Data Protection Laws and Regulations Australia 2024-2025

ICLG - Data Protection Laws and Regulations - Australia Chapter covers common issues including relevant legislation and competent authorities, territorial scope, key principles, individual rights, registration formalities, appointment of a data protection officer and processors.

Published: 31/07/2024

Chapter Content Free Access

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* (Australian Capital Territory); the *Privacy and Personal Information Protection Act 1998* (New South Wales, '**NSW**'); the *Information Privacy Act 2009* (Queensland, '**QLD**'); the *Personal Information and Protection Act 2004* (Tasmania); and the *Privacy and Data Protection Act 2014* (Victoria, '**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* ('**MHR**') *Act 2012* (Cth) 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.[i]

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 Telecommunications Act; the *Health Records Act 2001* (VIC); the *Health Records*; and the *Workplace Surveillance Act 2005* (NSW).[ii]

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

The Office of the Australian Information Commissioner ('**OAIC**') is an independent statutory agency which is endowed with functions under the Privacy Act and other legislation relating to data protection.

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. In coordination with the OAIC, the National Health and Medical Research Council has issued a number of 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' as information or an opinion about an individual's:
    - 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,that is also personal information or:
    - 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.
- "I**dentification 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; or

- an unincorporated association that has its central management and control in Australia or an external territory.

An organisation or small business operator also has an Australian link if all of the following apply:

- the organisation or operator is not described in subsection 2; and
- the organisation or operator carries on business in Australia or an external territory.

However, section 6A of the Privacy Act dictates that the APPs will not be breached by any conduct external to Australia that is required by an applicable foreign law.

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.

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 deidentified.
- **Crossborder 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 the information is being disclosed 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. The APP entity is not required to give the individual access to the personal information in certain circumstances set out in 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.

- **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.

- **Right to deletion/right to be forgotten**: Where an APP entity holds personal information about an individual and the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity, APP 11.2 requires that the APP entity take reasonable steps to destroy the information or to ensure that it is deidentified. This is subject to the information not being contained in a Commonwealth record and the APP entity not being required by or under an Australian law, or a court/tribunal order, to retain 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). 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.
- **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)), there is no right bestowed on individuals 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.
- **Right to data portability**: A broad right to data portability does not presently exist under Australian law (although, pursuant to APP 12, individuals can request a copy of

their personal information held by an APP entity). However, the Australian Government is actively moving to progressively legislate this right – to be known as 'consumer data right' ('**CDR**') – into Australian law. The Australian Competition and Consumer Commission will be the lead regulator of CDR.

- **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. 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. Individuals should be made aware of the potential implications of withdrawing consent, such as no longer being able to access a service.
- **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. If such a request is made, the entity must cease direct marketing to the individual.
- **Right protecting against 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.
- **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. For example, if an individual's privacy complaint is about a bank in Australia, he or she can contact the Australian Financial Complaints Authority.
- **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.
- **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.

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.

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.

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.

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 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 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 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 question 7.1.

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

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

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

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

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

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

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

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

7.10 Can the registration/notification be completed online?

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

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

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

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

This is not applicable in Australia – please see 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.[iii]

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.[iv] 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.'[v]

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.[vi]

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 organisations size, functions and structure, an organisation may decide to appoint more than one Data Protection Officer/Privacy Officer.[vii]

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.[viii]

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.[ix]

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.[x]

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 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?).

APP 7.1 imposes a general prohibition on the use of personal information for the purpose of direct marketing.[xi] 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.[xii]

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.[xiii]

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.[xiv]

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.

A recent ACMA investigation found that between December 2022 and May 2023, Outdoor Supacentre sent 81,698 text messages to recipients without their consent and 1,575 texts to customers who had previously unsubscribed.[xv] Outdoor Supacentre Pty Ltd (trading as 4WD Supacentre) has paid a $302,500 penalty for sending more than 83,000 marketing text messages in breach of Australian spam laws.[xvi]

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.[xvii]

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.[xviii]

However, for organisations, the exception to the rule requiring direct collection is that it would be unreasonable or impracticable to do so.[xix] 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.[xx]

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.[xxi]

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 $2.1 million, and individual liability for up to $420,000 per day. This will depend on the number of breaches and the history of the actor.[xxii] 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.

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.[xxiii]

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.

'The Attorney General's *Privacy Act Report 2022* proposed certain amendments to be made to APP 8 to apply to de-identified datasets. The Report also recommends prohibiting APP entities from re-identifying de-identified information received from a third party and introducing a new criminal offence for "malicious" re-identification intended to harm or cause illegitimate benefit.' [xxiv]

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.[xxv]

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.

