6 Things You Should Know About the New NDB Scheme

Valeska Bloch, a partner at Allens, takes us through some of the key issues arising out of the new notifiable data breach scheme.[1]

The Office of the Australian Information Commissioner (***OAIC***) recently reported that sixty-three data breaches were notified to it in the first six weeks of the new notifiable data breaches scheme (**NDB scheme**) taking effect. Although the basic components of the scheme are now reasonably well known, organisations are still grappling with the practicalities of assessing and notifying data breaches, particularly in circumstances where the facts are unclear and the data the subject of the breach was jointly held. This article attempts to provide some practical guidance in navigating the new scheme.

1 The 30 day time limit to assess whether an eligible data breach has occurred is not a hard stop.

Where an entity becomes aware of reasonable grounds to suspect that an *eligible data breach* has occurred, it must carry out an assessment of this suspicion expeditiously and must take *all reasonable steps* to carry out this assessment within 30 days.[2]

The OAIC has said that entities should treat this 30 day period as the maximum time limit, particularly given that the risk of serious harm to individuals tends to increase with time. However, the OAIC also recognises that it will not always be possible to complete an assessment of a suspected data breach within 30 days, for example, if systems or records were lost during the intrusion and significant recovery effort is required.

Top tip: Where an entity cannot reasonably conduct a data breach assessment within 30 days, the OAIC recommends that an entity prepare and retain documentation that will allow it to demonstrate:

- that all reasonable steps were taken to complete the assessment within 30 days;
- the reasons for the delay; and
- that the assessment was reasonable and expeditious.

2 The scheme does not apply to employee records.

The OAIC has confirmed in its *Data breach preparation and response* guide that businesses will not be required to notify the OAIC or individuals about data breaches relating to employee records – that is, personal information of an employee relating to their employment. This is because the employee records exemption provided for in the *Privacy Act 1988* (Cth) (*the **Privacy Act***) applies to the NDB Scheme.[3]

A few words of caution.

- Even where the employee records exemption applies, the OAIC recommends notifying individuals affected by a breach of employee record if it is likely to result in serious harm.
- Think carefully about whether the information involved in a data breach is *truly* covered by the exemption.

For example, employees often use their work email accounts to receive personal emails, such as communications from their bank which would not be covered by the exemption. In practice, it may be difficult to distinguish between what data does and does not fall within the exemption.

- The employee records exemption will not extend to a data breach involving tax file numbers.[4]
- The employee records exemption only applies to an employee record held by the employer. If your organisation stores its employee records with a third party, the exemption will extend to a data breach involving those records and your service provider will need to notify the OAIC of the breach.

3 The OAIC can make a declaration that an entity does not have to notify, or can defer notification, for a specified period.

The NDB Scheme allows the OAIC to declare that an entity may dispense with or delay notification following an *eligible data breach*.[5] The decision to exercise this power may be on the OAIC's own initiative or follow an application by an entity that has experienced a data breach.[6]

In deciding whether to make such a declaration, the Commissioner must be satisfied that it is reasonable in the circumstances to do so, having regard to:

1 Thank you to Sam Dutaillis and Alexi Polden for their assistance in preparing this article.
2 *Privacy Act 1988* (Cth), s 26WH.
3 *Privacy Act 1988* (Cth), s 7B.
4 *Privacy Act 1988* (Cth), ss 17, 18 and 26WE(1)(d).
5 *Privacy Act 1988* (Cth), s 26WQ.
6 *Privacy Act 1988* (Cth), s 26WQ(5).

1. The public interest;
2. Any relevant advice provided to the OAIC by an enforcement body or the Australian Signals Directorate; and
3. Any other matter that the OAIC considers to be relevant to the situation.[7]

The OAIC has also identified a number of additional factors that they may consider before making a declaration to this effect, including whether the risks associated with notification outweigh the benefits to individuals at risk of serious harm.

Things to consider when making an application:

- The OAIC expects that declarations will only be made in exceptional circumstances. Unfortunately, owing to the practical reality that only entities which are granted declarations will be made aware of the circumstances in which they occur, it is difficult to predict what will be considered sufficiently *'exceptional'*.
- Entities that request an exemption should be prepared to present a compelling case with detailed evidence as to why it is reasonable in the circumstances for the notification requirements to be dispensed with, including why no other exemptions apply.

4 You may still need to notify even if the eligible data breach requirement is not triggered

It is a common misconception that once a data breach has occurred, your notification obligations are limited to those required by the NDB scheme. In fact, there may be other good reasons why you may choose or need to notify.

