Global Data Privacy and Cybersecurity Handbook - Australia

Breach Notification Requirements

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last review date: 31 December 2023*

Yes.

The Privacy Act uses the term "eligible data breach" to describe data breaches, which are subject to the NDB scheme.

An "**eligible data breach**" is when there is an unauthorized access, disclosure, or loss of personal information and a reasonable person would conclude that this is likely to result in serious harm to any of the individuals to whom the personal information relates.

There are several exceptions from the requirements to notify eligible data breaches:

Where another APP entity has already met the NDB scheme requirements

Where compliance by a law enforcement body would be likely to prejudice its enforcement-related activities

Where notification would be inconsistent with a Commonwealth secrecy provision

Where the OAIC grants an exception (note that an APP entity would need to apply for an exception in order for the OAIC to grant one)

Notification obligations apply in respect of the breach under the MHR Act (see question 19)

It should also be noted that, where sufficient remedial action is taken in response to a data breach and this eliminates the likelihood of serious harm, there will not be an eligible data breach for the purposes of the Privacy Act, and notifications will not be required.

Finally, even where an eligible data breach has not occurred and so notifications are not mandated, an organization might choose to voluntarily go public about data breaches that have affected them, for public relations and/or risk mitigation reasons.

Note also that:

Section 26WH of the Privacy Act provides that if an entity is aware that there are reasonable grounds to suspect that there may have been an eligible data breach of the entity, but is not aware that there are reasonable grounds to believe that this amounts to an eligible data breach of the entity, the entity must carry out a "reasonable and expeditious assessment" of whether there are in fact reasonable grounds to believe that the relevant circumstances amount to an eligible data breach of the entity. The entity must take all reasonable steps to ensure that the assessment is completed within 30 days after the entity becomes aware.

The NDB scheme is under consideration as part of the government's wider review of the Privacy Act, so there may be changes in the future.

The review of the Privacy Act considered the NDB scheme and whether any changes should be made to it. The report recommends that:

media organizations should be required to comply with the reporting obligations in the NDB scheme, and

the NDB scheme should be extended to cover de-identified data where access or disclosure would be likely to result in serious harm because of the risk of re-identification together with the sensitivity of the information and other relevant harm factors.

The [Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 (Cth)](https://www.legislation.gov.au/Series/C2022A00083) enhanced the OAIC's powers with respect to the NDB scheme, allowing the OAIC to (i) pre-emptively assess a business' compliance with the NDB scheme, regardless of whether a "eligible data breach" has occurred; and (ii) declare that a business which has suffered an "eligible data breach" to engage an independent and suitably qualified external advisor to assist in rectifying the business' information security practices. The appointment of such an advisor would be at the business' own cost.

In NSW, the [Privacy and Personal Information Protection Amendment Act 2022 (NSW)](https://www.parliament.nsw.gov.au/bills/Pages/bill-details.aspx?pk=4040) commenced on 28 November 2023, making changes to the PPIP Act to introduce a mandatory notification of data breach (MNDB) scheme for NSW public sector agencies. In effect, the amendments mirror the NDB scheme in the Privacy Act for NSW-based public agencies which sit outside the scope of the Privacy Act. The amendments also empower the NSW Information and Commission to investigate, monitor and audit compliance with the new MNDB scheme and provide guidance for agencies now regulated by the scheme.. Queensland has also passed the [Information Privacy and Other Legislation Amendment Act 2023](https://www.legislation.qld.gov.au/view/whole/html/asmade/act-2023-032) (Qld) which introduces its own mandatory data breach scheme for the state public sector and will commence on a day to be proclaimed.

Other than in NSW and QLD, there are currently no other State- or Territory-specific regulations concerning notification about data breaches.

# Controllers/ Owners have to notify:

*Last review date: 31 December 2023*

☒        data protection authorities

Unless an exception applies, an APP entity must prepare and provide the OAIC a copy of a statement in accordance with section 26WK of the Privacy Act. The statement must set out the matters described in section 26WK(3), being:

The identity and contact details of the entity

A description of the eligible data breach

The particular kind or kinds of information concerned

Recommendations about the steps that individuals should take in response to the eligible data breach

Section 26WK(4) also notes that, if an APP entity has reasonable grounds to believe that its eligible data breach is an eligible data breach of one or more other entities, the statement it provides to the OAIC may also set out the identity and contact details of those other entities.

Section 26WK(1) of the Privacy Act provides that "This section applies if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity," and section 26WK(2) requires the above statement to be prepared and given "as soon as practicable after the entity becomes so aware."

☐       cybersecurity authorities

There is currently no general obligation for all APP entities to notify a separate cybersecurity regulator regarding a data breach. However, there are sector-specific notification obligations in relation to certain incidents (see the later response on this).

☒        affected individuals

Unless an exception applies, an APP entity must take reasonable steps to notify the contents of the statement provided to the OAIC in accordance with section 26WL of the Privacy Act either:

To each individual to whom the relevant information relates

To each individual who is at risk of serious harm from the eligible data breach

Where neither of the above is practicable, the APP entity must publish the statement on its website and take reasonable steps to publicize its contents.

Section 26WL(1) of the Privacy Act provides that "This section applies if: (a) an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity; and (b) the entity has prepared a statement that: (i) complies with subsection 26WK(3); and (ii) relates to the eligible data breach that the entity has reasonable grounds to believe has happened." Section 26WL(3) of the Privacy Act provides that "The entity must comply with subsection (2) as soon as practicable after the completion of the preparation of the statement".

☒        other

The Privacy Act does not require APP entities to notify other bodies, but the guidance issued by the OAIC suggests that consideration be given to notifying the Federal Police, insurers, credit card companies, professional regulatory bodies and/or any government agency that has an association with the relevant information.

Sector-specific or non-privacy related data breach notification requirements may apply in some instances (see the later response on this point).

The PIPP Act broadly replicates the mechanics of the NDB scheme, as set out in the Privacy Act, to NSW-based public sector agencies.

Additionally, it is always open to notify the Australian Cyber Security Centre of any cybersecurity incidents.

# Processors/ Agents have to notify:

*Last review date: 31 December 2023*

☐        controller/ owner

Same as for controllers.

☒        data protection authorities

Same as for controllers.

☐        cybersecurity authorities

Same as for controllers.

☒        affected individuals

Same as for controllers.

☒        others

Same as for controllers.

The report on the review of the Privacy Act proposed that the law should be amended so that only controllers are responsible for notifying individuals affected by an eligible data breach. However, processors would continue to be required to prepare a statement on the breach and provide a copy to the OAIC, unless the breach has already been reported by another entity. The government response to the review report does not specifically discuss whether it agrees with this proposal, but it does support introducing a controller / processor distinction to recognize that different entities have differing degrees of control over the handling of personal information.