International Comparative Legal Guides

# Data Protection 2026

A practical cross-border resource to inform legal minds

**13th Edition**

Contributing Editors:
**Tim Hickman & Dr. Detlev Gabel**
White & Case LLP


glg Global Legal Group

iclg

# Expert Analysis Chapters



# Q&A Chapters

# Australia

Nyman Gibson Miralis


Dennis Miralis


Jack Dennis


Phillip Salakas


Henry Yu

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

In Australia, there is data protection legislation at a state, territory and federal level. At the federal level, the principal data protection legislation is the *Privacy Act 1988* (Cth) ('**Privacy Act**'), including the Australian Privacy Principles ('**APPs**').

### 1.2 Is there any other general legislation that impacts data protection?

The *Do Not Call Register Act 2006* (Cth) ('**DNCRA**') and *Spam Act 2003* (Cth) ('**Spam Act**') set out limits to direct marketing activities.

At the state and territory level, the legislation concerned with data protection includes, for example:

- the *Information Privacy Act 2014* (ACT);
- the *Privacy and Personal Information Protection Act 1998* (NSW);
- the *Information Privacy Act 2009* (QLD);
- the *Personal Information and Protection Act 2004* (Tas); and
- the *Privacy and Data Protection Act 2014* (Vic).

### 1.3 Is there any sector-specific legislation that impacts data protection?

Privacy issues specific to the telecommunications sector are contained within the *Telecommunications Act 1997* (Cth) ('**Telecommunications Act**') and the *Telecommunications (Interception and Access) Act 1979* (Cth).

Information related to healthcare is further protected under the *My Health Records Act 2012* (Cth) ('**MHR Act**') and the *Healthcare Identifiers Act 2010* (Cth). A multiplicity of state legislation also exists in relation to the protection of health-based privacy.

Businesses in industries such as financial services and gambling must comply with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) and the Anti-Money Laundering and Counter-Terrorism Financing Rules.

The *Security of Critical Infrastructure Act 2018* (Cth) applies to organisations that own or operate (or hold a direct interest in) assets in a range of sectors, including communications, energy, defence, financial services, transport, data processing or storage, supermarket/grocery supply chains, health and medical, education and space.[1]

More generally, Australia has also introduced mandatory data breach notification requirements under the Privacy Act through the Notifiable Data Breaches ('**NDB**') scheme.[2] Under this scheme, APP entities[3] including Australian Government agencies and private sector organisations with an annual turnover exceeding AU$3 million, as well as certain smaller entities such as health service providers and businesses that trade in personal information, must notify affected individuals and the Office of the Australian Information Commissioner ('**OAIC**') (see question 1.4 below) where a data breach is likely to result in serious harm to any individual whose personal information is involved.[4]

Other examples of state, territory and federal legislation that relate to specific data protection or activities include:

- the *Criminal Code Act 1995* (Cth);
- the *National Health Act 1953* (Cth);
- the *Health Records Act 2001* (Vic); and
- the *Workplace Surveillance Act 2005* (NSW).[5]

### 1.4 What authority(ies) are responsible for data protection?

The OAIC is an independent statutory agency which has functions under the Privacy Act and other legislation relating to data protection. These powers have been strengthened in recent reforms, including increased investigative and enforcement powers and significantly higher civil penalties for serious or repeated interferences with privacy.[6]

The Australian Communications and Media Authority ('**ACMA**') is the regulatory authority charged with enforcing the DNCRA and Spam Act, as well as having other functions under the Telecommunications Act.

The Commonwealth Attorney-General's Department has responsibilities under the *Telecommunications (Interception and Access) Act 1974* (Cth). In coordination with the OAIC, the National Health and Medical Research Council has issued several binding guidelines in respect of privacy concerning health-related information.

The Australian Transaction Reports and Analysis Centre is the agency responsible for administering the Anti-Money Laundering and Counter-Terrorism Financing Act.

Various state and territory authorities also regulate privacy law issues in those jurisdictions. These include: the ACT Information Privacy Commissioner; the NSW Information and Privacy Commission; the Office of the Information Commissioner for the Northern Territory; the QLD Office of the Information Commissioner; the South Australian Privacy Committee; the Tasmanian Ombudsman; the Office of the Victorian Information Commissioner; and the Office of the Information Commissioner for Western Australia.

## 2 Definitions

**2.1 Please provide the key definitions used in the relevant legislation:**

- **"Personal Data"**
  The analogous term used in the Privacy Act is 'personal information'. This is defined in section 6 of the Privacy Act to mean information or an opinion about an identified individual or an individual who is reasonably identifiable:
  - whether the information or opinion is true or not; and
  - whether the information or opinion is recorded in a material form or not.
- **"Processing"**
  The Privacy Act does not refer to 'processing' but regulates 'dealing with' personal information in terms of 'use' and 'disclosure' (see Part 3 of the APPs). Though both terms are not defined in the Privacy Act, the OAIC indicates that:
  - 'Use' means the handling or undertaking of activity in respect of information within its effective control.
  - 'Disclose' means to make information accessible to others outside the entity and to release subsequent handling of such information from the entity's control. The state of mind or intentions of the recipient does not affect the act of disclosure. Further, there will be a disclosure in these circumstances even where the information is already known to the recipient.
- **"Controller"**
  The Privacy Act does not refer to 'controllers' but rather covers the information-processing activities of APP entities. An APP entity is defined to be an agency or organisation.
  An 'organisation' is defined to be:
  - an individual (including a sole trader);
  - a body corporate;
  - a partnership;
  - any other unincorporated association; or
  - a trust,

  unless it is a small business operator, registered political party, state or territory authority or a prescribed instrumentality of a state.
  'Agency' refers to Australian Government (and Norfolk Island Government) agencies but does not include state and territory agencies. An 'agency' is defined to be:
  - a Minister;
  - a Department;
  - a body (whether incorporated or not) or a tribunal, established or appointed for a public purpose by or under a Commonwealth enactment, not being:
    - an incorporated company, society or association; or
    - an organisation that is registered under the Fair Work (Registered Organisations) Act 2009 or a branch of such an organisation;
  - a body established or appointed by the Governor-General or by a Minister, other than by or under a Commonwealth enactment;
  - a person holding or performing the duties of an office established by or under, or an appointment made under, a Commonwealth enactment, other than a person who, by virtue of holding that office, is the Secretary of a Department;
  - a person holding or performing the duties of an appointment, being an appointment made by the Governor-General or by a Minister, other than under a Commonwealth enactment;
  - a federal court;
  - the Australian Federal Police;
  - a Norfolk Island agency;
  - the nominated Australian Government Health Service company;
  - an eligible hearing service provider; or
  - the service operator under the Healthcare Identifiers Act 2010.

  A person shall not be taken to be an agency merely because the person is the holder of, or performs the duties of, certain offices, such as a judicial office or of an office of magistrate.
- **"Processor"**
  Whilst the term 'processor' is not used in the Privacy Act, the APPs naturally apply to APP entities to the extent that they hold personal information. According to the OAIC, this is sufficiently broad to encompass outsourced serviced providers which, for example, in Europe might be considered 'processors'.
- **"Data Subject"**
  The Privacy Act regulates the processing of personal information about individuals, defined in section 6 to mean natural persons.
- **"Sensitive Personal Data"/"Special Categories of Personal Data"**
  The Privacy Act defines 'sensitive information' in five ways. The first way is information or an opinion about certain characteristics of an individual. These characteristics are:
  - racial or ethnic origin;
  - political opinions;
  - membership of a political association;
  - religious beliefs or affiliations;
  - philosophical beliefs;
  - membership of a professional or trade association;
  - membership of a trade union;
  - sexual orientation or practices; or
  - criminal record.

  The other four ways are personal information that is specifically:
  - health information about an individual;
  - genetic information about an individual that is not otherwise health information;
  - biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
  - biometric templates.
- **"Data Breach"**
  For the purposes of the Privacy Act, an 'eligible data breach' occurs where there is unauthorised access to, or unauthorised disclosure of, certain information and a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.
- **"Collects"**
  As defined in section 6 of the Privacy Act, an entity collects personal information only if this is done for inclusion in a record or generally available publication.
- **"De-identified"**
  Personal information is de-identified if it is no longer about an identified individual or an individual who is reasonably identifiable. De-identification involves two steps. The first is the removal of direct identifiers. The second is taking one or both of the following additional steps:

- the removal or alteration of other information that could potentially be used to re-identify an individual; and/or
- the use of controls and safeguards in the data access environment to prevent re-identification.

- "**Employee Record**"
  The Privacy Act defines an 'employee record' as a record of personal information relating to the employment of the employee. Examples of personal information relating to the employment of the employee are health information about the employee and personal information about all or any of the following:
  - the engagement, training, disciplining or resignation of the employee;
  - the termination of the employment of the employee;
  - the terms and conditions of employment of the employee;
  - the employee's personal and emergency contact details;
  - the employee's performance or conduct;
  - the employee's hours of employment;
  - the employee's salary or wages;
  - the employee's membership of a professional or trade association;
  - the employee's trade union membership;
  - the employee's recreation, long service, sick, personal, maternity, paternity or other leave; or
  - the employee's taxation, banking or superannuation affairs.
- "**Holds**"
  An entity holds personal information if the entity has possession or control of a record that contains the personal information.
- "**Identification Information**"
  Identification information about an individual means:
  - the individual's full name;
  - an alias or previous name of the individual;
  - the individual's date of birth;
  - the individual's sex;
  - the individual's current or last known address and two previous addresses (if any);
  - the name of the individual's current or last known employer; or
  - if the individual holds a driver's licence – the individual's driver's licence number.
- "**Record**"
  A record includes a document or an electronic or other device. It does not, however, include:
  - generally available public information;
  - anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition;
  - Commonwealth records in the open access period;
  - records in the care of the National Archives of Australia;
  - documents placed in the memorial collection of the Australian War Memorial; or
  - letters or articles transmitted by post.

