Submission deadline looms for public comment on the Notifiable Data Breaches scheme

4 July 2017

Overview

The opportunity to provide public comment on the "draft guidance" released by The Office of the Australian Information Commissioner (**OAIC**) in relation to the new Notifiable Data Breaches (**NDB**) scheme is fast closing. Organisations have until 14 July 2017 to lodge submissions with the OAIC via this link.

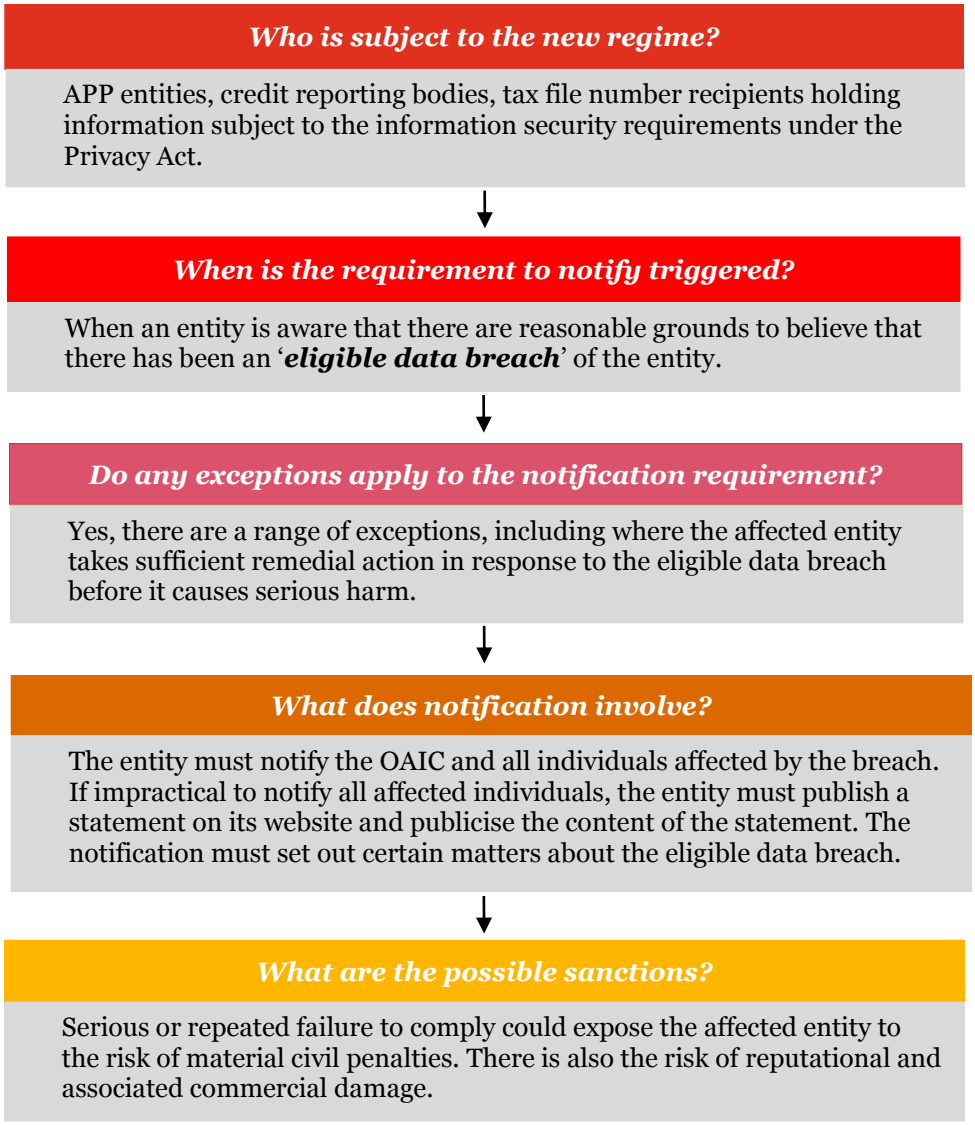
On 2 June 2017 the OAIC released initial guidance to help affected entities understand and comply with the new NDB scheme which commences on 22 February 2018. Whilst further guidance is expected, including in relation to critical components of the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (e.g. guidance on assessing a "suspected data breach"), organisations can provide public comment on the following four components of the draft guidance:

- *Entities covered by the NDB scheme;*
- *Notifying individuals about an eligible data breach;*
- *Identifying eligible data breaches; and*
- *Australian Information Commissioner's role in the NDB scheme.*

When PwC hosted the Australian Information and Privacy Commissioner, Timothy Pilgrim PSM, at an event in March this year, the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (the **Act**) had only just received royal assent. Many in the room that day were still grappling with fundamental concepts contained within the Act, including:

- Who was subject to the new regime?
- What was an "eligible data breach"?
- When was the requirement to "notify" triggered?
- Did any exceptions apply and how did they work?
- What did "notification" involve?

To help understand the new NDB scheme, we prepared some preliminary guidance alongside a series of flow diagrams to help organisations understand how various components of the Act interacted. This previous guidance can be found here. A flow diagram setting out the new regime is set out below, with a more detailed summary attached to this paper (***see Appendix 1***).



While the Act (and the supporting Explanatory Memorandum) provided some guidance, material components were left undefined. In this context, the OAIC released four draft resources or "guidance notes" to assist organisations to prepare for the commencement of the NDB scheme. For more information on the resources released by the OAIC, click here.

We encourage those organisations impacted by the NDB scheme to actively engage in this consultation exercise. To assist, we have set out below a brief summary of the key takeaways from the four components of the draft guidance.

Entities covered by the NDB scheme

In many respects, the "Entities covered by the NDB scheme" guidance seeks to restate the position set out under the Act.

The NDB scheme will apply to organisations that are already required by the *Privacy Act 1988* (Cth) (**Privacy Act**) to keep information secure, including businesses and Australian Government agencies that are APP entities, credit reporting bodies and holders of tax file numbers. Specifically, the NDB scheme applies to entities that have an obligation under APP 11 of the Privacy Act to protect the personal information they hold.

While small business operators are generally not subject to the Privacy Act, the Privacy Act does extend the APPs (and therefore also the NDB scheme) to certain small businesses (depending on the nature of the business) and to credit reporting bodies, credit providers and tax file number recipients.

The draft guidance note clarifies that entities which have security obligations under the Privacy Act in relation to particular types of information (e.g. small businesses required to secure tax file number information), do not need to notify the Commissioner about data breaches that affect types of information that fall outside the scope of their obligations under the Privacy Act.

Notifying individuals about an eligible data breach

When an entity subject to the NDB scheme experiences an "eligible data breach", that entity must, in certain circumstances, issue a statement to the Commissioner, and as soon as practicable after notifying the Commissioner, the entity must also notify those individuals at risk of serious harm of the contents of that statement.

The guidance note considers the following three options for notifying affected individuals:

1. ***Notify all individuals*** – this involves notifying all individuals whose personal information was part of the eligible data breach;

2. ***Notify only those individuals at risk of serious harm*** – if practicable, the entity may only notify those individuals who are at risk of serious harm; or

3. ***Publish notification*** – if neither of the above two options are practicable, the entity must publish a copy of the statement on its website (if it has one) and take reasonable steps to publicise the contents of the statement.

The draft guidance note seeks to clarify that if a single data breach has affected multiple entities, only one entity need notify the Commissioner and the affected individuals at risk of serious harm. The entities involved have the responsibility of deciding which of them notifies the relevant parties. The guidance note recommends that the entity that has the most direct relationship with the individuals at risk should undertake the notification process on behalf of the affected entities.

Examples of different methods for notification are given - ranging from telephone calls, SMS, in-person conversations through to print / online advertising. The entity can use any method to notify affected individuals, so long as the method is reasonable. In determining whether a method (or combination of methods) is reasonable, the guidance note suggests that the entity should consider the likelihood that the individuals they are notifying will become aware of and understand the notification.