A transfer impact assessment under the GDPR is only mandatory when an entity transfers personal data from the EU or the UK to certain non-European countries like Australia. The goal of the transfer impact assessment is to conduct a risk assessment that aims to mitigate the risks associated with the transfer of personal data.

The organisation exporting personal data outside of the EU needs to carry out this assessment, to ascertain that individuals' rights are protected and maintained in the same way they must be protected under the GDPR.[xxvi]

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, which may help Australian organisations' ability to show GDPR equivalence where Standard Contract Clauses ('**SCCs**') are used.

The landmark *Schrems II* decision addressed the reliance of data controllers and processors on the EU–US Privacy Shield Framework and considered the use of SCCs to demonstrate GDPR compliance.

'The CJEU, while not invalidating SCCs, imposed additional requirements for their use. The CJEU found that SCCs won't always be enough to ensure personal data transferred externally from the EU is adequately protected and therefore compliant with the GDPR.'[xxvii] 'Whether there is adequate protection requires a case-by-case assessment. The CJEU did not provide a full assessment framework, which has led to some uncertainty.'[xxviii]

Australian organisations transferring data from the EU now must promptly analyse their data flows, as doing so on a case-by-case basis is essential for compliance despite the potential burden it poses.[xxix]

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).

From 1 July 2019, the whistleblower protections in Part 9.4AAA of the Corporations Act were expanded to provide greater protections for whistleblowers who report misconduct about companies and company officers. The reforms to the regime were contained in the *Treasury Laws Amendment (Enhancing Whistleblower Protections) Act 2019*, which received Royal Assent on 12 March 2019.[xxx]

The changes to the Corporations Act broaden the scope of protected disclosures, encompassing a wider range of conduct related to 'misconduct' or an 'improper state of affairs', with definitions expanded. Previously, protected disclosures were limited to contraventions of the Corporations legislation. Under the amendments, whistleblowers can make anonymous disclosures without the requirement of 'good faith', although reasonable grounds for concern are necessary.[xxxi]

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 S.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'.[xxxii]

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.[xxxiii] 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.'*[xxxiv]

The Privacy Act does not cover security cameras operated by an individual acting in a private capacity, but state or territory laws may apply to that person.[xxxv]

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).[xxxvi] 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.[xxxvii]
- 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.[xxxviii]

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, it would be appropriate to contact the relevant state or territory Attorney-General department.[xxxix]

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

Similarly to above, the limitations will vary between jurisdictions.

Federal jurisdiction

The OIAC covers the limits of the purposes for which CCTV data may be gathered, this is enunciated to a degree within the APP guidelines.[xl]

State and territories jurisdiction

As cited above, NSW and QLD have respective laws that limit the usage of the CCTV data and that must be for a legitimate purpose and proportionate to achieving that goal.

In NSW, Part 5 Division 1 of the *Surveillance Devices Act 2007* (NSW) governs the usage of data.[xli] In QLD, the *Invasion of Privacy Act 1971* (QLD) governs the usage of data.[xlii]

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,[xliii] 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,[xliv] the surveillance of employees in certain places and circumstances is prohibited.

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.[xlv] 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.[xlvi]

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

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.[xlviii]

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.'[xlix]

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 Notifiable Data Breach ('**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.[l]

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.[li]

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.[lii]

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.[liii]

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,[liv] 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).[lv]

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',[lvi] 'notify only those individuals at risk of serious harm'[lvii] and 'publish notification'. The OAIC has published guidance on what is expected to be included in an eligible data breach statement.[lviii]

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

In light of recent data breach scandals, the Australian Government passed the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022.[lix]

The current penalties have been laid out by the OIAC as of March 2024:[lx]

'Under s 13G of the Privacy Act, the maximum penalty for serious or repeated interferences with privacy are:

- For a body corporate, the greater of either:
    - $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 $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.[lxi] 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.[lxii]

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 Commissioner Initiated Investigation ('**CII**'). Once a CII has been commenced, the OAIC will conduct its investigation in accordance with Part V of the Privacy Act.'[lxiii]

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.[lxiv]

(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'.[lxv]

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

(c) Authorisation and Advisory Powers:

Authorisation: The OAIC has published guidance on authorisation, particularly with regard to consumer authorisation,[lxvii] 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.