## 3 Territorial and Material Scope

### 3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Section 5B(1A) of the Privacy Act extends its application to acts done, or practice engaged in, outside Australia and the external territories by an organisation or small business operator with an Australian link. An organisation or small business operator has an Australian link if the organisation or operator is:

- an Australian citizen;
- a person whose continued presence in Australia is not subject to a limitation as to time imposed by law;
- a partnership formed in Australia or an external territory;
- a trust created in Australia or an external territory;
- a body corporate incorporated in Australia or an external territory;
- an unincorporated association that has its central management and control in Australia or an external territory; or
- if the organisation or operator does not meet any of the above criteria, but does carry on business in Australia or an external territory.

However, section 6A of the Privacy Act dictates that the APPs is not informed by foreign law, even where conduct wholly occurs outside Australia.

### 3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

Pursuant to section 16 of the Privacy Act, the APPs do not apply to the collection, holding, use or disclosure of personal information by an individual, or personal information held by an individual, only for the purposes of, or in connection with, his/her personal, family or household affairs.

In addition, the Act contains several specific exemptions and carve-outs, including:

- the employee records exemption, which excludes acts or practices directly related to a current or former employment relationship and an employee record held by a private sector employer;[7]
- small business operators (generally those with an annual turnover of AU$3 million or less), subject to a number of exceptions (for example, health service providers and entities trading in personal information);[8]
- registered political parties and political acts and practices;[9] and
- certain journalistic activities, where undertaken by media organisations committed to published privacy standards.[10]

## 4 Key Principles

### 4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  The object of APP 1 is to ensure that APP entities manage personal information in an open and transparent way. An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:
  - will ensure that the entity complies with the APPs and a registered APP code (if any) that binds the entity; and
  - will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the APPs or such a code.

An APP entity must have a clearly expressed and up-to-date policy ('**APP privacy policy**') about the management of personal information by the entity. An APP entity must also take such steps as are reasonable in the circumstances to make its APP privacy policy available free of charge and in such form as is appropriate.

- **Lawful basis for processing**
  Broadly speaking, the lawful basis upon which an entity may process personal data is the consent of the individual. However, the majority of the APPs contain limitations or extensions relating to the application of Commonwealth laws, records and/or agreements. APP 3.5 specifies that personal information may only be collected by lawful and fair means.
- **Purpose limitation**
  Pursuant to APP 6, where an entity has collected personal information for a particular person, that information cannot then be used or disclosed for any further purpose other than with consent of the individual. This is limited, however, by certain defined exceptions, such as where the individual would hold a reasonable expectation of disclosure, where disclosure is required/authorised by a court or tribunal, or where a certain permitted health situation exists (see APPs 6.2 and 6.3).
- **Data minimisation**
  The APPs address data minimisation in a piecemeal approach, combining a prohibition on reallocation of the purpose for holding information without consent (APP 6), limiting the collection of information to that which is reasonably necessary for the function in question (APP 3), and mandating destruction/de-identification where no purpose for use or disclosure of the information remains (APP 11).
- **Proportionality**
  Pursuant to APP 3, an APP entity may only collect personal information to the extent that it is reasonably necessary for, or directly related to, one or more of the entity's functions or activities. For sensitive information, collection further requires the individual's consent.
- **Retention**
  APP 11.2 requires an APP entity to take such steps as are reasonable in the circumstances to destroy or de-identify personal information it holds about an individual when:
  - the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule;
  - the information is not contained in a Commonwealth record; and
  - the entity is not required by or under an Australian law or a court/tribunal order to retain the information.
- **Accuracy**
  APP 10.1 requires an APP entity to take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete. Pursuant to APP 10.2, an APP entity must also take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.
- **Dealing with unsolicited personal information**
  Where an APP entity receives unsolicited personal information, APP 4 requires that the entity must, within a reasonable period after receiving the information, determine whether the entity could have collected the information under APP 3 if the entity had solicited the information. If the APP entity determines that the entity could not have collected the personal information, and the information is not contained in a Commonwealth record, the entity must, as soon as practicable, but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.
- **Cross-border disclosure of personal information**
  Unless authorised, entities that intend to disclose personal information in a cross-border context must, pursuant to APP 8, take reasonable steps to ensure that the foreign entity receiving such information complies with the APPs. This is subject to exceptions, such as where that foreign entity is subject to a similar privacy regime under foreign law, or an agency discloses information pursuant to a treaty obligation.
- **Government-related identifiers**
  APP 9 prohibits (with certain exceptions) the adoption, use or disclosure of government-related identifiers for individuals by non-government organisations.
- **Security of personal information**
  Pursuant to APP 11, if an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to (copies of) data/information about processing**
  Pursuant to APP 12, if an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.[11] The APP entity is not required to give the individual access to the personal information in certain circumstances (see APP 12.3), including where giving access would be unlawful, have an unreasonable impact on the privacy of other individuals, or would pose a serious threat to the life, health or safety of any individual, or to public health or public safety.[12]
- **Right to rectification of errors**
  Pursuant to APP 13, if an APP entity holds personal information about an individual and either:
  - the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; or
  - the individual requests the entity to correct the information,

  the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.[13]
- **Right to deletion/right to be forgotten**
  There is no general, enforceable right to have information deleted.
  However, APP entities must actively consider whether they can continue to retain personal information, subject to certain exceptions, where information is no longer needed per the APPs; APP 11.2 requires the APP entity to take reasonable steps to destroy or de-identify the information.

- **Right to object to processing**
  In practice, an individual's power to restrict processing of their personal information is limited to their initial withholding of consent to the collection of such information. APP 2 permits individuals to use a pseudonym or not identify themselves when dealing with an APP entity (unless required/permitted by law, or if this would be impractical).[14] Additionally, APP 5 requires that individuals be notified before (or as soon as practicable after) their personal information is collected, thereby giving them the opportunity to object to such collection by disengaging with the entity.[15]
- **Right to restrict processing**
  Whilst the APPs impose certain restrictions on how personal information can be dealt with (such as those relating to the purpose for which information is held (APPs 3 and 6)),[16] there is no right to restrict the manner with which their information is dealt. Any such control held by an individual is largely relinquished upon the initial giving of consent to its collection.[17]
- **Right to data portability**
  There is a narrower right to data portability under Australian law in comparison to the General Data Protection Regulation ('**GDPR**').
  The Consumer Data Right ('**CDR**') was established under Part IVD of the federal *Competition and Consumer Act 2010* (Cth). The CDR allows consumers to safely share data that businesses hold about them in banking and energy sectors. Although there were plans to expand this regime to at least the telecommunications and insurance sectors, these are now under review primarily due to compliance costs.
  The Australian Competition and Consumer Commission is the lead regulator of the CDR.[18]
- **Right to withdraw consent**
  The OAIC's APP guidelines indicate that consent must be current and specific. This includes enabling an individual to withdraw their consent at any time, which should be an easy and accessible process.[19] Once an individual has withdrawn consent, an APP entity can no longer rely on that past consent for any future use or disclosure of the individual's personal information.[20] Individuals should be made aware of the potential implications of withdrawing consent, such as no longer being able to access a service.[21]
- **Right to object to marketing**
  APPs 7.2 and 7.3 require APP entities using personal information to engage in direct marketing to provide a simple means by which individuals may easily request to not receive such communications.[22] If such a request is made, the entity must cease direct marketing to the individual.[23]
- **Right to be informed of solely automated decision-making and profiling**
  A broad right addressing the right of individuals to be informed regarding the existence of solely automated decision-making and profiling does not presently exist under Australian law.
  From 10 December 2026, under the new APP 1, APP entities will have new obligations where it arranges a computer program, using personal information about an individual, to make or directly support a decision that could reasonably be expected to significantly affect the individual's rights or interests. Such APP entities must disclose in their privacy policies the kinds of personal information used and decisions made in the computer programs.
- **Right to complain to the relevant data protection authority(ies)**
  The OAIC is empowered to receive individual complaints about the handling of personal information. It can also recognise external dispute-resolution schemes that handle particular privacy-related complaints under section 35A of the Privacy Act. For example, if an individual's privacy complaint is about a bank in Australia, he or she can contact the Australian Financial Complaints Authority under section 36 of the Privacy Act.
- **Right to anonymity**
  Pursuant to APP 2, individuals must have the option of not identifying themselves or using a pseudonym when dealing with APP entities, unless that entity is required/authorised by law to deal with individuals who have identified themselves, or if dealing with non-identified individuals would be impracticable.[24]
- **Right to notification**
  Pursuant to APP 5, APP entities must notify individuals about the collection of their personal information before, or as soon as practicable after, it occurs.[25]

**5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.**

There is no express provision addressing data subjects having the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress. However, a representative complaint may be lodged under section 36 of the Privacy Act if the conditions of section 38 of the Privacy Act are satisfied.

