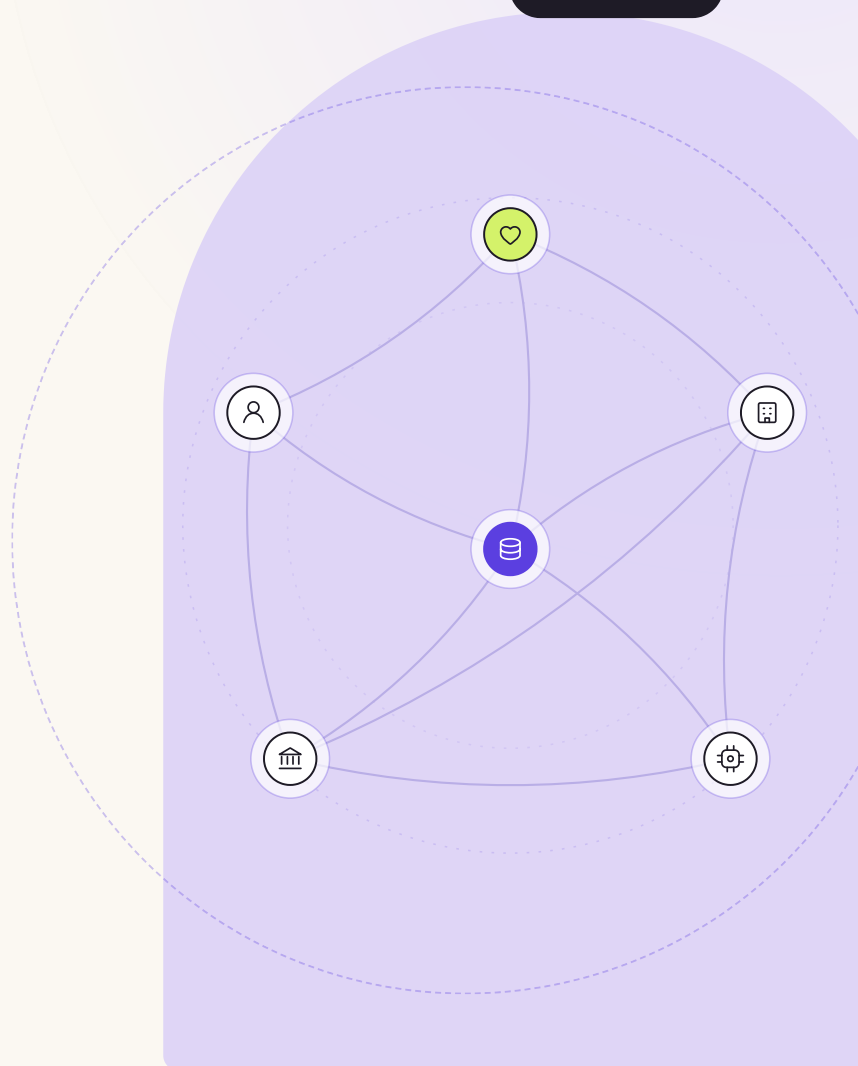




 GUIDE · PRIVACY & DATA PROTECTION

Is it an eligible data breach? An assessment guide

How to work out whether a suspected breach must be notified under the Notifiable Data Breaches scheme, step by step.

Not every data breach has to be notified. Under Part IIIC of the Privacy Act 1988, the Notifiable Data Breaches (NDB) scheme requires notification only of an **eligible data breach**. Deciding whether a breach meets that test has to be fast, reasoned and documented.

This guide focuses on that assessment. For the overall response sequence of contain, assess, notify and review, see our [data breach response checklist](#).

When the assessment duty starts

If an entity has reasonable grounds to suspect there may have been an eligible data breach, it must carry out a reasonable and expeditious assessment, and take all reasonable steps to complete it within **30 days** (section 26WH). The 30 days run from when the entity becomes aware of the grounds for suspicion, not from when the breach occurred.

The OAIC expects entities to treat 30 days as a maximum. If an assessment genuinely cannot be finished in time, the OAIC recommends documenting the reasonable steps taken, the reasons for the delay, and why the assessment was still reasonable and expeditious. The OAIC also suggests three stages: **initiate** (decide an assessment is needed and who is responsible), **investigate** (quickly gather the facts) and **evaluate** (decide whether it is an eligible data breach).

The three criteria

Under section 26WE, there is an eligible data breach when all three of these are met:

1. **Unauthorised access, unauthorised disclosure or loss.** There is unauthorised access to, or unauthorised disclosure of, personal information the entity holds, or the information is lost in circumstances where unauthorised access or disclosure is likely to occur.
2. **Likely serious harm.** A reasonable person would conclude the access or disclosure would be likely to result in serious harm to any of the individuals the information relates to.
3. **No prevention by remedial action.** The entity has not been able to prevent the likely risk of serious harm with remedial action.

