Notifying individuals about an eligible data breach

The Office of the Australian Information Commissioner (OAIC) published this resource as an exposure draft on 2 June 2017. The OAIC would welcome comments from any interested parties about this resource before it is finalised. If you would like to provide comment on this resource, please email consultation@oaic.gov.au by 14 July 2017.

» Further information on providing comment

Key points

- When an entity experiences an eligible data breach, it must provide a statement to the Commissioner, and notify individuals at risk of serious harm of the contents of the statement.

- If it is not practicable to notify individuals at risk of serious harm, an entity must publish a copy of the statement prepared for the Commissioner on its website, and take reasonable steps to bring its contents to the attention of individuals at risk of serious harm.

- If a single eligible data breach applies to multiple entities, only one entity needs to notify the Commissioner and individuals at risk of serious harm. It is up to the entities to decide who notifies. Generally, the Commissioner suggests that the entity with the most direct relationship with the individuals at risk of serious harm should undertake the notification.

Who needs to be notified?

Once an entity has reasonable grounds to believe there has been an eligible data breach, the entity must promptly prepare a statement for the Commissioner and make a prompt decision about which individuals to notify.

The Notifiable Data Breaches (NDB) scheme provides flexibility — there are three options for notifying individuals at risk of serious harm, depending on what is ‘practicable’ for the entity (s 26WK(2)).

Whether a particular option is practicable involves a consideration of the time, effort, and cost of notifying individuals at risk of serious harm in a particular manner. These factors should be considered in light of the capabilities and capacity of the entity.
Option 1 — Notify all individuals

If it is practicable, an entity can notify each of the individuals to whom the relevant information relates (s 26WL(2)(a)). That is, all individuals whose personal information was part of the data breach.

This option may be appropriate, and the simplest method, if an entity cannot reasonably assess which particular individuals are at risk of serious harm from an eligible data breach that involves personal information about many people, but where the entity has formed the view that serious harm is likely for one or more of the individuals.

The benefits of this approach include ensuring that all individuals who may be at risk of serious harm are notified, and allowing them to consider whether they need to take any action in response to the data breach.

Option 2 — Notify only those individuals at risk of serious harm

If it is practicable, an entity can notify only those individuals who are at risk of serious harm from the eligible data breach (s 26WL(2)(b)).

That is, individuals who are likely to experience serious harm as a result of the data breach. If an entity identifies that only a particular individual, or a specific subset of individuals, involved in an eligible data breach is at risk of serious harm, and can specifically identify those individuals, only those individuals need to be notified.

The benefits of this targeted approach include avoiding possible notification fatigue among members of the public, and reducing administrative costs, where it is not required by the NDB scheme.

Example: An attacker installs malicious software on a retailer’s website. The software allows the attacker to intercept payment card details when customers make purchases on the website. The attacker is also able to access basic account details for all customers who have an account on the website. Following a comprehensive risk assessment, the retailer considers that the individuals who made purchases during the period that the malicious software was active are at likely risk of serious harm, due to the likelihood of payment card fraud. Based on this assessment, the retailer also considers that those customers who only had basic account details accessed are not at likely risk of serious harm. The retailer is only required to notify those individuals that it considers to be at likely risk of serious harm.

Option 3 — Publish notification

If neither option 1 or 2 above are practicable, the entity must:

- publish a copy of the statement on its website if it has one
- take reasonable steps to publicise the contents of the statement (s26WL(2)(c)).

It is not enough to simply upload a copy of the statement prepared for the Commissioner on any webpage of the entity’s website. Entities must also take proactive steps to publicise the substance of the data breach (and at least the contents of the statement), to increase the likelihood that the eligible data breach will come to the attention of individuals at risk of serious harm.
How do I notify and what do I need to say?

**Options 1 and 2**

Options 1 and 2 above require that entities take ‘such steps as are reasonable in the circumstances to notify individuals about the contents of the statement’ that the entity prepared for the Commissioner (s 26WL(2)(a) and (b)).

The entity can use any method to notify individuals (for example, a telephone call, SMS, physical mail, social media post, or in-person conversation), so long as the method is reasonable. In considering whether a particular method, or combination of methods is reasonable, the notifying entity should consider the likelihood that the people it is notifying will become aware of, and understand the notification, and weigh this against the resources involved in undertaking notification.

