DATA PROTECTION & PRIVACY

Australia

LEXOLOGY
Getting The Deal Through

Consulting editor

Hunton Andrews Kurth LLP

Data Protection & Privacy

Consulting editors

Aaron P Simpson, Lisa J Sotto

Hunton Andrews Kurth LLP

Quick reference guide enabling side-by-side comparison of local insights into the legislative framework; relevant authorities; treatment of breaches; legitimate processing; data handling responsibilities of PII owners; security obligations; internal controls, including the data protection officer; registration formalities transfer and disclosure of PII; rights of individuals; judicial supervision; specific data processing use cases such as cookies, electronic communications marketing, and cloud services; and recent trends.

Generated 29 July 2022

Table of contents

Contributors

Australia

Joshua Annese
jannese@piperalderman.com.au
Piper Alderman

Andrea Beatty
abeatty@piperalderman.com.au
Piper Alderman

Lis Boyce
lboyce@piperalderman.com.au
Piper Alderman

Andrew Rankin
arankin@piperalderman.com.au
Piper Alderman

Craig Subocz
csubocz@piperalderman.com.au
Piper Alderman

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The legislative framework in Australia is based on both federal laws and state and territory laws.

At the federal level, the collection, use, disclosure and holding of personal information by an agency or organisation to which the Australian Privacy Principles (APPs) apply, including Australian Commonwealth government agencies and most private organisations (excluding small businesses with an annual turnover of less than A$3 million unless they engage in certain activities – see below), is governed by the Privacy Act 1988 (Cth) (the Privacy Act). The Privacy Act incorporates 13 APPs and facilitates additional obligations being imposed on specific sectors by the registration of additional Privacy Codes such as the Credit Reporting Code.

Most Australian states and territories have adopted their own regimes for collecting and handling personal information and for collecting and handling health information that applies to either public sector providers only or both public sector and other health service providers. The state and territory legislative framework is summarised in the table below.

State/territory	Legislation	Applies to
New South Wales	• Privacy and Personal Information Protection Act 1998 (NSW) • The Health Records and Information Privacy Act 2002 (NSW)	Public sector agencies Public sector and other health service providers
Australian Capital Territory	• Information Privacy Act 2014 (ACT) • Health Records (Privacy and Access) Act 1997 (ACT)	Public sector agencies and contracted service providers Public sector and other health service providers
Victoria	• Privacy and Data Protection Act 2014 (Vic) • Health Records Act 2001 (Vic)	Victorian public sector and contracted service providers Public sector and other health service providers
Tasmania	• Personal Information and Protection Act 2004	Public sector agencies
South Australia and Western Australia	No specific privacy legislation	

Northern Territory	• Information Act 2002 (NT)	Public sector agencies
Queensland	• Information Privacy Act 2009 (QLD) • Invasion of Privacy Act 1971 (QLD)	Public sector agencies Any individual or entity

Law stated - 24 May 2022

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Privacy Act is administered by the Office of the Australian Information Commissioner.

The Privacy Act grants power to the Information Commissioner to investigate complaints about breaches of the Privacy Act.

As part of an investigation, the Information Commissioner has broad powers to:

- obtain information and documents;
- examine witnesses; and
- issue directions to persons to attend a compulsory conference.

The Information Commissioner also has investigative powers under other statutes, which give the Information Commissioner privacy-related functions, including the power to investigate breaches of the Privacy Safeguards in respect of the Australian Consumer Data Right regime under the Competition and Consumer Act 2010 (Cth) .

Law stated - 24 May 2022

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The Privacy Commissioner is not required to cooperate with data protection authorities overseas. The Commissioner has entered into memorandums of understanding (MOUs) with the Singaporean Personal Data Protection Commissioner, the United Kingdom Information Commissioner and the Irish Data Protection Commissioner. They outline frameworks between authorities to assist each other with the enforcement of laws protecting PI. They specifically exclude the sharing of PI.

Domestically, the Privacy Commissioner has entered into MOUs with government agencies and regulators such as the Australian Competition and Consumer Commission and the Australian Digital Health Agency to perform specific services in relation to data privacy.

Law stated - 24 May 2022

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Failing to comply with the Privacy Act may result in proceedings being brought for the imposition of a civil penalty by the Information Commissioner. Some offences under the Privacy Act may lead to criminal prosecution and penalties. The Information Commissioner may also apply for enforceable undertakings and injunctions.

Law stated - 24 May 2022

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

Complainants can:

- seek a merits review of certain decisions by the Administrative Appeals Tribunal under section 96 of the Privacy Act; and
- seek judicial review under the Administrative Decisions (Judicial Review) Act 1977 (Cth) of:
  - an Information Commissioner decision as to whether or not to investigate a complaint; or
  - following an investigation, a determination of the Information Commissioner.