1. APP 11 – Prior to the introduction of the NDB scheme, the OAIC had suggested that in certain circumstances, a failure to notify may in and of itself constitute a breach of APP 11. This is because notifying may in fact enable individuals to protect their personal information, for example, by changing their passwords.

Although the introduction of the NDB Scheme makes it less likely that the OAIC would seek to assert that a breach of APP 11 has occurred in a data breach scenario, it is still open to the OAIC to do so. This means that even if you suffer a data breach that is not an eligible data breach, you should still consider notifying.

2. Continuous disclosure – If you are a listed entity and there is a possibility that a data breach you suffer might reasonably be expected to have a material effect on the price of your securities, you may need to disclose the data breach to the ASX.

3. Other notification requirements – Depending on the nature of your business, how and where you hold your data and who you hold data about, you may be subject to other notification requirements, for example, under state-based or international data protection laws, or under sector specific laws. Keep in mind:

The EU General Data Protection Regulation (***GDPR***) which has significant extra-territorial reach.

Reporting obligations under the National Cancer Screening Register Act 2016 and the My Health Records Act 2012.

4. Public and customer relations – Even if there is no legal obligation to notify affected customers, you may decide to notify about a non-eligible data breach in the interests of maintaining good public relations, particularly if there is a reasonable chance that the data breach may become public through sources that are out of your control. If you get on the front foot with notification and a public statement, you can control the narrative and ensure that your customers receive accurate information.

5 You will be liable for the notification of breaches suffered by an overseas recipient of personal information

Ordinarily, where an entity discloses personal information to an overseas recipient in accordance with Australian Privacy Principle 8.1, the disclosing party will only be liable for a breach of the Australian Privacy Principles (***APPs***) by that overseas recipient where the APPs ***do not*** apply to the overseas recipient.[8]

The NDB scheme takes a stricter approach, such that a party who discloses personal information in accordance with APP 8.1 is deemed liable even where the overseas recipient is itself subject to the Privacy Act.[9] Keep in mind that this deemed liability will not apply to personal information disclosed overseas under an exception in APP 8.2.

There is similar deemed liability for credit providers who disclose credit eligibility information in specified circumstances to certain bodies without an 'Australian link'[10] but there is no deemed liability for credit reporting bodies who are not permitted to disclose credit reporting information unless certain exceptions apply. Those exceptions are limited and

7 *Privacy Act 1988* (Cth), s 26WQ(3).

8 Section 16C, *Privacy Act 1988*.

9 *Privacy Act* 1988 (Cth), s 26WC; Although this is the position under the legislation, curiously, the Explanatory Memorandum to the bill introducing the NDB Scheme appears to suggest that s 26WC and s 16C will operate in the same way, when in fact, the latter contains a critical caveat to the effect that where the APPs apply to an overseas recipient of personal information, the disclosing entity will not be deemed liable. In contrast, the drafting of s 26WC indicates that a disclosing entity is liable for any breach of the NDB Scheme by an overseas organisation, regardless of whether the overseas recipient is subject to the APPs. Interestingly, the Explanatory Memorandum does not provide an explanation for this distinction between the two provisions.

10 Defined in s 5B of the *Privacy Act 1988*.

in most cases require that the party receiving the information has an 'Australian link'.

Although the OAIC recommends that where a single data breach involves multiple entities, the entity with the most direct relationship with the affected individuals should make the notification, if an overseas recipient of information disclosed by you suffers a data breach, keep in mind that you will be deemed liable for any failure to notify that breach.

It may still be appropriate for the overseas recipient to notify, depending on who has the closer relationship with affected individuals, but you should make sure that you retain appropriate oversight and input into the assessment of the breach, what the notification contains and how it is carried out.

Importantly, if no assessment or notification is undertaken when required, all of entities involved may be taken to have breached those requirements. In light of that it is worth looking in a little more depth at how you should consider responding to the uncertainty of a data breach involving jointly held information.

6 Data breaches involving jointly held information involve an additional layer of complexity.

When will you hold information?

For the purposes of the NDB Scheme, an entity will be considered to 'hold' personal information if it has possession or control over the relevant record,[11] that is where it has a right or power to deal with the record. This is not limited to physical possession.

This means you cannot simply avoid your obligation to notify under the NDB Scheme by outsourcing your data storage to a third party.

When will you *'jointly'* hold information?

Information will be held jointly where two or more entities hold the same record of personal information.

There is an important difference between jointly held data and newly created records that are derived from mutually held information.