An entity can notify an individual using their usual method of communicating with that particular individual (s 26WL(4)).

The entity can tailor the form of its notification to individuals, as long as it includes the content of the statement required by s 26WK. That statement (and consequently, the notification to individuals) must include the following information:

1. the identity and contact details of the entity (s 26WK(3)(a))
2. a description of the eligible data breach that the entity has reasonable grounds to believe has happened (s 26WK(3)(b))
3. the kind, or kinds, of information concerned (s 26WK(3)(c))
4. recommendations about the steps that individuals should take in response to the data breach (s 26WK(3)(d)).

**Option 3**

Option 3, which can only be used if Options 1 or 2 are not practicable, requires an entity to publish a copy of the statement prepared for the Commissioner on its website, and take reasonable steps to publicise the contents of that statement.

An entity should consider what steps are reasonable in the circumstances of the entity and the data breach to publicise the statement. The purpose of publicising the statement is to draw it to the attention of individuals at risk of serious harm, so the entity should consider what mechanisms would be most likely to bring the statement to the attention of those people.

A reasonable step when publicising an online notice, might include:

- ensuring that the webpage on which the notice is placed can be located and indexed by search engines
- publishing an announcement on the entity’s social media channels
- taking out a print or online advertisement in a publication or on a website the entity considers reasonably likely to reach individuals at risk of serious harm.
In some cases, it might be reasonable to take more than one step to publicise the contents of the statement. For example, if a data breach involves a particularly serious form of harm, or affects a large number of individuals, 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.

The approach to publicising the statement may depend on the publication method. For example, where space and cost allows, an entity may republish the entirety of the information required to be included in the statement. Another option, if the available space is limited, or the cost of republishing the entire statement would not be reasonable in all the circumstances, would be to summarise the information required to be included in the statement and provide a hyperlink to the copy of the statement published on the entity’s website. Entities should keep in mind the ability and likelihood of individuals at risk of serious harm being able to access the statement when determining the appropriateness of relying solely on such an approach.

**Timing of notification**

Entities must notify individuals as soon as practicable after completing the statement prepared for notifying the Commissioner (s 26WL(3)).

Considerations of cost, time, and effort may be relevant in deciding an entity’s decision about when to notify individuals. However, the Commissioner generally expects entities to expeditiously notify individuals at risk of serious harm about an eligible data breach unless cost, time, and effort are excessively prohibitive in all the circumstances.

If entities have notified individuals at risk of serious harm of the data breach before they notify the Commissioner, they do not need to notify those individuals again, so long as the individuals were notified of the contents of the statement given to the Commissioner. The scheme does not require that notification be given to the Commissioner before individuals at risk of serious harm, so if entities wish to begin notifying those individuals before, or at the same time as notifying the Commissioner, they may do so.

**Data breaches involving more than one organisation**

If more than one entity holds personal information that was compromised in an eligible data breach, only one entity needs to notify individuals about the data breach. For example, more than one entity may hold personal information compromised in an eligible data breach due to outsourcing, a joint venture, or shared services arrangements between entities. However, if none of the entities notifies, each of the entities may be found to have breached s 26WL(2).

In these circumstances the Privacy Act intentionally does not specify which entity must undertake the notification, in order to allow entities flexibility in making arrangements appropriate for their business and their customers.

Entities should consider making arrangements regarding compliance with NDB scheme requirements, including notification to individuals at risk of serious harm, such as in service agreements or other relevant contractual arrangements, as a matter of course when entering into such agreements.

The Commissioner suggests that, in general, the entity with the most direct relationship with the individuals at risk of serious harm should notify. This will allow individuals to better understand the notification, and how the data breach might affect them.
Example: A medical practice stores paper-based patient records with a contracted storage provider. The storage provider’s premises are broken into, and the patient records stolen. Both the medical practice and the storage provider hold the records for the purpose of the Privacy Act, so both have an obligation to notify. Although the storage provider’s insurance company has agreed to cover the cost of the break in, including the cost of notification, the storage provider and medical practice agree that it is most appropriate that notification come from the medical practice, as the individuals at risk of serious harm do not have any pre-existing relationship with the storage provider. As such, the medical practice notifies the individuals about the incident and is reimbursed by the storage provider and its insurer for the costs of notification.