Australian Government

Office of the Australian Information Commissioner

Responding to data breaches

Quick reference guide

30 June 2026

OAIC

This guide is for entities that have obligations under the Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act. If you have existing obligations under the Privacy Act to secure personal information under APP 11, you must comply with the NDB scheme. This includes Australian Government agencies, businesses and not-for-profit organisations with an annual turnover of more than $3 million, private sector health service providers, credit reporting bodies, credit providers, and some small business operators with an annual turnover of $3 million or less (such as TFN recipients and more).

This guide will help you understand what to do in the event of a data breach. **Part B** will help you assess whether your entity has experienced a data breach that needs to be notified under the NDB scheme. Please refer to the resources linked throughout for additional information and guidance.

Resources

For more information, see 'Entities covered by the NDB scheme' in Part 4: Notifiable Data Breach (NDB) Scheme | OAIC

If your entity does not have obligations under the NDB scheme, consider whether you have obligations under other laws, for example state-based or international data protection laws. See 'Other obligations' in Part 1: Data breaches and the Australian Privacy Act | OAIC.

Part A
What to do in the event of a data breach

Generally, the actions taken following a data breach should include four key steps:

1

Contain

Contain the data breach to prevent any further compromise of personal information.

2

Assess

Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm. Assess whether the breach is an 'eligible data breach' under the NDB scheme (refer to **Part B** of this guide).

3

Notify

Notify individuals and the OAIC if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for your entity to notify (refer to **Part B** of this guide).

4

Review

Review the incident and consider what actions can be taken to prevent future breaches.

Resources

For more information on these steps, refer to Part 3 of the OAIC's Data breach preparation and response guide. You can also view these steps as part of the data breach response flowchart.

Part B
Determine whether the data breach is notifiable under the NDB scheme

Step 1
Has there been a **data breach** for the purposes of the NDB scheme?

Has the personal information your entity holds been subject to **unauthorised access, unauthorised disclosure**, or **loss**?

For example:

- an employee browsing sensitive customer records without any legitimate purpose
- a computer network being compromised by an external attacker resulting in personal information being accessed without authority
- an employee of your entity accidentally publishing a confidential data file containing the personal information of one or more individuals on the internet
- an employee of your entity leaves personal information (including hard copy documents, unsecured computer equipment, or portable storage devices containing personal information) on public transport

Yes

Proceed to the next step.

No

Continue to comply with your ongoing information security and governance obligations under APP 1 and APP 11.

Next step

Resources

See '**What is a data breach?**' Part 1: Data breaches and the Australian Privacy Act | OAIC
See "**What is a 'data breach'?**" Identifying eligible data breaches for interpretations of 'unauthorised access', 'unauthorised disclosure', and 'loss'.

Step 2

Is it an eligible data breach?

The NDB scheme requires notification of eligible data breaches. A data breach is 'eligible' if it is likely to result in serious harm to one or more individuals and your entity has not been able to prevent the likely risk of serious harm with remedial action.

Is the data breach likely to result in serious harm to any of the individuals whose personal information was involved?

Assess this from the perspective of a 'reasonable person'. A 'reasonable person' means a person in your entity's position (rather than the position of an individual whose personal information was part of the data breach or any other person), who is properly informed, based on information immediately available or following reasonable inquiries or an assessment of the data breach.

'Serious harm' to an individual may include serious physical, psychological, emotional, financial, or reputational harm. Serious harm is 'likely' to occur if the risk of serious harm to an individual is more probable than not (rather than possible). Assess the risk of serious harm holistically, having regard to the likelihood of the harm eventuating for individuals whose personal information was part of the data breach and the consequences of the harm. The NDB scheme includes a non-exhaustive list of 'relevant matters' that may assist you to assess the likelihood of serious harm. These are listed under 'Is serious harm likely?' in Identifying eligible data breaches.

Has your entity been able to prevent the likely risk of serious harm through remedial action?

If your entity takes remedial action such that the data breach would not be likely to result in serious harm, then the breach is not an eligible data breach. For breaches where information is lost, the remedial action is adequate if it prevents unauthorised access to, or disclosure of personal information.

If the remedial action prevents the likelihood of serious harm to some individuals within a larger group of individuals whose information was compromised in a data breach, notification to those individuals for whom harm has been prevented is not required.

Yes

If your entity has **reasonable grounds to believe** that it has experienced an eligible data breach, your entity must promptly notify individuals and the OAIC about the breach, unless an exception applies. Proceed to the next step.