Advisory: 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.[lxviii] 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 infringement notice under section 80UB of the Privacy Act with Part 5 of the Regulatory Powers 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.[lxix]

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 further 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.[lxx]

The OAIC has highlighted what 'civil penalty provisions' below:

- 'a serious or repeated interference with privacy (s 13G) with maximum penalties including $2.5 million for a person other than a body corporate, and for a body corporate, an amount not exceeding the greater of:
    - $50 million;
    - three times the value of the benefit obtained directly or indirectly by the body corporate and any related bodies corporate, that is reasonably attributable to the conduct constituting the contravention; or
    - if the court cannot determine the value of the benefit, 30% of the body corporate's adjusted turnover during the breach turnover period for the contravention; and
- various civil penalty provisions set out in Part IIIA – credit reporting, with penalties of either 500, 1,000 or 2,000 penalty units.'

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.[lxxi]

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'.[lxxii]

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

An example of the OAIC's investigative powers can be seen in the case of *Cardiac Dynamics (Privacy)* [2023] AICmr 96 (24 October 2023), the OAIC had opened an investigation into the respondent's compliance with rules within the *MRH Rules 2016*.[lxxiii]

The Commissioner found that the respondents had challenges in producing documents and were not utilising the MHR system despite being registered to do so. The respondent did not have a written policy that complied with rule 42 of the MHR, which required health providers to have a written policy on the use of the MHR system.

The Commissioner made a determination under section 52(1A)(a) and (b) that the respondent must take specific steps outlined to ensure the act or practice is not repeated.

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.[lxxiv]

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

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.[lxxvi]

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 APP8.2(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.[lxxvii]

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 *UKUSA 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.[lxxviii]
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.[lxxix]
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. [lxxx]
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. [lxxxi]

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.[lxxxii]

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.[lxxxiii]

19. Trends and Developments

19.1 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 non-compliance with the OAIC APPs.

The OAIC publishes its privacy determination, in which an observation can be made that there has been an uptick in investigations of healthcare providers not complying with having written a policy on the MHR system. Notable recent cases such as *Cardiac Dynamics*,[lxxxiv] *Rao Medical Centre*,[lxxxv] *Cherrybrook Medical Centre*[lxxxvi] and *Burwood Westfield Medical Centre*[lxxxvii] are cases of medical providers within the past 12 months, where the Commissioner has made a determination that their respective practices have not complied with the MHR Rules.[lxxxviii]

19.2 What "hot topics" are currently a focus for the data protection regulator?

As of 15 January 2024, the OAIC has published its corporate plan for 2023–24, where four areas of regulatory focus have been identified:[lxxxix]

1. **Online platforms, social media and high-privacy impact technologies:** The OAIC is prioritising regulatory activity addressing the harm that arises from specific practices of online platforms and services, through opaque terms and conditions.
2. **Security of personal information**: The OAIC is focusing on the finance and health sector for serious failures to take reasonable steps to protect personal information and use of inappropriate data retention practices and failure to comply with reporting requirements of the NDB Scheme.
3. **Ensuring the privacy safeguards in the CDR are effective** : The OAIC focus will be on ensuring privacy safeguards are being upheld by new entrants to the system, particularly the energy sector.
4. **The timely and proactive release of government-held information**: The OAIC stated 'the timely release of government-held information, with a focus on timely decision-making and proactive release of information, is consistent with the objects of the *Freedom of Information Act 1982* and supports participative democracy', which is the key point of this area of focus.

Endnotes

[i] 'Law in Australia' *DLA Piper* < [Hyperlink];c=AU > (last modified 31 December 2023) (accessed 30 March 2024).

[ii] *Ibid*.

[iii] 'Data Protection Laws of the World' *DLA Piper* < [Hyperlink];c=AU > (last modified 31 December 2023) (accessed 28 March 2024).

[iv] 'Australia – Data Protection Overview' *Alec Christie Clyde and Co* < [Hyperlink] > (October 2023) (accessed 28 March 2024).

[v] Attorney-General's Department (Australia), *Privacy Act Review Final Report* (2022) < [Hyperlink] >, p44.

[vi] Office of the Australian Information Commissioner, *Privacy Officer Toolkit* < [Hyperlink] > (accessed 29 March 2024).

[vii] Office of the Australian Information Commissioner, *Privacy Officer Toolkit* < [Hyperlink] > (accessed 29 March 2024).

[viii] Office of the Victorian Information Commissioner, 'The Role of the Privacy Officer' < [Hyperlink] > (accessed 29 March 2024).

