



LEXORA RESOURCES · CHECKLIST

Data breach response checklist

What to do, in order, when you suspect
personal information has been lost or accessed
without authorisation.

Under the Notifiable Data Breaches scheme, an organisation that suspects an eligible data breach must take reasonable steps to assess it within **30 days**, and must notify affected individuals and the OAIC as soon as practicable if it is an eligible data breach. The OAIC describes four steps: contain, assess, notify and review.

1. Contain

- ☐ Stop the breach where you can: revoke access, recover records, isolate systems.
- ☐ Preserve evidence. Do not delete logs or wipe devices.
- ☐ Start a written record of what happened, when, and who did what.

2. Assess

- ☐ Identify what personal information is involved and whose.
- ☐ Assess whether serious harm to any individual is likely, and whether remedial action can prevent it.
- ☐ Complete the assessment within 30 days of becoming aware of the suspected breach.

3. Notify

- ☐ If it is an eligible data breach, prepare the statement to the OAIC.
- ☐ Notify affected individuals as soon as practicable, with what happened and what they should do.
- ☐ Brief your legal adviser and, where relevant, insurers and other regulators.

4. Review

- ☐ Identify the cause and fix it.
- ☐ Update your response plan and run a tabletop exercise on the lessons learned.

General information only, not legal advice. If you are dealing with a breach now, contact your legal adviser and use the OAIC's guidance.

Sources

1. OAIC, Data breach preparation and response guide

<https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response>

2. OAIC, Notifiable Data Breaches scheme

<https://www.oaic.gov.au/privacy/notifiable-data-breaches>

About Lexora. Privacy, Data & AI Governance Advisory. We help organisations navigate privacy obligations, govern information responsibly and manage the risks of artificial intelligence. Contact info@lexora.global · lexoraai.com.au

This resource 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. © Lexora. You may share this document unaltered within your organisation.