Complainants may also complain to the Commonwealth Ombudsman.

Law stated - 24 May 2022

SCOPE

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Notwithstanding state and territory-based legislation covering private and public health service providers, the Privacy Act 1988 (Cth) (the Privacy Act) covers all federal government agencies, and all private organisations with an annual turnover of more than A$3 million. The Privacy Act also covers some businesses with a turnover of A$3 million or less, including:

- private sector health providers;
- businesses that purchase personal information;
- credit reporting bodies;
- contracted service providers for Australian government contracts;
- employee associations registered or recognised under the Fair Work (Registered Organisations) Act 2009;
- businesses that hold accreditation under the Consumer Data Right system;
- businesses that have opted in; and
- businesses that are related to a business covered by the Privacy Act.

Law stated - 24 May 2022

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The Privacy Act does not regulate interception of communications or monitoring and surveillance of individuals. It regulates direct marketing (including direct electronic marketing).

The Telecommunications (Interception and Access) Act 1979 (Cth) outlines the general prohibition on intercepting communications passing over telecommunications systems, with exceptions.

The Surveillance Devices Act 2004 (Cth) establishes procedures for law enforcement officers to obtain warrants, emergency authorisations and tracking device authorisations for the installation and use of surveillance devices.

The Spam Act 2003 (Cth) regulates commercial emails and SMS messages by prohibiting their transmission (except with the recipient's consent) and ensuring that any permitted emails and messages contain certain information about the sender and a functional unsubscribe facility.

The Do Not Call Register Act 2006 (Cth) prohibits making unsolicited telemarketing calls or sending unsolicited marketing faxes to numbers on the Do Not Call Register, except with the recipient's consent.

State-based Acts restrict usage of 'surveillance devices', including in the workplace.

Law stated - 24 May 2022

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

There are several additional laws protecting specific types of data, detailed below.

The My Health Records Act 2012 (Cth) specifies which entities can collect, use and disclose information in the My Health Record system. It also sets out the penalties that can be imposed for improper collection, use and disclosure of such information.

The Australian Prudential Regulation Authority (APRA) regulates authorised deposit-taking institutions in Australia. APRA has established Prudential Standard CPS 234 that requires all APRA-regulated entities to take measures to be resilient against information security incidents. In particular, authorised deposit-taking institutions must take steps to minimise the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets.

Thirteen privacy safeguards in Part IVD of the Competition and Consumer Act 2010 (Cth) apply to the handling of personal information collected through Australia's Consumer Data Right regime, largely in substitution of the Australian Privacy Principles. These safeguards set out the privacy rights and obligations for consumers, data holders and accredited data recipients through the regime, including strict requirements in relation to consent.

Law stated - 24 May 2022

PI formats

What categories and types of PI are covered by the law?

Personal information under the Privacy Act is information or an opinion about an identified individual or an individual who is reasonably identifiable, regardless of whether the information or opinion is (1) true or (2) recorded in material form.

The above definition is expansive and, as the Full Federal Court made clear in Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4, captures all information or opinions about an individual and can include digital and paper records as well as, in some cases, metadata.

Law stated - 24 May 2022

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The Privacy Act has extraterritorial effect provided that the relevant entity has an 'Australian link'. An entity has an Australian link if it 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 is formed in Australia;
- a trust created in Australia;
- a body corporate incorporated in Australia; or
- an incorporated association with its central management and control in Australia or an external Territory.

However, an organisation also has an Australian link if all of the following apply:

- the organisation is not one of the above;
- the organisation carries on business in Australia; and
- the personal information was collected or held by the organisation in Australia.

In Facebook Inc v Australian Information Commissioner [2022] FCAFC 9 (7 February 2022) the court held that it is possible for an entity to carry on business in Australia without a physical presence in Australia, and that Facebook was carrying on business in Australia by installing cookies on devices in Australia and providing Australian application developers with an interface known as the 'Graph API'.

Law stated - 24 May 2022

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

All collection, use and disclosure of PI is covered by the Privacy Act and generally no distinction is made between those who control or own PI and those who process PI on behalf of the owners. However, generally, where PI is transferred by one person to another person in circumstances where the first person retains control of the PI (eg, where PI is stored on cloud computing infrastructure hosted by another person), the information transfer may constitute a use of the PI by

the first party rather than disclosure by the first person and collection by the second person.

Law stated - 24 May 2022

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

There is no concept of 'legitimate processing' under Australian law. The Australian Privacy Principles specify that an entity may only use, hold or disclose personal information for the primary purpose for which it was collected, or for a secondary purpose if an exception applies. Exceptions include where the individual has consented or they would reasonably expect the entity to use or disclose their personal information for a secondary purpose related to the primary purpose of collection for personal information and in the case of sensitive information, directly related to the primary purpose of collection.