## 6 Children's Personal Data

**6.1 What additional obligations apply to the processing of children's personal data?**

According to the OAIC, an organisation or agency handling the personal information of an individual under the age of 18 must decide if the individual has the capacity to consent on a case-by-case basis. As a general rule, an individual under the age of 18 has the capacity to consent if they have the maturity to understand what is being proposed. If they lack maturity, it may be appropriate for a parent or guardian to consent on their behalf.[26]

If it is not practical for an organisation or agency to assess the capacity of individuals on a case-by-case basis, as a general rule, an organisation or agency may assume an individual over the age of 15 has capacity, unless they are unsure.[27]

The OAIC is developing a Children's Online Privacy Code, which will impose additional obligations on the processing of children's personal data. The Code will establish specific requirements for organisations regarding the collection, use, and disclosure of children's personal information when they access digital services. It requires entities operating apps, websites, or online games likely to be used by children to handle personal information responsibly, including details such as name, age, and online activity preferences.[28]

## 7 Registration Formalities and Prior Approval

**7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

There is no legal obligation on businesses to register with or notify the OAIC or any other bodies in relation to their data-processing activities in general. Specific obligations arise when eligible data breaches occur, as detailed in section 16. However, the OAIC has issued guidance to assist APP entities to prepare responses to any such breaches.[29]

There is an option to 'opt-in' for small businesses and not-for-profits to good privacy practices and be covered under section 6EA of the Privacy Act.

**7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

This is not applicable in Australia – please see response to question 7.1.

**7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?**

This is not applicable in Australia – please see response to question 7.1.

**7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?**

This is not applicable in Australia – please see response to question 7.1.

**7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?**

This is not applicable in Australia – please see response to question 7.1.

**7.6 What are the sanctions for failure to register/notify where required?**

This is not applicable in Australia – please see response to question 7.1.

**7.7 What is the fee per registration/notification (if applicable)?**

This is not applicable in Australia – please see response to question 7.1.

**7.8 How frequently must registrations/notifications be renewed (if applicable)?**

This is not applicable in Australia – please see response to question 7.1.

**7.9 Is any prior approval required from the data protection regulator?**

This is not applicable in Australia – please see response to question 7.1.

**7.10 Can the registration/notification be completed online?**

This is not applicable in Australia – please see response to question 7.1.

**7.11 Is there a publicly available list of completed registrations/notifications?**

This is not applicable in Australia – please see response to question 7.1.

**7.12 How long does a typical registration/notification process take?**

This is not applicable in Australia – please see response to question 7.1.

## 8 Appointment of a Data Protection Officer

**8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

Currently, in Australia, organisations are not required to appoint a Data Protection Officer. However, the Information Commissioner has issued guidance recommending that organisations appoint a Data Protection Officer as good practice.[30]

A Data Protection Officer in Australia is known as a Privacy Officer and whilst not mandated by law, it is arguably essential in practice to comply with APP 1.2.[31] The *Privacy Act Review Report 2022* spoke directly about the role of Privacy Officers in Australia: 'The role should be recognised as an important one within the entity. For larger organisations, it would be expected that the Privacy Officer would be at a senior level that reports to the highest management level.'[32]

**8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

Currently, in Australia, there are no formal sanctions for failing to appoint a Data Protection Officer or Privacy Officer.

**8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

In Australia, there is no specific legislation that outlines protections or safeguards for Privacy Officers or Data Protection Officers during their course of employment. However, according to best practice within government agencies, a Privacy Officer will not be held personally responsible for non-compliance with the Australian Government Agency Privacy Code.[33]

**8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

According to best industry practice by government agencies, a Data Protection Officer or Privacy Officer may be appointed to act for a group of companies or a public authority. However, it is understood that depending on an organisation's size, functions, and structure, an organisation may decide to appoint more than one Data Protection Officer/Privacy Officer.[34]

**8.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

Under Australian legislation, there are no prescribed academic or working background qualifications to be a Data Protection Officer or Privacy Officer.[35]

**8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

The OAIC recommends that Privacy Officers regularly report to their entity's governance body. In relation to best practice for government agencies, the OAIC recommends that Privacy Contact Officers should be at least at the executive level and:

- participate in the development of initiatives with a privacy impact;
- advise on the application of the Privacy Act;
- handle or supervise the handling of privacy complaints;
- train staff in relation to relevant aspects of the Privacy Act; and
- be the primary contact for the OAIC.[36]

**8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

No, registration/notification is not required.

**8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

No. The OAIC requires privacy policies to be high-level documents that are not expected to contain specific details about all the entity's practices, procedures, and systems relating to management of personal data.

## 9 Appointment of Processors

**9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

As the APPs do not specifically refer to 'processors', this is not strictly the case. However, although the Privacy Act and APPs do not refer explicitly to processors, the OAIC's view is that APP entities that are outsourced service providers holding personal information, even if not controlling it as such, must comply with this legal regime.

Where the processor is located overseas, the regulation of foreign information transfer is detailed in APP 8 and the OAIC has provided guidance for data processors or controllers with an establishment in the EU to ensure they are GDPR compliant.[37]

**9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

Although not applicable, entering such agreements remains best practice. In the context of cross-border disclosure, the OAIC under APP 8 recommends that such contracts cover:

- the type of personal information and purpose for its disclosure;
- a requirement that the recipient of the information complies with the APPs;
- the complaints-handling process; and
- a requirement as to the implementation of a data-breach response plan.

## 10 Marketing

**10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

In practice, the Spam Act is the primary legislation governing electronic marketing, requiring:

- consent (express or inferred);
- sender identification; and
- a functional unsubscribe mechanism.

APP 7.1 imposes a general prohibition on the use of personal information for the purpose of direct marketing.[38] This does not apply where the organisation provides a simple means through which the individual can opt-out of the marketing and:

- the information was collected in circumstances that would give rise to reasonable expectation of the information being used in such marketing; or
- the individual has consented to the receipt of such marketing.[39]

**10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

The APPs do not speak specifically to the business-to-business context. However, it could be argued that these restrictions do in fact apply in the business-to-business context.

**10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

The national DNCRA prohibits most unsolicited telemarketing calls and fax messages to numbers placed on a national Do Not Call Register, without the consent of the person/organisation being contacted.

The Spam Act proscribes the sending of most unsolicited and non-consensual electronic messages. Some exceptions to this prohibition are electronic messages by government bodies, political parties and charities.[40]

**10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

The Spam Act regulates the sending of commercial electronic messages with 'an Australian link'. This covers messages that:

- originate in Australia;
- were sent, or authorised by, an individual/organisation physically present in Australia, or with central management and control in Australia, when the message was sent;
- were accessed by a computer, server or device that is located in Australia;
- is connected to an electronic account-holder that is either an individual physically present in Australia or an organisation carrying on business or activities in Australia when the message is accessed; or
- if unable to be delivered due to the non-existence of a delivery address would, had the address existed, reasonably likely have been accessed using a computer, server or device located in Australia.[41]

The DNCRA concerns telephone calls and fax messages sent to 'an Australian number'. This means numbers that are specified in the plan set out in the Telecommunications Act and for use in connection with the supply of carriage services to the public in Australia. Section 9 of the DNCRA also expressly extends the legislation's application to acts carried out outside Australia's territory. Under APP 7.6(e), individuals may request to be advised of the source of their personal information used or disclosed in relation to direct marketing.

**10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

The ACMA is responsible for enforcing and investigating breaches of the Spam Act. The ACMA is a robust organisation which actively enforces breaches of marketing restrictions in Australia.

In 2026, Lululemon Athletica Australia Pty Ltd was fined AU$702,900 by the ACMA for sending over 370,000 emails containing marketing content without an unsubscribe option, in breach of the Spam Act. The ACMA found that Lululemon had mischaracterised service emails (such as delivery and order confirmations) as non-commercial, despite including promotional content and links.[42]

The case confirms that any message containing marketing material is considered commercial and must include a functional unsubscribe mechanism.[43] In addition to the penalty, Lululemon entered into an enforceable undertaking requiring compliance improvements and ongoing reporting to the regulator.[44]

**10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

In Australia, APP 3.6 governs the solicitation of personal information. It states that an entity 'solicits' personal information 'if the entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included'. This request may be made to an agency, organisation, individual or a small business operator on behalf of another. A 'request' under this principle is an active step taken by an entity to collect personal information and may not involve direct communication between the entity and an individual.[45]

Arguably, APP 3.6 to some extent prevents the purchasing of marketing lists from third parties. The essence of this rule is that personal information should be collected directly from the individual concerned ('direct collection'), rather than from third parties or other sources.[46]

However, for organisations, the exception to the rule requiring direct collection is that it would be unreasonable or impracticable to do so.[47] APP 3.65 stipulates that determining whether it is unreasonable or impracticable to collect personal information solely from the individual depends on specific circumstances. Relevant considerations include the individual's expectation of direct collection, the sensitivity of the information, potential jeopardy to the collection purpose or data integrity, privacy risks from alternate sources, and the time and cost of direct collection.[48]

APP 3.68 provides an example where an agency may collect personal information from a third party, such as when an individual consents to one agency disclosing their information to another agency. Regarding consent, as discussed in paragraph 3.23 and Chapter B, it can be express or implied, must be voluntary, informed, current and specific, and the individual must possess the capacity to consent.[49]

**10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

Breaches of the DNCRA may result in corporate liability for civil penalties up to AU$3.3 million, and individual liability for up to AU$660,000 per day. This will depend on the number of breaches and the history of the actor.[50] Compensation can also be ordered where a victim has suffered loss or damage.

