Asia Pacific Insurance - Australia

Data Protection and Cybersecurity

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

# Who is the main regulator with oversight of data privacy matters?

The Office of the Australian Information Commissioner (OAIC)

# What is the main legislation on the protection of personal data privacy?

Privacy Act 1988 (Cth)

# Who is the main regulator with oversight of cybersecurity matters?

There is no particular regulator tasked with oversight of cybersecurity matters per se. The OAIC is the relevant regulator if personal data is involved. The Australian Prudential Regulatory Authority (APRA), the regulator which oversees banks, other financial institutions and insurance industries, provides a set of standards/guidelines in relation to IT security, which applies, among other institutions, to general insurance, life insurance and superannuation industries. The Australian Securities and Investments Commission (ASIC) also may have some oversight of cybersecurity matters in the insurance industry.

# Is there existing legislation governing cybersecurity issues?

The Privacy Act, which governs personal information; the Cybercrime Act 2001; Australian Security Intelligence Organisation (ASIO) Act 1979; Telecommunications (Interception & Access) Act 1979; Telecommunications Act 1997; Spam Act 2003.

# What are the main requirements with respect to collection, use, disclosure or transfer of personal data?

An insurer handling personal information should follow the Australian Privacy Principles (APPs) below:

Open and transparent management of personal information – All entities subject to the Privacy Act must have an APP Privacy Policy.

Anonymity and pseudonymity – Individuals should have an option of not identifying themselves when dealing with an organization, unless this is impracticable or the organization is required by law to deal with an individual on an identified basis.

Collection of solicited personal information – An organization must not collect personal information unless reasonably necessary for one or more of the entity's functions or activities.

Dealing with unsolicited information – Organization must take specific steps if it obtains personal information that it did not specifically solicit.

Notification – Individuals must be provided with a collection statement before or at the time their information is collected.

Disclosure for a primary purpose – Use or disclosure of personal information is not permitted for purposes other than the primary purpose for which it was collected.

Direct marketing – Subject to exceptions, use or disclosure of personal information for direct marketing purposes is not permitted without consent.

Cross-border disclosure of personal information – Entities are required to take reasonable steps to ensure that an overseas recipient of Australian personal information does not breach the APPs, and such entity will remain liable for any misuse by the overseas recipient.

Integrity of personal information – An organization may not adopt a government-related identifier (such as a tax file number) as its own identifier.

Quality of personal information – An organization must take reasonable steps to ensure that personal information it collects, uses or discloses is accurate, up to date and complete.

Security of personal information – An organization must take reasonable steps to protect personal information it holds from misuse, interference and loss as well as from unauthorized access, modification or disclosure.

Access to personal information – Individuals have a right to access their personal information on request.

Correction of personal information – Organizations must take reasonable steps to correct personal information on request by an individual.

# What are the main requirements for ensuring security of personal data?

Under APP 11, an APP entity must take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted to retain personal information. An APP entity that holds personal information must do the following:

take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorized access, modification or disclosure

take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs

# Are there additional requirements with respect to "sensitive personal data"?

"Sensitive information" is defined in the Privacy Act as personal information relating to racial or ethnic origin, political opinions, membership of a political association, professional or trade association or trade union, religious beliefs or affiliations, philosophical beliefs, sexual preferences or practices, criminal record, biometric information or health information. Pursuant to APP 3, an entity must not collect sensitive information unless:

the entity obtains the consent of the individual and the information is reasonable necessary for the activities or functions of the entity

collection is required by law

collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where it is unreasonable or impracticable to obtain the consent of the individual to whom the information relates

the information is collected by a nonprofit organization and relates solely to the organization’s activities and to the organization’s members or persons who have regular contact with the organization in connection with its activities

collection is necessary for the establishment, exercise or defense of a legal or equitable claim

where the entity is a Commonwealth enforcement body, the collection is necessary for the performance of that enforcement body’s functions or activities

the information is collected in the process of providing a health service, and is either collected as authorized by law or subject to a professional code of ethics

the information is collected in the course of medical research that is subject to professional safeguards and where obtaining consent is impracticable, and the research cannot be performed without the information being collected

Unless consent is given for an additional use, sensitive information may only be used for the purpose for which it was collected or for a secondary purpose directly related to the purpose of its collection for which the individual would reasonably expect the information to be used.

Sensitive information is subject to additional and special consent requirements. In non-binding guidelines, the Privacy Commissioner expressed the view that an entity would ordinarily need clear evidence that an individual had consented to it collecting sensitive information.