Entities must adopt and make publicly available a privacy policy that sets out how they collect, hold, use and disclose personal information.

Additional restrictions apply under Part IIIA of the Privacy Act in relation to the collection, use, holding and disclosure of credit information and credit reporting information by credit reporting bodies and credit providers, which may only be used and disclosed in specific circumstances. In addition to a general privacy policy, credit reporting bodies and credit providers must also have a credit reporting policy that sets out certain details about the credit information and credit reporting information they collect, hold, use and disclose.

Law stated - 24 May 2022

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

Under the Privacy Act 1988 (Cth), sensitive information is regulated more strictly than other forms of personal information. 'Sensitive Information' is any information or opinion regarding an individual's ethnic or racial origin; political opinions; professional, political or religious affiliations or memberships; sexual orientation or practices; criminal record; health; genetics; and biometrics.

Health information is also subject to additional requirements and restrictions under state and territory legislation. For instance, in New South Wales (NSW), Victoria and the Australian Capital Territory (ACT), health information must only be collected by lawful and fair means. In NSW, health information may only be used for the purpose that it was collected or a directly related purpose, and in the ACT, health information must be collected for a lawful purpose that is directly related to a function or activity of the collector, and the purpose of collection of personal health information must be made known. In Victoria, health information may only be used or disclosed for the primary purpose in which the information was collected or for a directly related and reasonably expected secondary purpose, or if an exception applies.

Law stated - 24 May 2022

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Owners of personal information must notify individuals about how they use and disclose personal information that they collect. Owners must take reasonable steps to notify individuals at or before the time of collection, or if not practicable, as soon as possible after they collect the person's personal information. The notice must contain information required by the Privacy Act 1988 (Cth) (the Privacy Act):

- the identity and contact details of the entity collecting the information;
- if the entity has collected the information from someone other than the individual or if the individual may not be aware that their personal information has been collected – the fact that the entity has collected the information and the circumstances of that collection;
- if the collection of personal information is required or authorised by law or court order – the fact that the collection is so required or authorised;
- any consequences for the individual if their personal information is not collected by the entity;
- any other entity, body or person to whom the information is usually disclosed by the entity;
- that the entity's privacy policy contains information about how the individual may access their personal information and seek correction of this information;
- that the privacy policy contains information about how the individual can complain about a breach of the Australian Privacy Principles (APPs) or a registered APP code, and how the entity will deal with this complaint; and
- whether the entity is likely to disclose the personal information to overseas recipients, and if so, the countries in which the recipients are likely to be located.

Additionally, at or before the time a credit provider collects personal information it is likely to disclose to a credit reporting body that the credit provider must notify the individual or otherwise ensure the individual is aware of the name and contact details of the credit reporting body and details required to be given to the individual under the Credit Reporting Code and ensure the notice referred to above includes additional information about the credit provider's credit reporting policy and certain rights the individual has under the Privacy Act.

Law stated - 24 May 2022

Exemptions from transparency obligations

When is notice not required?

Entities are exempt from the need to comply with the Privacy Act if they engage in certain acts or practices. Exempt entities are not required to notify individuals that their personal information has been collected. The following are exempt:

- individuals in a non-business capacity;
- organisations acting under a Commonwealth contract;
- employee records;
- journalism; and
- organisations acting under a state contract.

Additionally, political acts and practices regarding members of Parliament, contracts for political representatives and volunteers for registered political parties are not subject to the notification requirements.

Law stated - 24 May 2022

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

Entities must take reasonable steps to ensure that the PI collected is accurate, up to date and complete. Furthermore, entities must also take reasonable steps to ensure the information they use or disclose is accurate, up to date, complete and relevant.

PI will be inaccurate if it contains an error or defect, or if it is misleading. An opinion about an individual is not inaccurate by reason that the individual disagrees with the opinion.

PI is incomplete if it presents a partial or misleading picture, rather than a true or full picture.

PI is irrelevant if it does not have a bearing upon or connection to the purpose for which the personal information is used or disclosed.

Whether reasonable steps have been taken will depend on the circumstances, such as the sensitivity of the PI, the nature of the entity's business, the possible adverse consequences for the individual if the quality of the PI is not ensured and the practicability involved.

Law stated - 24 May 2022

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

Government agencies must only collect the personal information reasonably necessary for, or directly related to, one or more of their functions or activities. Private sector organisations must only collect personal information if it is necessary for one or more of their functions or activities.

An agency's functions or activities are conferred by legislation (including subordinate legislation) or an executive scheme or arrangement established by the government. The agency's activities will relate to its functions. These activities include incidental and support activities such as human resources, corporate administration, property management and public relations activities.