Identifying eligible data breaches

The draft guidance note provides that a data breach is considered an "eligible data breach" if three conditions are satisfied (consistent with the Act):

1. *There is unauthorised access to or unauthorised disclosure of personal information, or loss of personal information, that an entity holds;*

2. *This is likely to result in serious harm to one or more individuals; and*

3. *The entity has not been able to prevent the likely risk of serious harm with remedial action.*

Whether a data breach is likely to result in serious harm is an objective assessment, based on the perspective of a reasonable person in the entity's position, with the harm to include physical, psychological, emotional, financial or reputational.

A data breach is not eligible if it is not likely to result in serious harm. For example, if there is a data breach, but the entity is able to take remedial action and address the breach in a timely manner preventing the likelihood of serious harm, the entity may not be required to notify the Commissioner and the affected individuals.

Separately, the OAIC is developing a separate resource "*Assessing a suspected data breach*" to provide guidance to entities in relation to the process to be followed in assessing "*whether there are reasonable grounds to suspect that there may have been an eligible data breach of the entity*".

Importantly, the guidance provides that it would be "prudent" for an entity to assume that a data breach that involves the loss of personal information of a very large number of individuals is likely to result in serious harm to at least one of those individuals.

Australian Information Commissioner's role in the NDB scheme

The draft guidance clarifies that the Commissioner is required to fulfil a number of roles in relation to the NDB scheme, including:

- receiving notifications of eligible data breaches, and where appropriate, making inquiries or offering advice and guidance in response to notifications;
- encouraging compliance with the scheme, including by handling complaints, conducting investigations and taking other regulatory action in response to instances of non-compliance; and
- offering advice and guidance to regulated entities, and providing information to the community about the scheme's operation.

The Commissioner has various enforcement powers available to it, to ensure entities meet their regulatory obligations under the NDB scheme. If an entity fails to comply with the NDB scheme, this will amount to an "*interference with the privacy of an individual*", in which case the Commissioner may elect to exercise any of the following responses:

- accept an enforceable undertaking and bring proceedings to enforce an enforceable undertaking;
- make a determination and bring proceedings to enforce a determination;
- seek an injunction to prevent ongoing activity or a recurrence; and
- apply to court for a civil penalty order for a breach of a civil penalty provision, which includes any serious or repeated interference with privacy.

Conclusion

We believe that the OAIC is likely to take an active role in monitoring, guiding and enforcing the new NDB scheme. Consistent with global trends, as seen the EU with the GDPR notification of breach requirements, we believe the OAIC will be notably active in monitoring compliance and enforcement under the NDB scheme.

Accordingly, we certainly encourage those organisations impacted by the NDB scheme to consider whether they have any concerns with the draft guidance and actively engage in this consultation exercise by submitting comments to the OAIC by **14 July 2017**. PwC can assist you in understanding your obligations under the Act and in preparing any comments to the OAIC.

Let's talk

For further information on how these issues might affect your business, please contact:

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

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

Rhys McWhirter
Senior Associate, Legal
+61 (2) 8266 2187
rhys.mcwhirter@pwc.com

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

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

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

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

Grace Guinto
Director, Cyber / Assurance
+61 (3) 8603 1344
grace.guinto@pwc.com

Hugo Chan
Associate, Legal
+61 (2) 8266 5721
hugo.chan@pwc.com

www.pwc.com.au

© 2017 PricewaterhouseCoopers. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers a partnership formed in Australia, which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity. This publication is a general summary. It is not legal or tax advice. Readers should not act on the basis of this publication before obtaining professional advice. PricewaterhouseCoopers is not licensed to provide financial product advice under the Corporations Act 2001 (Cth). Taxation is only one of the matters that you need to consider when making a decision on a financial product. You should consider taking advice from the holder of an Australian Financial Services License before making a decision on a financial product.

Appendix 1

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.

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.

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 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.