No

If no (the data breach is not 'eligible'), consider whether you have obligations outside of the Privacy Act that relate to personal information protection and responding to a data breach (e.g. state-based or international data protection laws). See **Other obligations** in Part 1: Data breaches and the Australian Privacy Act | OAIC. You should also review the data breach and take action to prevent future breaches.

Unsure

If your entity **suspects that it may have** experienced an eligible data breach, it must quickly assess the situation to decide whether there has been an eligible data breach. Your entity must take all reasonable steps to complete this assessment within 30 calendar days after the day you become aware of the grounds/information that caused you to suspect an eligible data breach.

If the data breach affects one or more other entities that jointly hold the personal information, only one entity needs to assess the data breach. See '**Data breaches involving more than one entity**' in Part 4: Notifiable Data Breach (NDB) Scheme | OAIC.

For guidance on how to assess the data breach, and if you can't reasonably complete an assessment within 30 days, see Assessing a suspected data breach.

If, during the assessment, it becomes clear that there has been an eligible data breach, proceed to the next step.

Next step

Resources

See '**Is serious harm likely?**' in Identifying eligible data breaches,
See '**Preventing serious harm with remedial action**' in Identifying eligible data breaches
See Assessing a suspected data breach

Step 3

Does an **exception** to the notification obligations apply?

Because your entity has experienced an eligible data breach and has not been able to mitigate the likelihood of serious harm, your entity must notify individuals at risk of serious harm and provide a statement to the OAIC as soon as practicable, **unless an exception applies**.

The exceptions to the notification obligations relate to:

- eligible data breaches of other entities (explained in final paragraph below)
- enforcement related activities
- inconsistency with secrecy provisions
- declarations by the OAIC.

In addition, if you have notified (or are required to notify) the OAIC and the My Health Record System Operator of a data breach under s 75 of the My Health Records Act, you are not required to separately notify under the NDB scheme.

If the eligible data breach applies to multiple entities, only one entity needs to notify the OAIC and individuals at risk of serious harm. It is up to you and the other entity/entities to decide who notifies. Generally, the entity with the most direct relationship with the individuals at risk of serious harm should undertake the notification. If it is decided that your entity will undertake the notification, proceed to the next step.

Yes

Yes (an exception applies) – review the OAIC's guidance to understand the requirements of each exception, as you may still need to partially comply with the notification obligations, for example by only notifying the OAIC: see Exceptions to notification obligations and '**Data breaches involving more than one entity**' in Part 4: Notifiable Data Breach (NDB) Scheme | OAIC.

In addition, consider whether you have obligations outside of the Privacy Act that relate to personal information protection and responding to a data breach (e.g. state-based or international data protection laws). See '**Other obligations**' in Part 1: Data breaches and the Australian Privacy Act | OAIC. You should also review the data breach and take action to prevent future breaches.

No

No (an exception does not apply) — proceed to the next step.

Next step

Resources

See '**Data breaches involving more than one entity**' in Part 4: Notifiable Data Breach (NDB) Scheme | OAIC
See Exceptions to notification obligations

Step 4

Notify individuals and the OAIC

Because your entity has experienced an eligible data breach, and has not been able to mitigate the likelihood of serious harm, your entity must **notify individuals at risk of serious harm and provide a statement to the OAIC as soon as practicable**.

How to notify the OAIC

To notify the OAIC of your eligible data breach, use the OAIC's online Notifiable Data Breach form. To see the type of information the OAIC needs, view this read only training version.

How to notify individuals

There are three options for notifying individuals at risk of serious harm, depending on what is 'practicable' for your entity. These options (and what information to include, and what communications method to use) are outlined in Assessing a suspected data breach under the subheading 'Who needs to be notified?'.

The OAIC expects practical steps to be provided to affected individuals based on the kinds of information involved in the data breach. As part of this your entity may wish to refer affected individuals to the OAIC's practical guidance on how to reduce their risk of harm, the OAIC's list of Data breach support and resources | OAIC, and/or this poster.

Notifications to affected individuals should be written in plain English so they are clear and easy to understand. Avoid complex terms or technical jargon.

◯ **Yes**

I have notified individuals and the OAIC. You should also consider reporting the data breach to other relevant bodies, and, if your entity operates in multiple jurisdictions, consider if you have notification obligations under other breach notification schemes. See '**Other obligations**' in Part 1: Data breaches and the Australian Privacy Act | OAIC.

You should further review the data breach and take action to prevent future breaches.

◯ **No**

I have not notified individuals and the OAIC. You will be in breach of your notification obligations under the NDB scheme. You must notify individuals and the OAIC as soon as practicable.

Resources

See '**Notifying individuals about an eligible data breach**' in Assessing a suspected data breach
See Report a data breach | OAIC