The organisation's functions or activities include its current functions or activities, any proposed functions or activities for which the entity has established plans, and activities carried out by the organisation in support of its other functions and activities (such as human resources, corporate administration, property management and public relations activities).

The functions and activities are usually described on a website, in an annual report, in corporate brochures, in advertising, in product disclosure statements and in client and customer letters and emails.

Sensitive information must only be collected if:

- under the first criterion:
  - the individual consents to collection of the information; and
  - if the entity is a government agency, the information is reasonably necessary for, or directly related to, one or

more of its functions or activities; or
  - if the entity is a private sector organisation, the information is reasonably necessary for one or more of its functions or activities; and
- under the second criterion;
  - the collection of the information is required or authorised by or under an Australian law or a court or tribunal order;
  - a permitted general situation (eg, lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety) exists in relation to the collection of the information by the entity;
  - the entity is an organisation and a permitted health situation (eg, collection of health information to provide a health service) exists in relation to the collection of the information by the entity;
  - the entity is an enforcement body and the entity reasonably believes that:
    - if the entity is the Immigration Department, the collection of the information is reasonably necessary for, or directly related to, one or more enforcement-related activities conducted by, or on behalf of, the entity; or
    - otherwise, the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or
  - the entity is a non-profit organisation and both of the following apply:
    - the information relates to the organisation's activities of the organisation; and
    - the information relates solely to the organisation's members, or to individuals who have regular contact with the organisation in connection with its activities.

Law stated - 24 May 2022

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

An entity that holds PI must destroy or de-identify the PI if it no longer needs the information for the purposes for which the information may be used or disclosed. The information must also not be contained in a Commonwealth record.

Entities cannot destroy or de-identify the PI if a law or a court or tribunal orders the entity to retain the information.

Law stated - 24 May 2022

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Entities may use PI for the primary purpose and any permitted secondary purposes.

The primary purpose is the purpose for which the PI was collected. The secondary purpose is any other purpose other than the primary purpose.

The entity cannot use or disclose information for secondary purposes unless:

- the individual consents to the use or disclosure of information for the secondary purpose; or
- either exception below applies.

If either exception below applies, the entity will be able to use the PI for a secondary purpose.

The first exception applies if:

- the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:
  - directly related to the primary purpose, if the information is sensitive information; or
  - related to the primary purpose, if the information is not sensitive information;
- the use or disclosure of the information is required or authorised by or under an Australian law or a court or tribunal order;
- a permitted general situation exists in relation to the use or disclosure of the information;
- the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or
- the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement-related activities conducted by, or on behalf of, an enforcement body.

The second exception applies if:

- the agency is not an enforcement body;
- the information is biometric information or biometric templates;
- the recipient is an enforcement body; and
- the disclosure is conducted in accordance with the guidelines made by the Information Commissioner.

Specific limitations apply to the use or disclosure of information for direct marketing. Sensitive information collected from an individual should only be used or disclosed for direct marketing to the individual if the individual consents to it. PI (other than sensitive information) can be used to directly market if the individual from whom the information was collected would reasonably expect the information to be used or disclosed for that purpose.

PI (other than sensitive information) can be used for direct marketing if the individual would not reasonably expect the organisation to use or disclose information for that purpose (or the information was collected from a third party), the individual has consented to the use or disclosure of PI for that purpose or it is impracticable to obtain the consent.

In both situations, the organisation must provide a simple means for the individual to opt out of receiving direct marketing communications, and the individual must not have opted out. Additionally, where the recipient would not reasonably expect PI to be used to directly market to them, but has consented to it, the organisation must draw the recipient's attention to the capacity to opt out.

Law stated - 24 May 2022

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The Privacy Act requires entities to be open and transparent about the purposes for which PI is being collected. If an entity intends to use an individual's PI for making automated decisions without human intervention that affect individuals (including profiling) then this should be noted in the privacy policy. As entities can only use information for a primary or permitted secondary purpose, it is best practice to keep policies and notices updated to ensure that individuals are aware that their PI may be used for automated decision-making purposes, including profiling, if applicable.

Law stated - 24 May 2022

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The Privacy Act 1988 (Cth) (the Privacy Act) requires entities that hold PI to take such steps as are reasonable in the circumstances to protect the information from misuse, interference, loss, and unauthorised access, modification or disclosure. An entity 'holds' personal information if it has possession or control of a record that contains the personal information or it has the right or power to deal with such a record.

Law stated - 24 May 2022

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The Privacy Act requires entities to notify the Office of the Australian Information Commissioner and affected individuals of 'eligible data breaches' as soon as practicable after confirming the breach. A breach becomes eligible where any unauthorised access to or disclosure of PI held by the entity is likely to result in serious harm to any of the individuals to whom the information relates. If the entity prevents the risk of serious harm to all affected individuals through remedial action, the breach does not need to be notified.