[ix] Office of the Australian Information Commissioner, *Privacy Officer Toolkit* < [Hyperlink] > (accessed 29 March 2024).

[x] Office of the Australian Information Commissioner, *Australian Entities and the European Union General Data Protection Regulation* < [Hyperlink] > (accessed 29 March 2024).

[xi] *Privacy Act 1988* (Cth) sch 1, APP 7.1 < [Hyperlink] >.

[xii] *Privacy Act 1988* (Cth) sch 1, APP 7.2 < [Hyperlink] >.

[xiii] Office of the Australian Information Commissioner, *Advertising, Marketing and Spam*, (Webpage, Office of the Australian Information Commissioner, 2024) < [Hyperlink] > (accessed 29 March 2024).

[xiv] *Spam Act 2003*, section 7.

[xv] Australian Communications and Media Authority, *Outdoor Supacentre pays $300k penalty for spam breaches*, (31 January 2024) < [Hyperlink] > (accessed 29 March 2024).

[xvi] *Ibid*.

[xvii] Office of the Australian Information Commissioner, *Chapter 3: APP 3 Collection of solicited personal information* < [Hyperlink];> (accessed 29 March 2023).

[xviii] 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* < [Hyperlink] >.

[xix] Office of the Australian Information Commissioner, *Chapter 3: APP 3 Collection of solicited personal information* < [Hyperlink] > (accessed 29 March 2023).

[xx] *Ibid*, 3.65.

[xxi] *Ibid*, 3.68.

[xxii] *Do Not Call Registry Act 2006*, section 25.

[xxiii] Office of the Australian Information Commissioner, *Targeted Online Marketing*, < [Hyperlink] > (accessed 29 March 2024).

[xxiv] Melissa Fai, Andrew Hii and Claire Harris, 'Privacy Act Review Report: Highlights and Hot takes', (16 February 2023) *Gilbert and Tobin*, < [Hyperlink] > (accessed 29 March 2023).

[xxv] Office of the Australian Information Commissioner, *Part 8: Overseas data flows* < [Hyperlink] > (accessed 29 March 2023).

[xxvi] Lillan Zhang, 'Transfer Impact Assessments (TIAs)' (29 August 2023) *Harper James Solicitors* < [Hyperlink] > (accessed 29 March 2023).

[xxvii] Dan Pearce and Louise Almedia, '*Schrems II*: What is the Australian impact of the GDPR decision?' (31 March 2021) *Holding Redlich* < [Hyperlink]; (accessed 29 March 2023).

[xxviii] *Ibid*.

[xxix] Paul Kallenbach, Zita Megyeri and Darcy O'Brien, '*Schrems II*: What the end of the EU-US Privacy Shield means in Australia' (12 November 2020) *MinterEllison* < [Hyperlink] > (accessed 29 March 2023).

[xxx] Australian Securities Investigation Commission, *Protection for Corporate Sector Whistleblowers* < [Hyperlink] > (accessed 29 March 2023).

[xxxi] Abigail McGregor, 'A new era for Whistleblowers in Australia', (January 2023), < [Hyperlink] > (accessed 29 March 2023).

[xxxii] *Corporations Act 2001*, section 137AI (5)(c).

[xxxiii] *Surveillance Devices Act 2004* (Cth).

[xxxiv] Office of the Australian Information Commissioner, 'Security Cameras' (Government website) < [Hyperlink] >.

[xxxv] *Ibid*.

[xxxvi] *Surveillance Devices Act 2007* (NSW).

[xxxvii] NSW Police Force, CCTV Register (PDF Brochure) < [Hyperlink] >.

[xxxviii] Office of the information Commissioner Queensland, Camera Surveillance and Privacy (Government Website) < [Hyperlink] >.

[xxxix] Office of the Australian Information Commissioner, 'Security Cameras' (Government website) < [Hyperlink] >.

[xl] *Ibid*.

[xli] *Surveillance Devices Act 2007* (NSW) Part 5 Division 1.

[xlii] *Invasion of Privacy Act 1971* (QLD).

[xliii] *Workplace Surveillance Act 2005* (NSW) Part 2.

[xliv] *Surveillance Devices Act 1999* (VIC) Part 2A.

[xlv] *Workplace Surveillance Act 2005* (NSW) Part 2 sections 10–13.

[xlvi] Office of the Australian Information Commissioner, 'Employee records exemption' (Government website) < [Hyperlink] >.

[xlvii] *Ibid*.

[xlviii] Office of the Australian Information Commissioner, 'Chapter 11: APP 11 Security of personal information'. (Government website) < [Hyperlink] >.

