Global Data and Cyber Handbook - Australia

Security Requirements and Breach Notification

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

# Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last review date: 31 December 2024*

☒ Yes

☒         general obligation to take appropriate / reasonable technical, physical and/or organizational security measures

APP 11 requires APP entities to take reasonable steps in the circumstances to protect information from (i) misuse, interference and loss; and (ii) unauthorized access, modification or disclosure. The review of the Privacy Act considered whether current security requirements are reasonable or appropriate. There is no specific obligation in the Privacy Act to adopt particular security measures or conduct third party due diligence but amendments made to the Privacy Act in December 2024 in response to the review of that Act clarify that reasonable steps in this context include technical and organizational measures. Additionally, the OAIC's [APP Guidelines](https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information#taking-reasonable-steps) and [Guide to securing personal information](https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information) (note the latter is in the process of being updated) indicate that reasonable steps should include implementing strategies regarding access and physical security, and third party providers. Other reform proposals included that there should be a set of baseline privacy outcomes under APP 11. This proposal is expected to be addressed in later reforms to the Privacy Act.

Additional requirements apply to the security of CDR data. Broadly speaking, the requirements for accredited data recipients are to: (i) define and implement security governance in relation to CDR data; (ii) and define the boundaries of the CDR data environment; (iii) have and maintain an information security capability; (iv) implement a formal controls assessment program; and (v) manage and report security incidents. The Digital ID system is also subject to its own special security regime. The legislation setting a minimum age for social media access also contains a set of additional privacy safeguards.

# Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last review date: 31 December 2024*

☒         health regulatory requirements

☒         financial services requirements

☒         telecommunication requirements

☒         providers of critical infrastructure

☒         other

There are no broadly applicable legal requirements that specifically require businesses to proactively protect systems against cyberattacks. Instead, APP 11 requires an APP entity to ensure that reasonable steps are taken in the circumstances to protect information from misuse, interference and loss and from unauthorized access, modification or disclosure. Additionally, where an entity suffers a cyberattack that involves an "eligible data breach," it will be required to report the attack through the NDB scheme in the Privacy Act. As many businesses store and process personal information digitally, this effectively requires them to take at least reasonable cybersecurity measures to protect systems used to store or process that personal information.

Various other sector-specific laws and rules require security measures to be taken. For example:

As well as registration and incident reporting obligations, the SOCI Act provides that the Minister for Home Affairs can issue a direction to an owner or operator of a critical infrastructure asset to mitigate national security risks, and address serious deficiencies within their risk management programs. Such directions could relate to cybersecurity measures. Additionally, there are enhanced cyber security obligations for responsible entities for systems of national significance; such entities are required to have incident response plans, conduct cyber security exercises and vulnerability assessments, and provide access to system information on request.

APRA CPS 234 on Information Security requires prudentially-regulated entities to take information security measures, and those entities are also expected to take account of CPG 235 on Managing Data Risk.

Financial services licensees have obligations to do all things necessary to ensure that the services covered by their license are provided efficiently, honestly and fairly and to have adequate risk management systems. This has been interpreted as requiring licensees to take steps relating to cybersecurity and cyber resilience and in 2022, the Federal Court [found](https://asic.gov.au/about-asic/news-centre/find-a-media-release/2022-releases/22-104mr-court-finds-ri-advice-failed-to-adequately-manage-cybersecurity-risks/) for the first time that a licensee had breached its license by having inadequate cyber security risk management in place.

Under the Telecommunications Act, carriers, carriage service providers and carriage service intermediaries have been required to protect networks and facilities from unauthorized access and interference, maintaining "competent supervision" and "effective control" over their telecommunications networks and facilities. Additionally, the Telecommunications Act requires various actors in the telecommunications sector to protect the confidentiality of certain information relating to communications. These obligations necessarily require regulated entities to take cybersecurity measures to protect their systems and communications. Certain aspects of the 2024 Cyber Security Legislative Package will impact this status quo to an extent. Once the relevant aspects of those reforms commence, critical telecommunications assets will be regulated under the SOCI Act, rather than under the Telecommunications Act, and will be subject to enhanced security obligations under the SOCI Act.

Specific security requirements are in place for the My Health Records system, and the system operator may deny, cancel or suspend an entity's registration for the system if it believes the entity may compromise the security or integrity of the system. Other health records laws also contain general obligations to keep health records secure and/or confidential. Given that many records are stored and processed digitally, compliance would involve taking cybersecurity measures.

The Cyber Security Act 2024 (Cth) contemplates that manufacturers and suppliers will be required to comply with minimum security standards for smart (IoT) devices acquired in Australia, with the standards to be specified in legislative instruments. An exposure draft of the [Cyber Security (Security Standards for Smart Devices) Rules 2024](https://www.cisc.gov.au/resources-subsite/Documents/cyber-security-security-standards-for-smart-devices-rules.pdf) sets out the proposed standards and exemptions for certain devices. The Australian government is conducting public consultation to develop these Rules from 16 December 2024 to 13 February 2025. It is not yet clear when any such standards will come into effect.