My Health Records

The My Health Records Act 2012 (Cth) requires entities to notify the Australian Information Commissioner of unauthorised collection, use or disclosure of health information included in a My Health Record, or of an event that has (or which may have) occurred that compromises (or which may compromise) the security or integrity of the My Health Record system. The reporting entity must contain the breach, evaluate the risks arising and arrange for the notification of all healthcare recipients should the entity conclude that the breach is likely to be serious for at least one healthcare recipient.

Prudential Standard CPS 234

Prudential Standard CPS 234 requires entities regulated by the Australian Prudential Regulation Authority (APRA) to notify APRA as soon as possible and no later than 72 hours after becoming aware of an information security incident that materially affects, or has the potential to materially affect (financially or non-financially), the entity or the interests of depositors, policyholders, beneficiaries or other customers, or has been notified to other regulators, either in Australia or other jurisdictions.

Critical infrastructure

The Security of Critical Infrastructure Act 2018 (Cth) requires an entity responsible for critical infrastructure assets to

report a cybersecurity incident that has a 'relevant impact' on the asset within 72 hours of becoming aware of the incident and within 12 hours of becoming aware of a 'significant impact'.

Law stated - 24 May 2022

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Entities must take such steps as are reasonable in the circumstances to:

- protect the PI they hold from misuse, interference and loss and from unauthorised access, modification or disclosure;
- ensure that the PI that the entity collects is accurate, up to date and complete; and
- ensure that the PI that the entity uses or discloses is, with regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

Law stated - 24 May 2022

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

There is no requirement to appoint a data protection officer.

Law stated - 24 May 2022

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

There is no general obligation to maintain internal records relating to PI held by entities. However, the Privacy Act requires entities to make a written note of the use or disclosure of PI based on the entity's reasonable belief that use or disclosure is reasonably necessary for one or more enforcement-related activities.

Credit reporting bodies and credit providers must record, in writing, the use or disclosure of credit information when the information is used in certain contexts, including where the information is used for direct marketing or if the use or disclosure is required by or under an Australian law or a court of tribunal order.

Law stated - 24 May 2022

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

There is no general obligation for non-government entities to carry out a risk assessment.

Commonwealth government agencies must complete privacy impact assessments (PIAs) for all 'high privacy risk projects' pursuant to the Privacy (Australian Government Agencies – Governance) APP Code 2017 .

A PIA must include an initial threshold assessment, a project description, a consultation with stakeholders, a mapping of the information flows, and a privacy impact analysis and compliance check. This check must include:

- the risk of privacy impacts on individuals as a result of how PI is handled;
- whether privacy impacts are necessary;
- whether there are factors that could mitigate negative privacy impacts;
- how the privacy impacts may affect the project's broad goals;
- the project's effect on an individual's choices about who has access to their personal information; and
- compliance with privacy law.

The PIA must outline recommendations to minimise identified risks. Lastly, a PIA process should involve an ongoing process of responding and reviewing changes implemented to minimise risks.

Law stated - 24 May 2022

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

There is no obligation to apply a privacy-by-design or a by-default approach when designing PI processing systems.

Law stated - 24 May 2022

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

PI owners or processors are not required to register with the Office of the Australian Information Commissioner (OAIC). However, small businesses and not-for-profit organisations that would otherwise not be captured by the Privacy Act 1988 (Cth) (the Privacy Act), may voluntarily opt in to the Privacy Act and be subject to the Privacy Act. Entities wishing to opt in must complete and submit an application with the OAIC. The Opt-in Register is publicly available on the OAIC's website.

Law stated - 24 May 2022

Other transparency duties

Are there any other public transparency duties?

Pursuant to Australian Privacy Principle (APP) 1 , entities must manage PI in an open and transparent way. Specifically, entities must have a clearly expressed and up-to-date privacy policy detailing the management of PI by the entity. The privacy policy must specify the types of information collected and held, how the entity collects and holds PI, and the purpose for which PI is collected, held, used and disclosed. The policy must disclose whether the entity will disclose PI to overseas recipients and, if so, the countries in which they are likely to be located. The entity must take reasonable steps to make its privacy policy available free of charge and in an appropriate form, such as on the entity's website.

APP 5 further requires entities to notify individuals of certain matters at or before the time, or as soon as practicable after, an entity collects PI about an individual, including information regarding the types of PI collected and the purposes for which PI is being collected.

Law stated - 24 May 2022

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The Privacy Act 1988 (Cth) (the Privacy Act) does not use the terms 'processor' or 'service providers', and also does not distinguish between a 'processor' and a 'controller'. Instead, Australian Privacy Principle (APP) 6 outlines the principle governing the use or disclosure of PI generally. APP 6 prohibits use or disclosure of PI for anything other than the primary purpose for which it was collected, unless certain exceptions apply. These exceptions include where the individual consented to the secondary purpose or would have reasonably expected the use or disclosure for the secondary purpose where the secondary purpose is related to the primary purpose.