[xlix] *Ibid*.

[l] Office of the Australian Information Commissioner, 'Report a data breach' (Government website) < [Hyperlink] >.

[li] Ibid.

[lii] Office of the Australian Information Commissioner, 'About the Notifiable Data Breaches scheme' (Government website) < [Hyperlink] >.

[liii] Office of the Australian Information Commissioner, 'Part 3: Responding to data breaches – four key steps' (Government website) < [Hyperlink] >.

[liv] *Privacy Act 1988* (Cth) section 26WH(1).

[lv] *Privacy Act 1988* (Cth) section 26WH(2).

[lvi] *Privacy Act 1988* (Cth) section 26WL(2)(a).

[lvii] *Privacy Act 1988* (Cth) section 26WL(2)(b).

[lviii] Office of the Australian Information Commissioner, 'What to include in an eligible data breach statement', (Government website) < [Hyperlink] >.

[lix] Attorney-General (Cth), 'Parliament approves Government's privacy penalty bill' (Media release, 28 November 2022).

[lx] Office of the Australian Information Commissioner, 'Civil Penalties – serious or repeated interferences with privacy and other penalty provisions' (Government website) < [Hyperlink] >.

[lxi] *Privacy Act 1988* (Cth) section 40.

[lxii] *Privacy Act 1988* (Cth) section 40(2).

[lxiii] Office of the Australian Information Commissioner, 'Chapter 2: Commissioner initiated investigations and referrals' (Government website) < [Hyperlink] >.

[lxiv] *Ibid*.

[lxv] Office of the Australian Information Commissioner, 'Chapter 13: APP 13 Correction of personal information' (Government website) < [Hyperlink] >.

[lxvi] *Ibid*.

[lxvii] Office of the Australian Information Commissioner, 'Consumer consent, authorisation and dashboards' (Government website) < [Hyperlink] >.

[lxviii] Office of the Australian Information Commissioner, 'Rules and guidelines' (Government website) < [Hyperlink] >.

[lxix] Office of the Australian Information Commissioner, 'Chapter 8: Infringement notices' (Government website) < [Hyperlink]

[lxx] Office of the Australian Information Commissioner, 'Civil Penalties – serious or repeated interferences with privacy and other penalty provisions' (Government website) < [Hyperlink] >.

[lxxi] *Privacy Act 1988* (Cth) section 80W.

[lxxii] Office of the Australian Information Commissioner, 'Chapter 6: Injunctions' (Government website) < [Hyperlink] >.

[lxxiii] *Cardiac Dynamics (Privacy)* [2023] AICmr 96 (24 October 2023).

[lxxiv] [Hyperlink]

[lxxv] *Privacy Act 1988* (Cth) section 33A.

[lxxvi] Office of the Australian Information Commissioner, 'Chapter 8: APP8 Cross-border disclosure of personal information' (Government website) < [Hyperlink] >.

[lxxvii] *Ibid*.

[lxxviii] Australian Signals Directorate, Intelligence partnerships (Government website) < [Hyperlink] >.

[lxxix] Attorney General (Cth), 'Mutual assistance overview' (Government website) < [Hyperlink] >.

[lxxx] Austlii, 'Accession by Australia to the Convention on Cybercrime' (Legal database) < [Hyperlink] >.

[lxxxi] Australian Taxation Office, 'Tax information exchange agreements – overview' (Government website) < [Hyperlink] >.

[lxxxii] Office of the Australian Information Commissioner, 'Chapter 8: APP 8 Cross-border disclosure of personal information' (Government website) < [Hyperlink] >.

[lxxxiii] *Ibid*.

[lxxxiv] [Hyperlink]

[lxxxv] [Hyperlink]

[lxxxvi] [Hyperlink]

[lxxxvii] [Hyperlink]

[lxxxviii] Office of the Australian Information Commissioner, 'Privacy determinations' (Government website) < [Hyperlink] >.

[lxxxix] Office of the Australian Information Commissioner, 'Corporate Plan 2023–2024' (Government website) < [Hyperlink] >.

Production Editor's Note

This chapter has been written by a member of ICLG's international panel of experts, who has been exclusively appointed for this task as a leading professional in their field by **Global Legal Group**, ICLG's publisher. ICLG's in-house editorial team carefully reviews and edits each chapter, updated annually, and audits each one for originality, relevance and style, including anti-plagiarism and AI-detection tools. This chapter was copy-edited by **Maya Tyrrell**, our in-house editor.