Where lost information is unlikely to be accessed, for example because a device was wiped remotely or strongly encrypted, the OAIC says there is no eligible data breach.

Assessing “likely to result in serious harm”

“Likely” means more probable than not, not merely possible. The OAIC says serious harm may include serious physical, psychological, emotional, financial or reputational harm, with examples

such as identity theft, significant financial loss, threats to physical safety and humiliation or damage to reputation.

Section 26WG sets out the matters relevant to whether serious harm is likely. They are not exhaustive:

- ☐ The kind or kinds of information involved
- ☐ The sensitivity of the information
- ☐ Whether it is protected by one or more security measures, and the likelihood those measures could be overcome
- ☐ The persons, or kinds of persons, who have obtained or could obtain it
- ☐ If a security technology or methodology designed to make it unintelligible or meaningless was used, the likelihood that the persons who have it, or could obtain it, intend to cause harm and have or could get the knowledge needed to get around that technology
- ☐ The nature of the harm
- ☐ Any other relevant matters

Assess harm from the affected individuals' point of view, and consider combinations: a name alone differs from a name with identity document numbers.

The remedial action exception

Under section 26WF, if the entity takes action that means the access, disclosure or loss would not be likely to result in serious harm, it is not an eligible data breach. For lost information, the action must prevent the unauthorised access or disclosure. Remedial action can happen at any time, including during the assessment. Record what was done and the evidence it worked.

A simple decision flow

1. Do you have reasonable grounds to suspect an eligible data breach? If yes, start the assessment and note the date. The 30-day period has begun.
2. Is personal information involved, and does your organisation hold it? If no, the NDB scheme may not apply, but record why.
3. Has there been unauthorised access, unauthorised disclosure, or loss likely to lead to either? If no, record the reasons and close the assessment.

4. Weighing the section 26WG matters, would a reasonable person conclude serious harm to any individual is more probable than not? If no, record the reasons and close.
5. Has remedial action removed the likelihood of serious harm? If yes, record the action and evidence. It is not an eligible data breach.
6. If not, it is an eligible data breach. Move to notification without waiting for the 30 days to run out.
7. Check whether another entity also holds the information, and whether a statutory exception applies.

Notification options

Once an entity is aware there are reasonable grounds to believe there has been an eligible data breach, it must prepare a statement and give it to the Commissioner as soon as practicable (section 26WK). The statement must include the entity's identity and contact details, a description of the breach, the kinds of information involved, and the steps individuals should take in response. Other entities involved may be named.

Under section 26WL, the entity must then notify individuals as soon as practicable, using one of three options:

- **Notify everyone** whose information was involved.
- **Notify only those at risk** of serious harm.
- **Publish the statement** on its website and take reasonable steps to publicise it, but only if the first two options are not practicable.

Other exceptions exist in limited cases, including for enforcement-related activities (section 26WN), inconsistency with secrecy provisions (section 26WP) and Commissioner declarations (section 26WQ).

Breaches involving more than one entity

Where personal information is held jointly, for example by your organisation and a cloud provider or contractor, an eligible data breach of one is generally an eligible data breach of each. One entity's assessment satisfies the assessment requirement for the others (section 26WJ), and notification by one satisfies the notification requirement for the others (section 26WM). If no entity notifies, each may be in breach. The OAIC suggests the entity with the most direct relationship with the affected individuals should usually notify them. Agree who does what early, ideally in the contract.

Next step

If your organisation has not yet tested how it would run this assessment under time pressure, a tabletop exercise on a realistic scenario is a useful start. Lexora's data protection review includes a look at breach assessment and notification readiness.

General information, not legal advice. If you are assessing a breach now, contact your legal adviser and refer to the OAIC's guidance.

Sources

1. Privacy Act 1988 (Cth), Part IIIC, Federal Register of Legislation
<https://www.legislation.gov.au/C2004A03712/latest/text>
2. OAIC, Data breach preparation and response, Part 4 Notifiable Data Breach (NDB) scheme
<https://www.oaic.gov.au/privacy/notifiable-data-breaches/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme>



Better governance. *Greater confidence.*

Lexora is an Australian-first advisory business. We help organisations understand their privacy, data and AI obligations, assess risk, build governance frameworks and put practical controls in place.

OUR PRACTICES

Privacy & Data Protection

AI Governance & Responsible AI

Data Governance

Regulatory Readiness & Compliance

WAYS TO START

Privacy Health Check

AI Governance Readiness Assessment

Data Governance Review

Regulatory Readiness Consultation

DISCUSS YOUR GOVERNANCE NEEDS

lexoraai.com.au

info@lexoraai.com.au

More free guides: lexoraai.com.au/resources

This guide is general information, current at the date shown. It is not legal advice and does not take account of your circumstances. Lexora is not a law firm. Check the primary sources before relying on any date or requirement. © 2026 Lexora. You are welcome to share this guide unaltered, with this page attached.