Where the entity is disclosing the information to a processing organisation that is situated overseas, APP 8 , unless an exception applies, creates obligations on the entity to take such steps as are reasonable to ensure that the recipient does not breach the APPs (other than APP 1).

Law stated - 24 May 2022

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

There are no direct restrictions on selling personal information or sharing such information for online targeted advertising purposes. Selling and sharing PI for such purposes is controlled by APP 6. APP 6 requires entities to only use or disclose PI for the primary purpose of collection, and any additional, secondary use is only allowed under specific conditions.

Therefore, an entity intending to sell PI must take reasonable steps to notify the individual from whom the information is collected at or before the time of collection (pursuant to APP 5) that the sharing or sale of PI is the entity's primary purpose or, alternatively, be able to justify such a sale as relating to the nominated primary purpose.

The entity to whom the information is sold is likely to be subject to the APPs as a result and needs to comply with the restrictions in APP 7 regarding direct marketing.

The Privacy Act generally exempts businesses with an annual turnover of less than A$3 million from complying with the Privacy Act (including the APPs). However, where an otherwise exempt entity discloses PI about another individual to anyone else for a benefit, service or advantage or provides a benefit, service or advantage to collect PI about another individual from anyone else will make the entity subject to the Privacy Act.

Law stated - 24 May 2022

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

The Privacy Act does not regulate the 'transfer' of PI to overseas third parties as distinct from 'disclosure' of PI to overseas third parties (which is regulated). APP 8.1 provides that disclosure should only occur if the entity takes reasonable steps to ensure that the recipient does not breach the APPs (other than APP 1) in relation to the information. The Office of the Australian Information Commissioner has provided (non-binding) guidance that this generally requires the entity and the overseas recipient to enter into a contract that binds the recipient to comply with the APPs.

APP 8.2 provides that disclosure of PI to an overseas recipient is permitted where:

- the entity reasonably believes that the recipient is subject to laws that have the effect of protecting the information that is substantially equivalent to, or exceeds the protections of, the APPs (and that can be enforced by the individual);
- the individual was informed that if he or she consents, the restriction on overseas disclosure would not apply and he or she consents after being so informed; or
- a 'permitted general situation' exists.

PI is disclosed when an entity makes it accessible to third parties and releases the subsequent handling of the information from its effective control. PI is used when it is handled within the entity's effective control.

Australian organisations that send information overseas under sufficient control and in compliance with the required obligations to constitute transfer may still be held accountable for the overseas organisation mishandling the information, as the Australian organisation still 'holds' the information owing to its degree of control, even if the information is physically located overseas.

Section 16C of the Privacy Act ensures that where an APP entity discloses information to an overseas recipient but the overseas recipient is not subject to the APPs and, where the overseas entity would have breached the APPs (other than APP 1), the APP entity is considered to have undertaken the act and breached the APP instead.

Part IIIA of the Privacy Act imposes restrictions on the disclosure of credit information to overseas recipients. Additionally, state-based privacy laws restrict the transfer of PI (including health information) to recipients located outside the relevant state.

Law stated - 24 May 2022

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The Privacy Act does not distinguish between first and onward transfers of information overseas. Where information

was disclosed to a recipient pursuant to APP 8.1, the information has been disclosed on the basis that the recipient is bound to comply with the APPs in relation to the use and disclosure of the information received from the Australian entity, and the disclosing party may have contractual grounds to enforce such compliance (depending on the terms on which the information was disclosed to the recipient). However, if information has been disclosed to an overseas recipient on the basis of APP 8.2, the Privacy Act would not apply to any onward transfer or disclosure of the information.

Section 16C of the Privacy Act covers the scenario where a disclosure to an overseas entity will not make the overseas entity subject to the APPs under the Privacy Act. In such a scenario, the entity that disclosed the information and is subject to the APPs will be held responsible for any actions of the overseas entity that would have been a breach of the APPs had they applied to the overseas entity.

Law stated - 24 May 2022

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There is no general requirement for a copy of PI to be retained in Australia when the PI is transferred overseas.

State laws relating to health records commonly include retention obligations. Where the laws allow the transfer of the health data outside their jurisdiction, such as interstate transfer, there is often a requirement for the record (or information about to whom it was transferred) to be maintained by the original health service provider.

Law stated - 24 May 2022

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

If an agency or organisation to which the Australian Privacy Principles (APPs) apply holds personal information about an individual, the entity must, on request of the individual, give the individual access to the information. If the entity is an 'agency' (which primarily refers to federal government entities), the agency must respond to a request for personal information within 30 days. If the entity is an 'organisation' (which is defined to include an individual, body corporate, partnership, unincorporated associate or trust), the organisation must respond within a reasonable period after the request is made. While an agency is precluded from charging an individual for requesting or giving access to personal information, organisations may charge individuals for giving access to personal information provided it is not excessive.

