new laws present companies with an opportunity to engage with its customers on privacy protection and to build / maintain trust in an increasingly digital world. This is an ideal time to review how your company manages its information (and manages itself) to take stock of its key information assets, its data protection measures (including response activities), and to ensure it minimises the risk of a breach in the first place.

PwC looks a data protection as a "whole of business" requirement. We advise our clients on compliance risk reviews and legal advice, third party supplier risk assessments, process development and reform, technology solutions and operational design. If you have any questions about the Bill, and the ways it may affect the whole of your business, let's talk…

For a deeper discussion of how these issues might affect your business, please contact:

Tony O'Malley
Partner, Legal
+61 (2) 8266 3015
tony.omally@pwc.com

Cameron Whittfield
Partner, Legal
+61 (3) 8603 0140
cameron.whittfield@pwc.com

Adrian Chotar
Director, Legal
+61 (2) 8266 1320
adrian.chotar@pwc.com

Sylvia Ng
Director, Legal
+61 (2) 8266 0338
sylvia.ng@pwc.com

Steve Ingram
Partner, Cyber
+61 (3) 8603 3676
steve.ingram@pwc.com

Peter Malan
Partner, Cyber / Assurance
+61 (3) 8603 0642
peter.malan@pwc.com

Anna Lin
Senior Associate, Legal
+61 (3) 8603 1751
anna.lin@pwc.com

Steph Baker
Solicitor, Legal
+61 (2) 8266 5054
steph.baker@pwc.com

Grace Guinto
Director, Digital Trust
+61 (3) 8603 1344
grace.guinto@pwc.com