This distinction is best demonstrated by an example given by the OAIC in its *Data breach preparation and response* guide. In this hypothetical scenario, a client company provides a market research firm with the personal information of individuals for a focus group. The information is provided in circumstances where contractual arrangements mean that the client retains control over how the information is used.

At this point in time, the personal information is jointly held between the client and the market research firm.

Following the focus group session, the market research team asks the focus group attendees whether they would like to participate in future research projects which they facilitate. All participants give their consent to have their personal information held by the market research company to be contacted for future research opportunities. The market research firm creates a new record containing this information.

This is a new record that is separate from the information that was held jointly by the client and the market research firm.

This new record is not *'held jointly'* for the purposes of the NDB Scheme, even though the personal information may be identical to that which is held jointly. As such, to the extent the new record is breached, only the market research firm will be responsible for notifying in respect of the new records, unless of course, the contractual arrangements stipulate that the client has the right or power to deal with newly created records.

Practically, this means that you should very carefully consider how different categories of data are dealt with in agreements, including by identifying which data you do have rights to deal with and when a newly created records will be out of your control.

Who should undertake the assessment and notification in relation to jointly held information?

The new scheme does not prescribe which entity should assess and/or notify,[1] allowing entities that hold information jointly to tailor their assessment and notification arrangements to accommodate their particular customer and contractual requirements.

Although the OAIC suggests that the entity with the most direct relationship with the individuals at risk of serious harm will often be best placed to notify, there may be situations where the OAIC's suggested approach isn't the preferred response from a commercial perspective (for example, where the system involved is so complex that the system host will be best equipped to deal with any further queries post-notification).

It is important to consider these issues in advance and to ensure that both parties are aligned as to who should assess and who should notify. In some circumstances, the parties might prefer that the entity that undertakes the assessment is different to the entity that notifies.

11 See *Data breaches involving more than one entity* in Part 4 of the OAIC's *Data breach preparation and response guide*

Top tips for dealing with jointly held information

1. Be careful not to rely too heavily on other organisations to carry out an assessment or make a notification in the absence of appropriate oversight. Ensure that you have clearly communicated the responsibilities of each entity holding that information in the event of a data breach (ideally by drafting this into your new and existing contractual arrangements), prior to any incident taking place. This will save any confusion and potential miscommunication in the aftermath of a significant data breach involving several entities across a number of possible locations.
2. In deciding how to allocate responsibility for undertaking an assessment and notifying the OAIC and affected individuals, weigh up all of the possible risks and benefits associated with the responsibility of notifying. Consider:
   - Who would be the 'public face' of the breach – are you or the other party likely to receive inquiries?
   - Who would affected individuals expect the notification to come from?
   - Who has the most direct access to the underlying systems that would be affected? Consider which entity will be best able to undertake the assessment and would be best placed to provide relevant and accurate information.
   - Is one party better resourced or more able to undertake the assessment or notification?
   - Who will be responsible for the costs of assessment and notification?
   - Who will be best placed to handle additional queries post-notification from the OAIC or affected individuals?
   - Do you or the other party have any additional notification obligations? For example, under continuous disclosure requirements or overseas data breach notification regimes.
3. Your contractual arrangements should contemplate:
   - a requirement that other parties be informed where one party suspects a data breach involving jointly held information has occurred;
   - the process for conducting an assessment where it is suspected that a data breach has occurred;
   - who should undertake an assessment of a suspected data breach in particular circumstances;
   - where an eligible data breach has occurred, who is responsible for notification to the OAIC and affected individuals; and
   - a right to review and/or sign-off on any data breach statement prepared for the OAIC and individuals whose information was involved in the data breach.
4. Other issues you may want to consider include:
   - If another party is responsible for the assessment and/or notification under the NDB Scheme, how might you ensure this has actually occurred?
   - What will happen if another party undertakes an assessment of the data breach and considers that notification is not required, but you disagree (or vice versa)? How might you resolve this stalemate?
5. Where the OAIC decides to review a data breach involving information you held jointly, it is important that you can demonstrate the steps taken to ensure compliance with the NDB Scheme. This might include any documentation prepared for the purposes of complying with the notification regime, any internal processes or procedures, and any correspondence with the entity responsible for notification at the time of the breach.

With the NDB scheme still in its infancy, it remains to be seen how bullish the OAIC will be in its pursuit of organisations that do not comply with it. That said, the considerable public outrage in response to the Cambridge Analytica Facebook scandal shows that privacy is clearly on the public's radar. If organisations want to retain the public's trust they should comply fully with the NDB scheme, not only because it is the law, but because it is what consumers are coming to expect.

Valeska Bloch is a partner in the Technology, Media and Telecommunications group at Allens.