If an agency is precluded from disclosing personal information under the Freedom of Information Act or any other Act of the Commonwealth or a Norfolk Island enactment, the agency is not required to comply with a request for information. Notably, an organisation is not required to give an individual access to personal information in a broad number of circumstances including where the request for access is frivolous or vexatious or the organisation reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety.

Law stated - 24 May 2022

Other rights

Do individuals have other substantive rights?

The Privacy Act 1988 (Cth) (the Privacy Act) provides individuals with a number of protections, including the right to:

- know why personal information is being collected, how it will be used and who it will be disclosed to;
- have the option of using a pseudonym in certain circumstances;
- stop receiving direct marketing;
- have personal information kept accurate, up to date and complete;
- ask for access to personal information (including health information);
- ask for personal information that is incorrect to be corrected; and
- make a complaint to the Office of the Australian Information Commissioner (OAIC) or the relevant external dispute resolution body about an APP entity if it has mishandled personal information.

Law stated - 24 May 2022

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The Privacy Act makes accommodations for an individual affected by a privacy breach through the dispensation of compensation from the organisation involved in the breach. Where a breach is shown to have occurred, the OAIC may make an order for compensation under section 52 of the Privacy Act. Pursuant to subsection 52(1)(a) or subsection 52(1)(b)(iii), the OAIC may make a declaration that 'the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint'. While there is no monetary ceiling, it is usual that these orders do not exceed the low thousands in Australian dollars. Alternatively, the OAIC may seek orders including injunctions and orders to give a public apology.

Law stated - 24 May 2022

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

At present, an individual has no exercisable right to make a claim directly against an APP entity for a breach of the Privacy Act. Where an individual has a complaint, their complaint must pass through the OAIC, which may then commence action against the APP entity. The OAIC is empowered with enforcement mechanisms to ensure individuals have access to quick and effective remedies for the protection of their privacy rights. The Privacy Act confers a range of privacy powers on the OAIC to work with entities to facilitate legal compliance and best practice, as well as investigative and enforcement powers to use in cases where a privacy breach has occurred.

Law stated - 24 May 2022

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

There is a myriad of exemptions for various entities and their handling of personal information. For example, pursuant to subsection 7B(3) of the Privacy Act 1988 (Cth), a private sector employer's handling of employee records in relation to current and former employment relationships is exempt from the Australian Privacy Principles if the organisation's actions or practices directly relate to:

- a current or former employment relationship between the employer and the individual; or
- an employee record held by the organisation relating to the individual.

Similar exemptions apply to small businesses, registered political parties, political acts and practices, and journalism.

Law stated - 24 May 2022

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

The Privacy Act 1988 (Cth) (the Privacy Act) does not specifically regulate the use of cookies or equivalent technology. However, as cookies and equivalent technology can be used to collect PI, entities must comply with the Australian Privacy Principles (APPs) in relation to the use of cookies (including the disclosure of the use of cookies in privacy policies).

Law stated - 24 May 2022

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

The Privacy Act prohibits APP entities from using or disclosing personal information for the purposes of direct marketing unless certain exemptions apply. In particular, an APP entity can use or disclose PI for the purpose of direct marketing where the PI was collected from the individual and the individual would reasonably expect this use purpose. Direct marketing is further allowed, where it was not reasonable to expect that the organisation would use the information for direct marketing, but the person gave consent for this use, or obtaining consent was impracticable. This exception applies whether the information was collected from the individual or from a third party. Both exceptions require an easy opt-out mechanism but differ in the degree in which notice of the mechanism must be provided to the individual.

The Spam Act 2003 (Cth) forbids unsolicited commercial electronic messages being sent and requires electronic messages to include an unsubscribe option and information about the individual or the organisation authorising the sending.

The Do Not Call Register Act 2006 (Cth) prohibits businesses from making unsolicited phone calls (eg, telemarketing)

or sending unsolicited facsimiles to individuals who have registered their telephone numbers (including mobile phone numbers) or facsimile numbers on the Do Not Call Register, unless specific exceptions apply.

Law stated - 24 May 2022

Targeted advertising

Are there any rules on targeted online advertising?

There are no rules specifically regulating the display of targeted or personalised advertising. Where the information used to target the advertising contains personal information, the entity collecting, holding or disclosing the information will be subject to the Privacy Act (including the APPs).