# Are there additional obligations imposed on insurance companies with respect to collection, use and transfer of personal data of customers? Are there registration requirements to be complied with?

lnsurance companies that are APP entities must comply with their obligations under the Privacy Act as set out in response to questions 5 to 7 above. There are no particular registration requirements to be complied with.

# Are insurance companies required to have a data protection officer?

In Australia, although it is considered best practice to do so, there is no legal requirement to appoint or designate a data privacy officer. However, organizations are required to make available a privacy policy on request from a data subject.

# Do insurance companies need to undertake privacy impact assessments prior to the implementation of new information systems and/or technologies for the processing of personal data?

While not a strict legal requirement, APP 1 requires APP entities to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs and enable them to deal with enquiries or complaints about privacy compliance. In this way, the APPs require “privacy by design,” an approach whereby privacy compliance is designed into projects dealing with personal information right from the start, rather than being bolted on afterward. Conducting privacy impact assessments (PIAs) helps entities to ensure privacy compliance and identify better practice. OAIC guidelines recommend and provide guidance for conducting PIAs for “projects” such as the implementation of new or amended programs, activities, systems or databases. Similarly, conducting PIAs would assist in complying with APRA standards surrounding cybersecurity and managing data risk.

# What are data subjects' rights, if any, in relation to the processing of their personal data?`

Data subjects have the general right to:

be informed by an organization of the personal data the organization holds about the data subject

access the data subject’s personal data, subject to some restrictions and/or qualifications

request the correction of the data subject’s personal data

request the deletion and/or destruction of the data subject’s personal data

# Are there restrictions regarding cross-border transfer of personal data for insurance companies?

If an insurance company discloses personal data to a recipient outside of Australia, it must take reasonable steps to ensure that the offshore recipient (including a related entity) does not breach the APPs. Unless an exception applies, if the recipient handles the personal data in a manner that would breach the APPs if that recipient were subject to the APPs, the organization that disclosed the information will be taken to have breached the APPs.

A key exception is if the recipient to which personal data is disclosed is subject to a law or binding scheme which provides the same protection as under the Privacy Act, and there are mechanisms that the data subject can access to enforce that law or binding scheme. A further exception is if the organization expressly informs data subjects that if information is disclosed outside of Australia, the  
organization will not be responsible for any failure of the recipient to protect the personal data in a manner consistent with the APPs, and having been so informed, the data subject consents to the disclosure.

# Are there specific requirements for insurance companies in relation to the use and transfer of personal data for marketing purposes? Can customers opt out?

Whether businesses can use personal data for direct marketing will depend on how they collected the information (whether it was directly from the relevant data subject or from a third party) and whether individuals would reasonably expect their information to be used for this purpose). There is also an opt-out requirement that applies to all direct marketing communications. Additional restrictions apply to the use of Sensitive Data for direct marketing.

In addition to requirements under the Privacy Act, direct marketing communications are also subject to requirements under the Spam Act 2003, which prohibits the sending of electronic commercial messages without consent and require all such messages to contain certain  
information and an unsubscribe facility. The Do Not Call Register Act 2006 prohibits businesses from contacting individuals on the Do Not Call Register by telephone or fax except in certain restricted circumstances.

To the extent the Spam Act or the Do Not Call Register Act applies, the Privacy Act does not apply.

# Are there specific requirements for insurance companies in relation to the receipt of personal data from its business partners?

Where personal data other than sensitive data is collected from a third party, an insurance company may use that data for direct marketing purposes provided that it has (a) obtained the relevant individual's consent for use of its personal data for those purposes; and (b) provided the individuals with a simple way to opt out of receiving direct marketing communications from the organization.

# Can insurance companies transfer the personal data of their insurance agents or intermediaries to other service providers such as investigation agents or debt collectors?

Insurance companies may disclose personal data of their agents or intermediaries to other service providers if such transfer is the primary purpose for collection, or such transfer is a related secondary purpose and an individual may reasonably expect the insurance company to  
disclose their personal information to such third parties. It is advisable for insurance companies to make such uses of personal data clear in their privacy policies and collection notices. If an individual may not reasonably expect the transfer of their personal data in this way, then their consent must be obtained before doing so.

# Are there additional regulatory requirements imposed with respect to the outsourcing of data processing to third-party data processors?