This penalty regime (and maximum sanctions) is largely mirrored in respect of the Spam Act.

Additionally, the Privacy Act contains numerous provisions addressing the payment of civil penalties, fines and compensation to victims.

## 11 Cookies

**11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

There is no specific legal regime that applies to cookies. Whilst the information collected through the use of cookies is often generalised, where it rises to the level of enabling identification of an individual, the use of cookies will be subject to the APPs.

However, there is new technology that combines cookie information, which is called data aggregation, and may be subject to legislative restrictions.

**11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

Whilst the APPs do not (in theory) apply differently to different cookies, the OAIC has issued public guidance about their distinctive operations and how individuals can adjust their browsing preferences accordingly.[51]

**11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

To date, the OAIC has not done so.

**11.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

This is not applicable in Australia.

## 12 Restrictions on International Data Transfers

**12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

The transfer of personal information to jurisdictions outside Australia is governed by APP 8. APP 8.1 requires that entities must take 'reasonable steps' to ensure that a foreign recipient of personal information complies with the APPs. According to APP 8.2, however, this is not necessary where:

- it is reasonably believed that the recipient is subject to a law, or binding scheme, that bears overall substantial similarity to the APPs and the individual can take action to enforce such protections;
- the entity has obtained the individual's consent to the foreign disclosure;
- the foreign disclosure is required or authorised by Australian law;
- a permitted general situation (such as to lessen or prevent serious health and safety risks, or to take appropriate action in relation to suspected serious misconduct) applies;
- such disclosure is required by a government agency under an agreement to which Australia is a party; or
- the disclosure is by a government agency and relates to foreign law-enforcement activities.

**12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

The OAIC espouses an expectation that, to take the necessary reasonable steps, entities transferring personal information to foreign recipients will enter into enforceable contracts requiring compliance with the APPs. Under section 16C of the Privacy Act, if an entity has disclosed personal information on the basis of a belief that the foreign recipient will be APP-compliant (i.e. under APP 8.1), the Australian entity bears legal responsibility for any breaches of the APPs by the recipient.[52]

**12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

No. The entity itself must assess whether or not the foreign recipient will comply with the APPs or is subject to a similar privacy regime and, if necessary, seek the individual's consent only.

**12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.**

Australian law does not require a transfer impact assessment. However, the OAIC's APP 8 guidance makes clear that before disclosing personal information to an overseas recipient, an entity must take 'reasonable steps in the circumstances' to ensure the recipient will not breach the APPs, and these steps commonly involve assessing relevant risk factors and implementing appropriate contractual safeguards.[53]

**12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?**

In Australia, there is no official guidance from the OAIC on the *Schrems II* decision.

**12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?**

There has been no official guidance released by the OAIC in the use of standard contractual models/clauses as a mechanism for international data transfers.

## 13 Whistle-blower Hotlines

**13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

Protections of corporate whistleblowers are provided for in the *Corporations Act 2001* ('**Corporations Act**'). This relates to the reporting of breaches of the Corporations Act or the *Australian Securities and Investments Commission Act 2001* (Cth).

The whistleblower protections in Part 9.4AAA of the Corporations Act provide protections for, among others, whistleblowers who report misconduct about companies and company officers.

The scope of protected disclosures encompasses a range of conduct related to 'misconduct' or an 'improper state of affairs'; whistleblowers can make anonymous disclosures without the requirement of 'good faith', although reasonable grounds for concern are necessary.[54]

Whistleblowers are protected from any litigation (civil or criminal), employment termination or victimisation as a result of their actions. To qualify for these protections, a person must:

- be an officer, employee or contractor of the company in question;
- disclose to a company auditor (or member of the audit team), officer or senior manager, a person authorised to receive whistleblower disclosure or the Australian Securities and Investments Commission; or
- have reasonable grounds to suspect that the information being disclosed about the company or organisation concerns misconduct, or an improper state of affairs or circumstances.

**13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous whistleblowers are afforded the same protections under the Corporations Act as discussed in the previous sections.

Australian businesses address the issues of anonymity by enshrining the rights of anonymous whistleblowers within their corporate governance framework and whistleblower policies that must comply with section 137AI(5)(c) of the Corporations Act, which ensures whistleblower policies must have 'information about how the company will support (all) whistleblowers and protect them from detriment'.[55]

## 14 CCTV

**14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

In Australia, the regulations surrounding the use of CCTV cameras vary depending on the jurisdiction.

**Federal jurisdiction**

Generally, the *Surveillance Devices Act 2004* (Cth) governs the practices for organisations and agencies on the usage of surveillance devices such as CCTV.[56] The OAIC has stated that:

> *'If the Privacy Act covers the organisation or agency, then any personal information they collect through a surveillance device must comply with the Australian Privacy Principles. The Privacy Act covers Australian Government agencies and organisations with an annual turnover of more than $3 million, and some other organisations. Such an organisation or agency must:*
>
> - *tell you that your image may be captured before you're recorded; and*
> - *make sure recorded personal information is secure and destroyed or de-identified when it is no longer needed.'*[57]

Importantly, over the last two years the use of CCTV and AI facial recognition by retailers has been in the spotlight with Bunnings Group Limited and Privacy Commissioner (Guidance and Appeals Panel) [2026] ARTA 130 and associated cases. In this specific and recent case, the Tribunal determined that Bunnings (a hardware retail chain) was entitled to use facial-recognition technology 'for the limited purpose of combatting very significant retail crime and protecting their staff and customers from violence, abuse and intimidation within its stores'.

While the Tribunal found Bunnings did not breach APP 3.3 by doing so, it held Bunnings did breach APPs 1.2, 1.3 and 5.1 in failing to notify that personal information is being collected and to implement appropriate practices, procedures and systems in doing so. The decision is instructive for businesses considering using facial-recognition technology or collecting personal information in a similar way. These include other recent cases such as Commissioner Initiated Investigation ('**CII**') into Kmart Australia Limited (Privacy) [2025] AICmr 155 (26 August 2025).

While the Privacy Act does not cover security cameras operated by an individual acting in a private capacity, state or territory laws may apply.[58]

**State and territories jurisdiction**

The governance for surveillance devices will differ between states and territories. For instance, a comparison will be drawn between NSW and QLD:

- In NSW, the use of CCTV is regulated under the *Surveillance Devices Act 2007* (NSW).[59] The legislation has strict requirements that should be consulted with the relevant authorities for compliance. There is a voluntary register that is maintained by NSW police, if private residents wish to register their private CCTV systems.[60]
- In QLD, entities using CCTV are required to take 'reasonable steps' to make individuals aware of the purpose and authority for camera surveillance, although specific requirements may vary.[61]

The examples cited above broadly explain how corporate bodies would be governed.

The OIAC has recommended for individuals, regarding compliance with state or territory laws on surveillance devices, that it would be appropriate to contact the relevant state or territory Attorney-General department.[62]

**14.2 Are there limits on the purposes for which CCTV data may be used?**

Similarly to above, the limitations will vary between jurisdictions.

## 15 Employee Monitoring

**15.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

There is no federal legislation that governs what types of employee monitoring are permissible and under what circumstances it is permitted, this is relegated to the states and territories to govern on. Examples below will consider NSW and VIC.

In NSW, under the *Workplace Surveillance Act 2005* Part 2,[63] the notice requirements that employers must adhere for compliance are listed. Notably, employees are given a minimum of 14 days' notice prior to surveillance being conducted. The notice will list the circumstances for surveillance being conducted.

In VIC, under the *Surveillance Devices Act 1999* Part 2A,[64] the surveillance of employees in certain places and circumstances is prohibited.

It may be reasonable for an employer to monitor some activities to ensure staff are doing their work and using resources appropriately. If the employer monitors staff use of email, internet, and other computer resources, and they have told the employee about the monitoring, this would generally be allowed.[65]

**15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

As outlined above, in NSW employees must be given at least 14 days' notice or notice prior to their commencing work.[66] This must include various details about the nature and extent of the monitoring. For VIC, there is no specific timeframe listed for notice.

**15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

There is no requirement under Australian privacy law for employee representatives or trade unions to be notified or consulted regarding employee monitoring.

