Australian Government

Office of the Australian Information Commissioner

Applicable notifiable data breach obligations for accredited entities

November 2026



OAIC

Contents

NDB obligations 3

- APP entities 3
- State or Territory government entities 3
- Small business operators 4

Additional notification obligations 4

NDB obligations

In Australia's Digital ID System, all accredited entities providing accredited services have data breach notification obligations, including small business operators under the *Privacy Act 1988* (Cth) (the Privacy Act).

These obligations arise from either the Notifiable Data Breaches (NDB) scheme in Part IIIC of the Privacy Act, or from state or territory legislation with a comparable data breach notification scheme.

A data breach occurs when personal information is accessed or disclosed without authorisation or is lost in circumstances where unauthorised access or disclosure is likely to occur. For entities covered by the NDB scheme in the Privacy Act, it requires the entity to notify affected individuals and the OAIC when a data breach involving personal information is likely to result in serious harm to individuals.

All accredited entities providing accredited services also have obligations under the *Digital ID (Accreditation) Rules 2024* (rule 4.45) to have a data breach response plan, which includes a communications plan. This plan should ensure clear lines of internal escalation and timely notifications to affected individuals and third parties in the event of a data breach. See the OAIC's guidance on preparing a data breach response plan for further information.

The applicable data breach notification obligations for different entities are set out below.

APP entities

Accredited entities who are APP entities under the Privacy Act will need to comply with the NDB scheme in the Privacy Act in relation to data breaches affecting their accredited services. As APP entities, these entities are already subject to the NDB scheme for all their activities.

The OAIC has detailed guidance on managing data breaches and complying with the NDB scheme, including a data breach preparation and response guide. See this webpage on the OAIC website for a range of resources.

State or Territory government entities

The applicable data breach notification obligations for a State or Territory government entity will depend on the entity's existing obligations.

For accredited entities that are State or Territory agencies covered by a data breach notification scheme that is comparable to the NDB scheme, that State or Territory scheme will apply to the entity's provision of accredited services. Accredited entities in this category must comply with that State or Territory based notification scheme and should refer to their State or Territory regulator for further guidance. Guidance on the OAIC's website provides links to applicable State and Territory privacy regulators.

For accredited entities that are State or Territory agencies who are not covered by a data breach notification scheme that is comparable to the NDB scheme, section 40 of the *Digital ID Act 2024* (Cth) (the Digital ID Act) extends the Privacy Act NDB scheme to apply to their provision of accredited services.

Small business operators

For accredited entities who are small business operators under the Privacy Act, section 40 of the Digital ID Act extends the Privacy Act NDB scheme to apply to their provision of accredited services. Small business operator relying parties are only required to comply with the Privacy Act NDB scheme if the Privacy Act otherwise applies to their acts or practices outside of their participation in Australia's Digital ID System.

Additional notification obligations

The Digital ID Act creates additional notification obligations where an accredited entity is required to notify the OAIC or a State or Territory regulator of a data breach.

For entities covered by the NDB scheme in the Privacy Act who are required under s 26WK of the Privacy Act to notify the OAIC of a data breach, the Digital ID Act requires the entity to give a copy of that statement to the Digital ID Regulator at the same time as the notification is given to the OAIC.[1]

For entities covered by a comparable State or Territory scheme who are required to notify their State or Territory regulator of a data breach, the Digital ID Act requires the entity to give a copy of that statement to both the OAIC and the Digital ID Regulator at the same time as the notification is given to their regulator.[2]

[1] ss 39(2) and 40(4) of the Digital ID Act.

[2] s 41(2) of the Digital ID Act.