Company directors also have a statutory duty of care. Arguably, depending on the circumstances, if a director is found to be responsible for their company breaching the law due to a cybersecurity failing, the director might be found to have breached their duty. In this regard, ASIC has issued guidance in relation to [Cyber Resilience](https://asic.gov.au/regulatory-resources/corporate-governance/cyber-resilience/) and the Australian Institute of Company Directors has issued [Cyber Security Governance Principles](https://www.aicd.com.au/risk-management/framework/cyber-security/cyber-security-governance-principles.html) and guidance on [Governing Through a Cyber Crisis](https://www.aicd.com.au/good-governance/it/cyber-safety/governing-through-a-cyber-crisis.html), which provides a framework of better practice guidance to assist Australian directors to navigate critical cyber incidents at their organizations.

Public sector agencies are also subject to security requirements as a matter of government policy (e.g., see the Commonwealth [Protective Security Policy Framework (PSPF)](https://www.protectivesecurity.gov.au/)), which does not have the force of law but with which Australian government entities are expected to comply. The ISM also provides guidance on cybersecurity measures but compliance is not generally mandatory. Additionally, from December 2024 – 28 February 2025, the Australian government is [consulting](https://www.homeaffairs.gov.au/cyber-security-subsite/Pages/commonwealth-cyber-security-policy-consultation-package.aspx) on Guiding Principles to embed Zero Trust Culture, seeking feedback to help shape policies about Commonwealth cyber security resilience.

# Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

*Last review date: 31 December 2024*

☒         Data privacy

☒         Securities or public company

☒         network information security

☒         health

☒         financial services

☒         telecommunications

☒         critical infrastructure

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

*Last review date: 31 December 2024*

☒  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 was considered as part of the government's wider review of the Privacy Act, so there may be changes in the future. In particular, the review report recommended – and the government agreed in principle – that:

Notification statements should be provided to OAIC no later than 72 hours after the entity becomes aware of the "eligible data breach," with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours, and

Media organizations should be required to comply with the reporting obligations in the NDB scheme.

These proposals are expected to be addressed in Tranche 2 reforms to the Privacy Act.

The OAIC is empowered to pre-emptively assess a business' compliance with the NDB scheme, regardless of whether an "eligible data breach" has occurred, and declare that a business that 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 (commencement is [expected to occur](https://www.oic.qld.gov.au/training-and-events/ipola) on 1 July 2025, with the data breach notification requirements taking effect one year later).

Western Australia has also passed the [Privacy and Responsible Information Sharing Act 2024 (WA)](https://www.legislation.wa.gov.au/legislation/statutes.nsf/law_a147470.html) and an associated [Information Commissioner Act 2024 (WA)](https://www.legislation.wa.gov.au/legislation/statutes.nsf/law_a147471.html&amp;view=consolidated). Among other things, the former establishes a mandatory information breach notification scheme for the public sector. However, this and other aspects of the legislation are awaiting commencement, on a date to be proclaimed.

Other than as indicated above, 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 2024*

☒         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."

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 and reporting obligations may apply where ransomware payments are made (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. Similar requirements will apply for Queensland public sector agencies after the [Information Privacy and Other Legislation Amendment Act 2023](https://www.legislation.qld.gov.au/view/whole/html/asmade/act-2023-032) (Qld) commences (commencement is [expected to occur](https://www.oic.qld.gov.au/training-and-events/ipola) on 1 July 2025, with the data breach notification requirements taking effect one year later). Western Australia has also passed legislation establishing a mandatory information breach notification scheme for the public sector. However, this and other aspects of the legislation are awaiting commencement, on a date to be proclaimed.

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 2024*

Same as for controllers.

☒         data protection authorities

Same as for controllers.

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.

# Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last review date: 31 December 2024*

☒  Yes

☒         public company obligations (e.g., to notify security incidents that may materially affect an investor's decision)

ASX Listing Rules subject participants in the ASX to continuous disclosure obligations. Listing Rule 3.1, which is given statutory force by section 674 of the *Corporations Act 2001* (Cth), requires that (unless an exception applies) once an entity is or becomes aware of information concerning it that a reasonable person would expect to have a material effect on the price or value of the entity's securities, the entity must immediately tell the ASX that information. This could include a privacy or security breach, depending on the nature and extent of the breach.

Although there is currently no general requirement to notify cybersecurity authorities of non-personal data security breaches, entities in certain sectors (see further details below) are required to notify authorities of cybersecurity incidents. Additionally, in late 2024, the Cyber Security Act introduced a mandatory ransomware and cyber extortion reporting obligation for certain businesses to report ransom payments made by them or on their behalf to a designated body within 72 hours of making the payment or becoming aware that it was made. This obligation will commence on a date to be proclaimed, or no later than 1 June 2025. This obligation will mean that, in practice, many non-personal data breaches will come to the attention of the Australian authorities.