**15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?**

Employers may be entitled to process information on an employee's attendance if it is required as part of the internal return-to-office policy that forms the employment relationship, in which the employee's records exemption may apply and that employers will not need to comply with the Privacy Act's requirements as stated by the OAIC.[67]

The OAIC does warn that this exemption does not apply to practices that are outside the scope of the employment relationship.[68]

## 16 Data Security and Data Breach

**16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Generally, APP entities are responsible for ensuring that data is kept secure. The definition for APP entities is defined under section 6(1) of the Privacy Act. An APP entity is defined as an agency or organisation, in which 'organisation' can be an individual, body corporate, partnership, unincorporated association or trust.[69]

The OAIC has published guidance on the security of personal information under APP 11. The OAIC has stated that: 'An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.'[70]

**16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The OAIC has a NDB scheme, where a Privacy Act-covered organisation or agency is required to report to the OAIC and relevant individual that an eligible data breach has occurred.[71]

The OAIC has defined 'eligible data breach' as:

- unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds;
- that is likely to result in serious harm to one or more individuals; and
- the organisation or agency has not been able to prevent the likely risk of serious harm with remedial action.[72]

The notification to the individual from an organisation or agency should list recommendations on what the next steps in response to the data breach should look like, ideally using the OAIC's NDB form.[73]

**16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

The OAIC has published guidance on responding to data breaches; there are four steps, which are contain, assess, notify and review. There is an emphasis that data breaches should be considered on a case-by-case basis and that the notify section of the four-step response details how individuals affected by the breach should be notified.[74]

The OAIC has stated that there are obligations for entities under the NDB scheme to assess a suspected breach under section 26WH(1) of the Privacy Act,[75] in which the entity must take all reasonable steps to complete the assessment within 30 days from when the entity became aware of the eligible data breach under section 26WH(2).[76]

Entities will have three options for notifying individuals at risk of serious harm, depending on what is 'practicable' for the entity under section 26WH(2). The options are 'notify all individuals',[77] 'notify only those individuals at risk of serious harm'[78] and 'publish notification'. The OAIC has published guidance on what is expected to be included in an eligible data breach statement.[79]

**16.4 What are the maximum penalties for personal data security breaches?**

Section 13G of the Privacy Act sets out the maximum penalty for serious or repeated interferences with privacy:

For a body corporate, they are the greater of either:

- AU$50 million;
- the value of any benefit the relevant court has determined that the body corporate, or any body corporate related to it, has obtained directly or indirectly that is reasonably attributable to the contravention, multiplied by three; or
- if the court cannot determine the value of that benefit, 30% of the annual turnover of the body corporate during the 12-month period ending at the end of the month in which the contravention happened or began.

For a person other than a body corporate, the maximum penalty amount is AU$2.5 million.

## 17 Enforcement and Sanctions

**17.1 Describe the enforcement powers of the data protection authority(ies).**

(a) **Investigative powers**:
The Commissioner of the OAIC can initiate an investigation under section 40 of the Privacy Act.[80] Section 40(2) of the Privacy Act enables the Commissioner to initiate an investigation where:

a. an act or practice may be an interference with the privacy of an individual or a breach of APP 1; and
b. the Commissioner thinks it is desirable to do so.[81]

The OAIC stated that: 'Prior to commencing an investigation, the Commissioner may conduct preliminary inquiries under section 42(2) of the Privacy Act, to determine whether to commence a CII. Once a CII has been commenced, the OAIC will conduct its investigation in accordance with Part V of the Privacy Act.'[82]

If the OAIC does in its discretion decide to initial a CII, there are four next steps that will occur:

1. Notification to the respondent: the OAIC will notify the respondent in writing about its decision to commence a CII and about the initial scope of the investigation.
2. Information gathering: the OAIC will seek the cooperation of the respondent in the provision of necessary information.
3. Decision making: as part of the preliminary review, if the correspondent fails to meet the requirements of the Privacy Act or the requirements of the privacy safeguards or CDR rules, the Commissioner may make the following regulatory actions:
   i. exercise a discretionary power under section 41 of the Privacy Act to discontinue an investigation;
   ii. seek an enforceable undertaking under section 33E of the Privacy Act and section 56EW of the Competition and Consumer Act;
   iii. make a determination under section 52(1A) of the Privacy Act;
   iv. seek an injunction under section 80W of the Privacy Act;
   v. apply for a civil penalty order under section 80U of the Privacy Act and section 56EU of the Competition and Consumer Act; or
   vi. report to the Minister about a CII under section 30 of the Privacy Act.
4. Conclusion and publication: the OAIC will place a notice on its website advising the public that the investigation of said matter has concluded.[83]

(b) **Corrective powers**:

The OAIC has advised that APP 13 will 'require an APP entity to take reasonable steps to correct information to ensure that, having regard to the purpose for which it is held, it is accurate and up-to-date, complete, relevant and not misleading'.[84]

The OAIC has an exhaustive explanation on the minimal procedural requirements that is expected in the correction of information.[85]

(c) **Authorisation and advisory powers**:

The OAIC has published guidance on authorisation, particularly with regard to consumer authorisation,[86] in which a data holder must ask for a consumer's authorisation before disclosing their CDR to an accredited data recipient. There are minimum requirements that data holders must meet for the authorisation notice.

Separately, the OAIC has powers under the Privacy Act and other legislative instruments to make and approve legally binding rules and guidelines as part of its advisory powers.[87] These guidelines help guide other agencies and APP entities who can use the guides to remain compliant with data laws and regulations.

(d) **Imposition of administrative fines for infringements of specified legal provisions**:

The OAIC can issue an infringement notice under section 80UB of the Privacy Act, where the Commissioner is of the belief that a contravention under section 66(1) of the Privacy Act has occurred because the individual has failed to give information, answer a question, or produce a document or record when required to do so under the Privacy Act.[88]

The infringement notice must be issued within 12 months of the alleged contravention, the expected penalty will be 12 units for a person and 60 for bodies corporate.

The OAIC has stated that any recipient of an infringement notice is permitted to seek a withdrawal of the infringement notice through written representations to the Commissioner; the OAIC has published guidance on what is expected of the written representations.

(e) **Non-compliance with a data protection authority**:

In cases of non-compliance, particularly for serious or repeated offences, the Commissioner under section 80W may apply to the Federal Court for an order against an entity that is alleged to have contravened a civil penalty provision of the Privacy Act at the Commissioner's discretion.[89]

### 17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The OAIC has powers to apply for an injunction under section 80W of the Privacy Act through application to the Federal Court to restraint a person from engaging in a particular conduct and if the Court's opinion is that it is 'desirable' to do so.[90]

With regard to bans on a particular processing activity, the courts must be satisfied that 'a person has engaged, is engaging in, or is proposing to engage in conduct in contravention of either the Privacy Act, the MHR Act or a privacy safeguard set out in Part IVD of the Competition and Consumer Act'.[91]

### 17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

There have been a variety of recent cases and investigations by the OAIC.

An emerging set concern consequences of data breaches. For example, OAIC reference CII21/00010. In February 2025, the OAIC obtained an enforceable undertaking from Oxfam Australia after a cyber incident led to Oxfam discovering 1.7 million records had been leaked, which had been retained for more than the seven-year allowed retention timeline.[92] Similar fact scenarios have led the OAIC to utilise different tools in their arsenal, including declarations.[93]

### 17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

The Commissioner under section 33A of the Privacy Act may share information with international bodies, which can comprise an authority of the government of a foreign country that functions to protect the privacy of individuals, similarly to the foreign equivalents of the OAIC.[94]

There are safeguard limitations in section 33A that ensures the exercise of this information sharing power is 'reasonable, necessary and proportionate'.[95]

In terms of enforcement, the OAIC is part of the Global Privacy Enforcement Network, which helps cross-border enforcement.

## 18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

**18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

Guidance on cross-border disclosure of information can be found in the OAIC's guide on APP 8, which details what reasonable steps an APP entity must take prior to the disclosure of personal information to an overseas recipient, in that the entity would not breach any APPs.[96]

The OAIC has allowed for the disclosure of personal information to an overseas recipient as required or authorised under an international agreement related to information sharing under APP 8.2(e). However, the OAIC has stated that there are requirements that the agreement must make specific arrangements for disclosure of information such as identifying agency, recipient, categories of personal information that may be disclosed and circumstances where information will be disclosed.[97]

Australia is also party to a number of international agreements that relate to the sharing of data across national borders. Although concerning the actions of public bodies, not businesses, they are of central relevance to the sharing of Australian information with foreign law enforcement. These instruments include the following examples:

a. The 'Five Eyes' is an intelligence pact between Australia, the United States, the United Kingdom, New Zealand, and Canada, all parties to the *UK–USA Agreement*. Part of this arrangement is 'critical information sharing' between the nations that relates to issues of law enforcement, border protection, and criminal justice. These partners also share information concerning financial sector intelligence.[98]
b. Australia is party to over 25 bilateral mutual legal assistance treaties with foreign nations. All these treaties contain provisions explicitly contemplating the exchange of information between governments in relation to criminal matters.[99]
c. Australia is a party to the multilateral 2001 *Budapest Convention on Cybercrime*. Over 70 nations are parties to this treaty. The Budapest Convention covers a range of issues related to international cyber-crime, including requests to/from foreign states for the seizure, collection, and interception of computer data. Article 26 specifically contemplates the spontaneous sharing of information between nations, without any prior request, that may be used in the investigation or prosecution of cyber-crime offences.[100]
d. Australia is also party to a number of Taxation Information Exchange Agreements ('**TIEAs**') with states outside the Organisation for Economic Cooperation and Development. TIEAs facilitate the exchange of information between countries concerning taxation matters and are aimed at combatting international tax avoidance.[101]

**18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?**

On disclosure of personal data to foreign law enforcement and governmental bodies, the OAIC has broadly issued guidance to APP entities on the reasonable steps to ensure an overseas recipient does not breach any APPs.[102]

The OAIC has stated that the 'requirement in APP 8.1 to ensure that an overseas recipient does not breach the APPs is qualified by a reasonable steps test'. It is generally expected that an APP entity will enter into an enforceable contractual arrangement with an overseas recipient that will enforce and require the recipient to govern the personal information in accordance with the APPs.[103]

## 19 Artificial Intelligence

**19.1 Are there any limitations on automated decision-making involving the processing of personal data using artificial intelligence?**

There are some provisions in Australian legislation, while not specifically geared towards artificial intelligence ('**AI**'), that capture the processing of data.[104]

The Privacy Act is the primary legislation governing the handling of personal information in Australia. While the Act does not specifically regulate automated decision-making, several provisions – particularly within the APPs – are relevant to the use of personal data in such systems.