Law stated - 24 May 2022

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

'Sensitive information' is any information or opinion regarding an individual's ethnic or racial origin; political opinions; professional, political or religious affiliations or memberships; sexual orientation or practices; criminal record; health; genetics; and biometrics. This information is under stricter regulation than other forms of personal information under the Privacy Act. Sensitive information may only be collected with consent, except in specified circumstances. Further, sensitive information:

- must not be used or disclosed for a secondary purpose unless the secondary purpose (being within the reasonable expectations of the individual) directly relates to the primary purpose;
- cannot be used for the purposes of direct marketing; and
- cannot be shared between related bodies corporate outside the normal consent and disclosure rules.

Law stated - 24 May 2022

Profiling

Are there any rules regarding individual profiling?

There are no specific rules regarding individual profiling. The Privacy Act does not require that an individual is specifically informed of a service using automated processing and profiling, except to the extent that an APP entity is required to disclose the purposes for which PI may be collected as part of general compliance obligations. The Privacy Act does not provide individuals with the right not to be subject to decisions based solely on automated processing, including profiling.

However, the requirements of the Privacy Act may still apply. In particular, APP 6 will protect a user by possibly requiring them to consent where the automated processing and profiling would be part of a purpose that constitutes the secondary rather than primary purpose of collection.

Law stated - 24 May 2022

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

The Office of the Australian Information Commissioner provides guidance explaining that organisations using and sending data to cloud service providers located overseas, under specific conditions, will be considered a 'use' of PI and not a 'disclosure' and will, therefore, be exempt from APP 8.

These conditions include the information being provided for the limited purpose of storing and access by the entity, in addition to creating contractual obligations on the provider that they and any subcontractor may only handle the personal information for these limited purposes. The effective control over how the personal information is handled by the provider must remain with the organisation.

While this use will mean that section 16 and APP 8.1 relating to disclosure will not apply, the cloud service provider will be considered to be 'holding' PI and must comply with APPs 6, 11, 12 and 13.

Law stated - 24 May 2022

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Over the past year, personal information law has undergone rapid change as advancing technology, social media and cultural values have shifted how industries and individuals perceive their privacy obligations.

In October 2021, the Office of the Australian Information Commissioner released a discussion paper seeking feedback for the ongoing review of the Privacy Act 1988 (Cth) (the Privacy Act) (the Review). In its response to the Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry report, the Morrison government committed to undertake a review of the Privacy Act. The Review was commenced on 12 December 2019 and considers whether the scope of the Privacy Act and its enforcement mechanisms remain fit for purpose. A discussion paper was released in October 2021 and covers a broad range of topics, including:

- the scope and application of the Privacy Act;
- the protections contained in the Australian Privacy Principles (APPs); and
- how the Act is regulated and enforced.

Notably, the discussion paper proposes to introduce a statutory tort for invasions of privacy and create a direct right of action for individuals or groups of individuals whose privacy has been interfered with by an APP entity. Submissions on the discussion paper closed on 10 January 2022, and these contributions will inform the review's final report.

Personal information will continue to adapt and change, as will the policies that regulate it. These aforementioned reforms represent a larger shift towards greater protection of privacy and personal information in Australia in 2022.

* The authors would like to extend special thanks to Jack Dean, Shannon Hatheier, Jan David Hohmann, Francesca Lombardo and Tom Murdoch for their contributions to the chapter.

Law stated - 24 May 2022

Jurisdictions

Australia	Piper Alderman
Austria	Knyrim Trieb Rechtsanwälte
Belgium	Hunton Andrews Kurth LLP
Brazil	Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados
Canada	Thompson Dorfman Sweatman LLP
Chile	Magliona Abogados
China	Mayer Brown
France	Aramis Law Firm
Germany	Hoffmann Liebs Fritsch & Partner
Greece	GKP Law Firm
Hong Kong	Mayer Brown
Hungary	VJT & Partners
India	AP & Partners
Indonesia	SSEK Legal Consultants
Ireland	Walkers
Italy	ICT Legal Consulting
Japan	Nagashima Ohno & Tsunematsu
Jordan	Nsair & Partners - Lawyers
Malaysia	SKRINE
Malta	Fenech & Fenech Advocates
Mexico	OLIVARES
New Zealand	Anderson Lloyd
Pakistan	S.U.Khan Associates Corporate & Legal Consultants
Poland	Kobylanska Lewoszewski Mednis
Portugal	Morais Leitão, Galvão Teles, Soares da Silva & Associados

Singapore	Drew & Napier LLC
South Korea	Bae, Kim & Lee LLC
Switzerland	Lenz & Staehelin
Taiwan	Formosa Transnational Attorneys at Law
Thailand	Formichella & Sritawat Attorneys at Law
Turkey	Turunç
United Arab Emirates	Bizilance Legal Consultants
United Kingdom	Hunton Andrews Kurth LLP
USA	Hunton Andrews Kurth LLP