Organizations that disclose personal data to third parties should ensure there are contractual or other means in place to protect the personal data. In case of a data breach incident, the outsourcing organization may be held liable together with the third-party provider.

When outsourcing/offshoring data management responsibilities, APRA Prudential Standards, which deal specifically with this area, would apply to insurance companies who plan to outsource material business activities. The key requirements of the Prudential Standard are  
that an APRA-regulated institution must:

have a policy, approved by their board, relating to outsourcing of material business activities

have sufficient monitoring processes in place to manage the outsourcing of material business activities

for all outsourcing of material business activities with third parties, have a legally binding agreement in place, unless otherwise agreed by APRA

consult with APRA prior to entering into agreements to outsource material business activities to service providers that conduct their activities outside Australia

notify APRA after entering into agreements to outsource material business activities

# Do insurance companies have to ensure third parties meet certain standards in outsourcing processing to third parties? Are there additional safeguards to be taken?

See response to question 16 above.

APRA Standards applicable to insurance companies expects that a regulated entity would be able to demonstrate the following:

ability to continue operations and meet core obligations following a loss of services

maintenance of the quality of critical or sensitive data

compliance with legislative and prudential requirements

a lack of impediments (from jurisdictional hurdles or technical complications) to APRA being able to fulfill its duties as prudential regulator (including timely access to data in a usable form)

# What is the data retention requirement?

There are no specific data retention requirements under Australian privacy law, though we note that organizations should only retain personal data for as long as it is required to be used for the primary purpose for which it was collected.

# Are there regulatory requirements to have local data centers and disaster recovery processes?

While not a strict legal or regulatory requirement, OAIC guidelines and APRA Prudential Practice Guides indicate the importance of adequate disaster recovery processes as part of an organization's robust IT, cybersecurity and privacy management systems.

# What are the consequences of a data privacy breach? Is it a criminal offense? What is the penalty?

The Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) (Privacy Amendment Act) which will take effect on 23 Feb 2018, will require certain “eligible” data breaches to be notified to the OAIC and affected individuals in accordance with that Act.

Failing to comply with the Privacy Amendment Act would be an "interference with the privacy of an individual," which may amount to a breach of a civil penalty provision of the Privacy Act. The main consequences include the risk of a determination to pay compensation and also the risk of paying civil penalties of an amount up to AUD 2.1 million (for corporations) and AUD 420,000 (for individuals).

# Is there a statutory obligation to disclose data breaches to regulators?

Subject to certain exceptions, under the Privacy Amendment Act, entities that have reasonable grounds to suspect that an eligible data breach has occurred will be required to carry out a “reasonable and expeditious assessment” of the suspected data breach. The entity will need to take reasonable steps to ensure the assessment is completed within 30 days after it becomes aware of the suspected data breach.

If an entity has reasonable grounds to believe that an eligible data breach has occurred, it must promptly notify the affected individuals and OAIC. This will involve:

Preparing a statement setting out the entity’s identity and contact details, a description of the breach, the kind of information concerned and recommendations about what the affected individuals should do in response.

Giving a copy of the statement to the Australian Information Commissioner.

If practicable, taking reasonable steps to notify the contents of the statement to each individual to whom the relevant information relates, or, if it is not practicable to do so, to the individuals who are "at risk" of serious harm from the breach. An entity might choose  
to notify a statement under the first option where it would require an unreasonable amount of resources to assess which affected individuals are “at risk” from an eligible data breach and which are not. On the other hand, the second option may be more practicable  
if an entity is able to ascertain with a high degree of confidence that only some particular individuals are “at risk” from the eligible data breach.

If neither of the above methods are practicable, the entity must publish the statement on its website and take reasonable steps to publicize its content.

# Is there a statutory obligation to disclose data breaches to data owners?

Yes, see response to question 21. The notification obligations require notification to be made to both the OAIC and affected individuals.

# What are the statutory obligations to cooperate with regulators if there is a data breach?

See response to question 21 above.

# Is there a publicly accessible cybersecurity assistance service, such as a computer emergency response team (CERT)?

Yes, CERT Australia provides a range of services, including a hotline, email support, technical guidance on mitigating cyber threats, incident response support and coordination, information sharing and capability building.

# Are there additional consequences which apply in the event of a data privacy breach under cybersecurity laws?

No, the Privacy Amendment Act sets out the primary obligations which apply in the event of a data breach in Australia.

©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 or copying of the Content on this Site without express written authorization is strictly prohibited.