☒         health regulatory requirements (e.g., to notify incidents affecting safety of medical devices)

Under section 75 of the MHR Act, participants in the My Health Record system must notify the ADHA (and the OAIC - unless the participant is a State or Territory authority or an instrumentality of a State or Territory) as soon as practicable after becoming aware that:

A person has, or may have, contravened the MHR Act in a manner involving an unauthorized collection, use or disclosure of health information included in a My Health Record

An event has, or may have, occurred or circumstances have, or may have, arisen that compromise, may compromise, have compromised or may have compromised, the security or integrity of the My Health Record system

The contravention, event or circumstances directly involved may have involved or may involve the entity. The ADHA then has an obligation to notify the OAIC of any eligible data breach involved in the reported matter.

☒         financial services requirements

For prudentially-regulated institutions overseen by the Australian Prudential Regulation Authority (APRA), which include banks, insurers, superannuation funds and other financial institutions, [Prudential Standard CPS 234](https://www.legislation.gov.au/Series/F2018L01745) on Information Security requires "APRA-regulated entities" to notify APRA of any material "information security incident." An "information security incident" includes any actual or potential compromise of information security, whether or not it involves personal information. Under [Prudential Standard CPS 230](https://www.apra.gov.au/sites/default/files/2023-07/Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management%20-%20clean.pdf) on Operational Risk Management, which is [expected](https://www.apra.gov.au/news-and-publications/apra-provides-an-update-on-implementation-of-new-operational-risk-standard) to be in effect from 1 July 2025, APRA-regulated entities will be required to notify APRA as soon as possible, and not later than 72 hours, after becoming aware of an operational risk incident that is determined to be likely to have a material financial impact or a material impact on the ability of the entity to maintain its critical operations.

Additionally, notification obligations under the SOCI Act apply to responsible entities for critical infrastructure assets in the financial services and markets sector (see below).

☒         telecommunication requirements

Under Part 14 of the Telecommunications Act, carriers and certain carriage service providers must notify the ACMA of changes to telecommunications services or telecommunications systems that are likely to have a material adverse effect on their capacity to comply with their duty to do their best to protect telecommunications networks and facilities from unauthorized interference or unauthorized access for the purposes of security. No deadline for the notification is specified in the legislation.

Carriers and eligible carriage service providers can also be subject to cyber security incident notification obligations in respect of critical telecommunications assets (see below).

☒         providers of critical infrastructure

Pursuant to section 24 of the SOCI Act, if a notifiable event occurs in relation to a **critical infrastructure asset** (including critical telecommunications assets), the relevant reporting entity for that asset must notify the Secretary for Home Affairs in the approved form and by the end of 30 days after the event occurs. Notifiable events include where operational information in relation to the asset previously obtained by the Secretary for the purposes of the SOCI Act becomes incorrect or incomplete. Additionally:

If a responsible entity becomes aware that a cyber security incident has occurred or is occurring and that that incident has had, or is having, a significant impact (whether direct or indirect) on the availability of a critical infrastructure asset for which it is responsible, it must notify the relevant government department "as soon as practicable, and in any event within 12 hours, after the entity becomes so aware." If such a report is given orally, a copy of a written record of that report must be provided to the relevant government department "within 84 hours after the report is given"

If a responsible entity becomes aware that another cyber security incident is occurring, has occurred or is imminent, and that that incident has had, is having, or is likely to have a relevant impact on a critical infrastructure asset for which it is responsible, it must report to the relevant department "as soon as practicable, and in any event within 72 hours, after the entity becomes so aware." If such a report is given orally, a copy of a written record of that report must be provided to the relevant government department "within 48 hours after the report is given"

Further reporting obligations apply in relation to "systems of national significance" and specific provisions apply in respect of telecommunications networks, although these are generally not specific to notification of security incidents or data breaches. One notable point is that the government has the power to require additional operational reports in respect of computers used to operate systems of national significance where a report might assist with determining whether to exercise government powers under the legislation and whether certain other criteria are met.

☒         other

From 28 November 2023, NSW public sector agencies have also been required to report data breaches to the NSW Information Commissioner under the MNDB scheme added to the PIPP Act, which broadly replicates the provisions of the NDB scheme under the Privacy Act. Similar requirements will apply for Queensland public sector agencies after the [Information Privacy and Other Legislation Amendment Act 2023](https://www.legislation.qld.gov.au/view/whole/html/asmade/act-2023-032) (Qld) commences (commencement is [expected to occur](https://www.oic.qld.gov.au/training-and-events/ipola) on 1 July 2025, with the data breach notification requirements taking effect one year later).

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.