APP 1, which concerns the open and transparent management of personal information, requires organisations to be clear and upfront about how they collect, use, and disclose personal data, including where automated systems are involved. This includes maintaining a clearly expressed and up-to-date privacy policy that outlines the use of automation where relevant.

APP 5 deals with the notification of the collection of personal information. It requires entities to inform individuals at or before the time of collection (or as soon as practicable thereafter) about the purpose for which their information is being collected, including if it will be used in automated decision-making processes.

APP 6 relates to the use and disclosure of personal information. It limits organisations to using or disclosing personal information only for the primary purpose for which it was collected, unless an exception applies. This principle ensures that any use of personal data for automated decision-making must align with the original purpose of collection or fall within a permitted exception.

Although the Privacy Act does not expressly regulate algorithmic or AI-based decisions, these principles impose obligations that indirectly constrain how personal information can be used in such contexts. As a result, entities deploying AI systems that process personal data must ensure compliance with the APPs to mitigate legal and regulatory risk.

**19.2 What guidance (if any) has/have the data protection authority(ies) issued in relation to the processing of personal data in connection with artificial intelligence?**

In Australia, while there is no AI-specific legislation, the OAIC has provided important guidance on the use of AI, particularly in relation to the handling of personal information under the Privacy Act and the APPs.[105]

The OAIC's guidance emphasises that organisations using AI systems should adopt a privacy-by-design approach, ensuring that personal information is handled lawfully, transparently and fairly throughout the data lifecycle. Key issues highlighted include minimising data collection, securing personal information, and ensuring transparency and explainability when

AI is used to make decisions that may significantly impact individuals. While the Privacy Act does not currently contain a specific right to human review or explanation of automated decisions (unlike the EU GDPR), the OAIC encourages entities to implement accountability mechanisms and human oversight, especially when decisions made by AI affect access to services or rights.[106]

The OAIC has released two guides to clarify how Australia's privacy laws apply to AI:[107]

- Guidance on Privacy and the Use of Commercially Available AI Products: This guide assists organisations in complying with privacy obligations when using AI products like chatbots and content-generation tools. It emphasises conducting due diligence, embedding human oversight, and regularly reviewing AI products to ensure they remain fit for purpose and compliant with privacy laws.[108]
- Guidance on Privacy and Developing and Training Generative AI Models: Targeting developers, this guide highlights the need to assess whether training data contains personal or sensitive information and ensures that its use complies with privacy obligations.[109]

In collaboration with the Australian Cyber Security Centre, the OAIC also released a joint statement on responsible AI use (2023), which reinforces the importance of robust security and de-identification practices when using personal data in AI training and inference processes. This joint guidance reflects increasing regulatory interest in safeguarding against misuse of personal data in AI development.

The OAIC also contributed to the development of the Australian Government's AI Ethics Principles, released in 2019 by the Department of Industry, Science and Resources. These eight voluntary principles include: human-centred values; privacy protection; fairness; transparency; contestability; and accountability. While non-binding, these principles are widely regarded as best practice for ethical AI use, particularly in government and regulated sectors.[110]

## 20 Trends and Developments

**20.1 In your opinion, what enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.**

The trending topic concerning enforcement over the previous 12 months and prior has primarily been the OAIC's proactive approach to ensuring compliance with privacy obligations, particularly through targeted reviews and regulatory action.[111] In December 2025, the OAIC launched its first-ever privacy compliance sweep, targeting businesses that collect personal information in person, and the initiative continues to draw attention in early 2026 as the regulator progresses its review. The sweep, announced on 9 December 2025, marked a significant step in the OAIC's proactive enforcement strategy, aiming to ensure that entities meet the requirements of the Privacy Act and provide clear, transparent privacy policies to individuals.

The compliance sweep focused on approximately 60 entities across six sectors where in-person the collection of personal information is common. These sectors included rental and property services, chemists and pharmacists, licensed venues, car rental companies, car dealerships, and pawnbrokers and second-hand dealers. These industries were selected due to the heightened privacy risks associated with the collection of personal information, including identity documents, and the history of breaches or compliance concerns. Target entities were chosen based on size, location, and risk profile, including those previously involved in data incidents.[112]

Central to the sweep was an assessment of entities' compliance with APP 1.4, which sets out the minimum content requirements for privacy policies. The OAIC evaluated whether businesses clearly communicated how personal information is collected, used, disclosed, and managed, reflecting the regulator's broader goal of promoting transparency and protecting individual rights. The OAIC also issued updated guidance on APP 1 to clarify regulatory expectations and assist businesses in improving their privacy practices.[113]

Privacy Commissioner Carly Kind highlighted the focus on in-person data collection as addressing significant power and information asymmetries: 'Consumers often have limited information when asked for personal details by retailers, licensed venues, or service providers, which can create risks of overcollection and undermine privacy'. The sweep was designed to encourage entities to reflect on the robustness of their privacy practices and ensure they are meeting their statutory obligations.[114]

Entities found to be non-compliant may face compliance or infringement notices, with penalties of up to AU$66,000 following legislative amendments in 2024 that expanded the OAIC's enforcement powers. The regulator has emphasised a risk-based and proportionate approach to enforcement, using the sweep not only to address non-compliance but also to signal broader expectations for privacy practices in sectors where individuals' information is collected directly.[115]

As of March 2026, the OAIC continues to progress the review, with early findings expected to inform further regulatory action and guidance, reinforcing the importance of clear, accessible privacy policies and the protection of personal information across high-risk sectors.

**20.2 In your opinion, what "hot topics" are currently a focus for the data protection regulator?**

The OAIC's Corporate Plan for 2025–26 outlines the agency's strategic priorities and key activities aimed at promoting and upholding privacy and information access rights in Australia.[116]

In 2024, the OAIC underwent significant leadership changes, including the appointment of three commissioners: the Australian Information Commissioner; a Privacy Commissioner; and a Freedom of Information Commissioner. This restructuring is intended to bolster the OAIC's capacity to address the increasing complexity and volume of privacy and information access matters.

The Corporate Plan emphasises several key areas, as outlined below.[117]

In 2025–26, the OAIC's regulatory priorities will centre on rebalancing power and information asymmetries, safeguarding rights in the context of emerging technologies, strengthening information governance across the Australian Public Service, and ensuring timely access to government information.[118]

Firstly, in addressing power and information asymmetries, the OAIC will target sectors and technologies that undermine individual rights and create structural imbalances. This will include regulatory attention on the rental and property sector, credit reporting, and data brokerage practices. The OAIC will also scrutinise advertising technology, such as pixel tracking, and practices involving the excessive collection and retention of personal information. Particular emphasis will be placed on

the application of AI where it erodes privacy and information access rights, as well as systemic failures that hinder timely access to government-held information.[119]

In relation to rights preservation in new and emerging technologies, the OAIC will actively protect privacy and information access rights in high-impact technological contexts. This will include oversight of facial-recognition systems and other forms of biometric scanning, alongside emerging surveillance technologies such as location tracking across applications, vehicles and connected devices. The OAIC will also focus on ensuring that government use of AI and automated decision-making systems align with established privacy and transparency obligations.[120]

On the information governance front, the OAIC will seek to strengthen the management and integrity of information within the Australian Public Service. This will involve identifying deficiencies in information handling practices across the data lifecycle, including the administration of requests under the Freedom of Information Act and the Privacy Act. The OAIC will provide guidance aimed at improving administrative decision-making, monitor the use of messaging applications by government agencies, and address integrity risks arising from poor information management practices that may undermine public trust.[121]

Finally, in promoting timely access to government information, the OAIC will reinforce compliance with the objects of the Freedom of Information Act. It will progress complaint investigations and undertake monitoring activities, using data-driven insights to identify systemic underperformance across agencies. Particular focus will be given to refusal rates, adherence to statutory timeframes, disclosure log practices, and compliance with the Information Publication Scheme, with a view to enhancing transparency and accountability across government.

## Endnotes

1 'Law in Australia' DLA Piper: https://www.dlapiperdataprotection.com/index.html?t=law&c=AU (last modified 31 December 2023) (accessed 30 March 2024).

2 Office of the Australian Information Commissioner, *Rights and responsibilities*: https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/rights-and-responsibilities#OrgAndAgencyPrivacyActCovers (accessed 23 April 2026).

3 See Chapter B of the *Australian Privacy Principle Guidelines* (APP Guidelines): https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#app-entity

4 Office of the Australian Information Commissioner, *Rights and responsibilities*: https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/rights-and-responsibilities#OrgAndAgencyPrivacyActCovers (accessed 23 April 2026).

5 *Ibid.*

6 Office of the Australian Information Commissioner, *Passing of bill a significant step for Australia's privacy law*: https://www.oaic.gov.au/news/media-centre/pasing-of-bill-a-significant-step-for-australias-privacy-law (accessed 23 April 2026).

7 Office of the Australian Information Commissioner, *Employee records exemption*: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/employee-records-exemption (accessed 23 April 2026).

8 Office of the Australian Information Commissioner, *Small business*: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/small-business (accessed 23 April 2026).

9 Office of the Australian Information Commissioner, *Political parties and elections*: https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/political-parties-and-elections (accessed 23 April 2026).

10 Office of the Australian Information Commissioner, *Part 4: Exemptions*: https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/part-4-exemptions (accessed 23 April 2026).

11 Office of the Australian Information Commissioner, *Chapter 12: APP 12 Access to personal information* – [Key points]: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-12-app-12-access-to-personal-information (accessed 20 March 2026).

12 *Ibid.* [12.3]: APP 12 operates alongside and does not replace other informal or legal procedures by which an individual can be given access to information. In particular, APP 12 does not prevent an APP entity from giving access to personal information under an informal administrative arrangement, provided the minimum access requirements stipulated in APP 12 have been met.

13 Office of the Australian Information Commissioner, *Chapter 13: APP 13 Correction of personal information* – [Key points]: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-13-app-13-correction-of-personal-information (accessed 20 March 2026).

14 Office of the Australian Information Commissioner, *Chapter 2: APP 2 Anonymity and pseudonymity* – [Key points]: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-2-app-2-anonymity-and-pseudonymity (accessed 20 March 2026).

15 Office of the Australian Information Commissioner, *Chapter 5: APP 5 Notification of the collection of personal information* – [Key points]: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information (accessed 20 March 2026).

16 Office of the Australian Information Commissioner, *Chapter 3: APP 3 Collection of solicited personal information* – [Key points]: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information (accessed 20 March 2026).

Office of the Australian Information Commissioner, *Chapter 6: APP 6 Use or disclosure of personal information*: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information (accessed 20 March 2026).

17 Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines (Chapter B: 'Consent')* [B.37]–[B.45]: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts (accessed 20 March 2026).

18 ACCC, *Consumer Data Right*: https://www.accc.gov.au/by-industry/banking-and-finance/the-consumer-data-right (accessed 20 March 2026).

19 Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines (Chapter B: 'Consent')* [B.37]–[B.45]: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts (accessed 20 March 2026).

20 *Ibid.*

21 *Ibid.*

22 Office of the Australian Information Commissioner, *Chapter 7: APP 7 Direct marketing* – [Key points]: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-7-app-7-direct-marketing (accessed 20 March 2026).

23 *Ibid*.

24 Office of the Australian Information Commissioner, *Chapter 2: APP 2 Anonymity and pseudonymity* – [Key points]: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-2-app-2-anonymity-and-pseudonymity (accessed 20 March 2026).

25 Office of the Australian Information Commissioner, *Chapter 5: APP 5 Notification of the collection of personal information* – [Key points]: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information (accessed 20 March 2026).

26 Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines (Chapter B: 'Consent')* [B.59]–[B.61]: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts (accessed 20 March 2026).

27 *Ibid*.

28 Office of the Australian Information Commissioner, Children's Online Privacy Code: https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes/childrens-online-privacy-code (accessed 25 March 2026).

29 Office of the Australian Information Commissioner, *Data breach preparation and response*: 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 (accessed 20 March 2026).

30 'Data Protection Laws of the World' *DLA Piper*: https://www.dlapiperdataprotection.com/index.html?t=data-protection-officers&c=AU (last modified 31 December 2023) (accessed 28 March 2024).

31 'Australia – Data Protection Overview' *Alec Christie Clyde and Co*: https://www.dataguidance.com/notes/australia-data-protection-overview (October 2023) (accessed 28 March 2024).

32 Attorney-General's Department (Australia), *Privacy Act Review Final Report* (2022): https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf, p. 44.

33 Office of the Australian Information Commissioner, *Privacy Officer Toolkit*: https://education.oaic.gov.au/privacy-officer-toolkit/#section-12 (accessed 29 March 2024).

34 Office of the Australian Information Commissioner, *Privacy Officer Toolkit*: https://education.oaic.gov.au/privacy-officer-toolkit/#section-12 (accessed 29 March 2024).

35 Office of the Victorian Information Commissioner, 'The Role of the Privacy Officer': https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-officer-toolkit/the-role-of-the-privacy-officer (accessed 29 March 2024).

36 Office of the Australian Information Commissioner, *Privacy Officer Toolkit*: https://education.oaic.gov.au/privacy-officer-toolkit/#section-1 (accessed 29 March 2024).

37 Office of the Australian Information Commissioner, *Australian Entities and the European Union General Data Protection Regulation*: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/more-guidance/australian-entities-and-the-european-union-general-data-protection-regulation (accessed 29 March 2024).

38 *Privacy Act 1988* (Cth) sch 1, APP 7.1: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-7-app-7-direct-marketing

39 *Privacy Act 1988* (Cth) sch 1, APP 7.2: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-7-app-7-direct-marketing

40 Office of the Australian Information Commissioner, *Advertising, Marketing and Spam*, (Webpage, Office of the Australian Information Commissioner, 2024): https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/advertising,-marketing-and-spam (accessed 29 March 2024).

41 *Spam Act 2003*, section 7.

42 Office of the Australian Information Commissioner, *Infringement Notice: Spam Act 2003:* https://www.acma.gov.au/sites/default/files/2026-03/Lululemon%20-%20Spam%20Infringement%20Notice_Redacted.pdf (accessed 19 March 2026).

43 *Ibid*.

44 *Ibid*.

45 Office of the Australian Information Commissioner, *Chapter 3: APP 3 Collection of solicited personal information* [3.6]: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information (accessed 29 March 2023).

46 Katherine Kemp, 'Australia's forgotten Privacy Principle: Why Common 'Enrichment' of Customer Data for profiling and targeting is Unlawful' (2022) *University of New South Wales*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4224653

47 Office of the Australian Information Commissioner, *Chapter 3: APP 3 Collection of solicited personal information* [3.6]: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information (accessed 29 March 2023).

48 *Ibid*., 3.65.

49 *Ibid*., 3.68.

50 *Do Not Call Registry Act 2006*, section 25.

51 Office of the Australian Information Commissioner, *Targeted Online Marketing*: https://www.oaic.gov.au/privacy/your-privacy-rights/social-media-and-online-privacy/targeted-online-marketing (accessed 29 March 2024).

52 Office of the Australian Information Commissioner, *Part 8: Overseas data flows*: https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/part-8-overseas-data-flows [8.1] (accessed 29 March 2023).

53 Office of the Australian Information Commissioner, *Cross-border disclosure of personal information – APP 8 guidance* [8.16]–[8.17]: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information (accessed 19 March 2026).

54 Abigail McGregor, 'A new era for Whistleblowers in Australia' (January 2023): https://www.nortonrosefulbright.com/en/knowledge/publications/63b0f230/update-on-new-whistleblower-protection-laws-in-australia (accessed 29 March 2023).

55 *Corporations Act 2001*, section 137AI (5)(c).

56 *Surveillance Devices Act 2004* (Cth).

57 Office of the Australian Information Commissioner, 'Security Cameras' (Government website): https://www.oaic.gov.au/privacy/your-privacy-rights/surveillance-and-monitoring/security-cameras

58 *Ibid*.

59 *Surveillance Devices Act 2007* (NSW).

60 NSW Police Force, CCTV Register (PDF Brochure): https://www.police.nsw.gov.au/__data/assets/pdf_file/0011/105113/nsw_cctv_brochure.pdf

61 Office of the Information Commissioner Queensland, Privacy and technology (Government website): https://www.oic.qld.gov.au/government/privacy/privacy-technology

62 Office of the Australian Information Commissioner, 'Security Cameras' (Government website): https://www.oaic.gov.au/privacy/your-privacy-rights/surveillance-and-monitoring/security-cameras

63 *Workplace Surveillance Act 2005* (NSW) Part 2.

64 *Surveillance Devices Act 1999* (VIC) Part 2A.

65 Office of the Australian Information Commissioner, *Workplace monitoring and surveillance* para 3: https://www.oaic.gov.au/privacy/your-privacy-rights/surveillance-and-monitoring/workplace-monitoring-and-surveillance (accessed 19 March 2026).

66 *Workplace Surveillance Act 2005* (NSW) Part 2 sections 10–13.

67 Office of the Australian Information Commissioner, 'Employee records exemption' (Government website): https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/employee-records-exemption

68 *Ibid.*

69 Office of the Australian Information Commissioner, 'Chapter 11: APP 11 Security of personal information' (Government website): https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information

70 *Ibid.*

71 Office of the Australian Information Commissioner, 'Report a data breach' (Government website): https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach

72 *Ibid.*

73 Office of the Australian Information Commissioner, 'About the Notifiable Data Breaches scheme' (Government website): https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme

74 Office of the Australian Information Commissioner, 'Part 3: Responding to data breaches – four key steps' (Government website): 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/part-3-responding-to-data-breaches-four-key-steps

75 *Privacy Act 1988* (Cth) section 26WH(1).

76 *Privacy Act 1988* (Cth) section 26WH(2).

77 *Privacy Act 1988* (Cth) section 26WL(2)(a).

78 *Privacy Act 1988* (Cth) section 26WL(2)(b).

79 Office of the Australian Information Commissioner, 'What to include in an eligible data breach statement' (Government website): 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/part-4-notifiable-data-breach-ndb-scheme#assessing-a-suspected-data-breach

80 *Privacy Act 1988* (Cth) section 40.

81 *Privacy Act 1988* (Cth) section 40(2).

82 Office of the Australian Information Commissioner, 'Chapter 2: Commissioner initiated investigations and referrals' (Government website): https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-2-commissioner-initiated-investigations-and-referrals

83 *Ibid.*

84 Office of the Australian Information Commissioner, 'Chapter 13: APP 13 Correction of personal information' (Government website): https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-13-app-13-correction-of-personal-information

85 *Ibid.*

86 Office of the Australian Information Commissioner, 'Consumer consent, authorisation and dashboards' (Government website): https://www.oaic.gov.au/consumer-data-right/consumer-data-right-guidance-for-business/privacy-obligations/consumer-consent,-authorisation-and-dashboards

87 Office of the Australian Information Commissioner, 'Rules and guidelines' (Government website): https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/rules-and-guidelines

88 Office of the Australian Information Commissioner, 'Chapter 8: Infringement notices' (Government website): https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-8-infringement-notices

89 Office of the Australian Information Commissioner, 'Civil Penalties – serious or repeated interferences with privacy and other penalty provisions' (Government website): https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-7-privacy-assessments

90 *Privacy Act 1988* (Cth) section 80W.

91 Office of the Australian Information Commissioner, 'Chapter 6: Injunctions' (Government website): https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-6-injunctions

92 https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-decisions/enforceable-undertakings/oxfam-australias-enforceable-undertaking-in-respect-of-the-australian-information-commissioners-investigation-into-oxfam-oaic-reference-cii2100010

93 Commissioner Initiated Investigation into Vinomofo Pty Ltd (Privacy) [2025] AICmr 175.

94 https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-3-information-sharing#information-sharing-with-other-authorities

95 *Privacy Act 1988* (Cth) section 33A.

96 Office of the Australian Information Commissioner, 'Chapter 8: APP 8 Cross-border disclosure of personal information' (Government website): https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information#when-does-an-app-entity-disclose-personal-information-about-an-individual-to-an-overseas-recipient

97 *Ibid.*

98 Australian Signals Directorate, Intelligence partnerships (Government website): https://www.asd.gov.au/about/history/75th-anniversary/stories/2022-03-16-intelligence-partnerships

99 Attorney General (Cth), 'Mutual assistance overview' (Government website): https://www.ag.gov.au/international-relations/publications/mutual-assistance-overview

100 Austlii, 'Accession by Australia to the Convention on Cybercrime' (Legal database): https://www.austlii.edu.au/au/other/dfat/nia/2011/9.html

101 Australian Taxation Office, 'Tax information exchange agreements – overview' (Government website): https://www.ato.gov.au/about-ato/international-tax-agreements/in-detail/tax-information-exchange-agreements-tiea/tax-information-exchange-agreements-overview

102 Office of the Australian Information Commissioner, 'Chapter 8: APP 8 Cross-border disclosure of personal information' (Government website): https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information

103 *Ibid.*

104 *Privacy Act 1988* (Cth) – Part IIIB.

105 Office of the Australian Information Commissioner, *Guidance on privacy and the use of commercially available AI products*: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products (accessed 23 April 2026).

106 *Ibid*.

107 Mondaq, *The crossroads of AI and privacy compliance: OAIC publishes new guidance*: https://www.mondaq.com/australia/privacy-protection/1538958/the-crossroads-of-ai-and-privacy-compliance-oaic-publishes-new-guidance (accessed 23 April 2026).

108 Office of the Australian Information Commissioner, *Guidance on privacy and the use of commercially available AI products*: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products (accessed 23 April 2026).

109 Office of the Australian Information Commissioner, *Guidance on privacy and developing and training generative AI models*: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-developing-and-training-generative-ai-models (accessed 23 April 2026).

110 Commonwealth of Australia, *National framework for the assurance of artificial intelligence in government*: https://www.finance.gov.au/sites/default/files/2024-06/National-framework-for-the-assurance-of-AI-in-government.pdf (accessed 23 April 2026).

111 Office of the Australian Information Commissioner, *Privacy compliance sweep to put privacy policies under the spotlight*: https://www.oaic.gov.au/news/media-centre/privacy-compliance-sweep-to-put-privacy-policies-under-the-spotlight (accessed 23 April 2026).

112 *Ibid*.

113 *Ibid*.

114 *Ibid*.

115 *Ibid*.

116 Office of the Australian Information Commissioner, *Corporate plan 2025–26*: https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/corporate-plans/corporate-plan-2025-26 (accessed 23 April 2026).

117 Office of the Australian Information Commissioner, *Corporate plan 2024–25*: https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/corporate-plans/corporate-plan-2024-25 (accessed 23 April 2026).

118 Office of the Australian Information Commissioner, *Corporate plan 2025–26*: https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/corporate-plans/corporate-plan-2025-26 (accessed 23 April 2026).

119 *Ibid*.

120 *Ibid*.

121 *Ibid*.

**Dennis Miralis** is a leading Australian defence lawyer specialising in international criminal law, with a focus on complex multi-jurisdictional regulatory investigations and prosecutions. His areas of expertise include: bribery and corruption; global tax investigations; proceeds of crime; AML; worldwide freezing orders; cybercrime; national security law; Interpol Red Notices; extradition; and mutual legal assistance law. Dennis advises individuals and companies under investigation for economic crimes both locally and internationally. He has extensive experience in dealing with all major Australian and international investigative agencies.

**Nyman Gibson Miralis**
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: dm@ngm.com.au
LinkedIn: www.linkedin.com/in/dennis-miralis-criminal-lawyer

**Jack Dennis** is a senior criminal defence lawyer who brings significant experience in international, corporate and tax matters to his role at Nyman Gibson Miralis, having worked at a top-tier commercial firm and advised on cross-border transactions and disputes involving foreign and domestic corporations and individuals across the software, financial services and crypto industries. His international criminal work involves transnational criminal and regulatory investigations, often working in parallel with other jurisdictions to co-ordinate with foreign law enforcement, intelligence and regulatory agencies. Through such matters, Jack has developed expertise in extraditions, sanctions, customs, white-collar crime and national security.

**Nyman Gibson Miralis**
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: jd@ngm.com.au
LinkedIn: www.linkedin.com/in/jack-jon-dennis

**Phillip Salakas** is a defence lawyer who assists the partners with complex criminal matters and investigations involving corporate and financial crime as part of Nyman Gibson Miralis's white-collar crime team. Phillip has completed a Bachelor of Laws degree at the University of Technology Sydney and has previously worked in the area of general crime.

**Nyman Gibson Miralis**
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: psa@ngm.com.au
LinkedIn: www.linkedin.com/in/phillip-salakas

**Henry Yu** is an international criminal lawyer and part of the white-collar investigations team at Nyman Gibson Miralis. He assists the partners in various international criminal law matters, focusing on white-collar crime, anti-bribery and corruption, anti-money laundering, tax fraud and evasion, and cybercrime. With extensive experience in financial crime, foreign bribery, high-value taxation investigations and disputes, tax fraud and evasion, money laundering, and unexplained wealth matters, Henry brings a comprehensive understanding to complex legal challenges.

**Nyman Gibson Miralis**
Level 9, 299 Elizabeth Street
Sydney NSW 2000
Australia

Tel: +61 2 9264 8884
Email: hy@ngm.com.au
LinkedIn: www.linkedin.com/in/henryyehuiyu-solicitor

Nyman Gibson Miralis is an international, award-winning criminal defence law firm based in Sydney, Australia. For over 55 years it has been leading the market in all aspects of general, complex and international crime, and is widely recognised for its involvement in some of Australia's most significant criminal cases.

Our international law practice focuses on white-collar and corporate crime, transnational financial crime, international sanctions, bribery and corruption, international money-laundering, cybercrime, international asset-freezing/forfeiture, extradition and mutual-assistance law.

Nyman Gibson Miralis strategically advises and appears in matters where cross-border investigations and prosecutions are being conducted in parallel jurisdictions, involving some of the largest law enforcement agencies and financial regulators worldwide.

Working with our international partners, we have advised and acted in investigations involving the British Virgin Islands, Cambodia, Canada, China, the EU, Hong Kong, Macao, Mexico, New Zealand, Russia, South Africa, South Korea, Singapore, Taiwan, the UK, the US and Vietnam.

**www.ngm.com.au**

NYMAN GIBSON MIRALIS
Defence Lawyers and Advisors est. 1966

# iclg International Comparative Legal Guides

The **International Comparative Legal Guides** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 59 practice areas.

**Data Protection 2026** features three expert analysis chapters and 23 Q&A jurisdiction chapters covering key issues, including:

- Relevant Legislation and Competent Authorities
- Territorial and Material Scope
- Key Principles
- Individual Rights
- Children's Personal Data
- Registration Formalities and Prior Approval
- Appointment of a Data Protection Officer
- Appointment of Processors
- Marketing
- Cookies
- Restrictions on International Data Transfers
- Whistle-blower Hotlines
- CCTV
- Employee Monitoring
- Data Security and Data Breach
- Enforcement and Sanctions
- E-discovery/Disclosure to Foreign Law Enforcement Agencies
- Artificial Intelligence
- Trends and Developments

The International Comparative Legal Guides are published by: glg Global Legal Group