DATA PROTECTION LAWS OF THE WORLD

Australia

AUSTRALIA

Last modified 31 December 2023

LAW

Australia regulates data privacy and protection through a mix of federal, state and territory laws. The federal Privacy Act 1988 (*Cth*) ("**Privacy Act**") and the Australian Privacy Principles ("**APPs**") contained in the Privacy Act apply to private sector entities (including body corporates, partnerships, trusts and unincorporated associations) with an annual turnover of at least AU$3 million, and all Commonwealth Government and Australian Capital Territory Government agencies.

The Privacy Act regulates the handling of personal information by relevant entities and under the Privacy Act, the Information Commissioner has authority to conduct investigations, including own motion investigations, to enforce the Privacy Act and seek civil penalties for serious and egregious breaches or for repeated breaches of the APPs where an entity has failed to implement remedial efforts.

The Privacy Act is currently undergoing a review and the Attorney General’s Department released the Privacy Act Review Report 2022 setting out 116 proposed amendments to the Privacy Act. The Government Response to the Privacy Act Review Report released in 2023 indicated that of the 116 recommendations, the Australian Government “agreed” to 38 of them, “agreed in principle” to another 68 and rejected 10. The timing for the implementation of these changes is not yet clear, however, it is likely that this will be undertaken during 2024 – 2025 and that any revisions will result in more prescriptive and onerous requirements being imposed on organisations handling personal information of Australian residents.

In late 2023, appointments were made of a separate Privacy Commissioner and Freedom of Information Commissioner - these roles were all performed by the Information Commissioner. The Privacy Commissioner will perform the privacy functions which relate to the privacy of individuals with both new appointments beginning in February 2024.

Most States and Territories in Australia (except Western Australia and South Australia) have their own data protection legislation applicable to relevant State or Territory government agencies, and private businesses that interact with State and Territory government agencies. These Acts include:

- *Information Privacy Act 2014* (Australian Capital Territory)
- *Information Act 2002* (Northern Territory)
- *Privacy and Personal Information Protection Act 1998* (New South Wales)
- *Information Privacy Act 2009* (Queensland)
- *Personal Information Protection Act 2004* (Tasmania), and
- *Privacy and Data Protection Act 2014* (Victoria)

Additionally, there are other parts of State, Territory and federal legislation that relate to data protection. For example, the following all impact privacy and data protection for specific types of data or activities: the *Telecommunications Act 1997* (*Cth*), the *Criminal Code Act 1995* (*Cth*), the *National Health Act 1953* (*Cth*), the *Health Records and Information Privacy Act 2002* (NSW), the *Health Records Act 2001* (Vic) and the *Workplace Surveillance Act 2005* (NSW).

Specific regulators have also expressed an expectation that regulated entities should have specified data protection practices in place. For example, the Australian Prudential and Regulatory Authority ("**APRA**"), which regulates financial services institutions requires regulated entities to comply with Prudential Standards, including Prudential Standard CPS 234 Information Security ("**CPS 234**"), and the Australian Securities and Investment Commission regulates corporations more generally.

Other important privacy and data protection laws

Assistance and Access Act

The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)* ("**AA Act**") provides law enforcement agencies with access to encrypted data for serious crime investigation and imposes obligations on "Designated Communications Providers". However, the AA Act may inadvertently have a much broader remit with limited judicial oversight, and has been the subject of much criticism from local and global technology firms which have stated the legislation has the potential to significantly impact security / encryption solutions in Australia.

The AA Act allows various agencies to do any of the following:

- Issue a "technical assistance notice", which requires a communications provider to give assistance that is reasonable, proportionate, practicable and technically feasible;
- Issue a "technical capability notice", which requires a communications provider to build new capabilities to assist the agency. The Attorney-General must consult with the communications provider prior to issuing the notice, and must be satisfied that the notice is reasonable, proportionate, practicable and technically feasible; and
- Make "technical assistance requests", to give foreign and domestic communications providers and device manufacturers a legal basis to provide voluntary assistance to various Australian intelligence organizations and interception agencies relating to issues of national interest, national security and law enforcement.

Organizations will need to ensure customer terms and conditions deal carefully with the matter of legal compliance and any commitments made to customers generally.

Security of Critical Infrastructure Act

The *Security of Critical Infrastructure Act 2018 (Cth)* ("**SOCI Act**") 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.

The key obligations under the SOCI Act include:

- Organisations must provide “operational” and ownership information to the Cyber Infrastructure Security Centre for inclusion on the Register of Critical Infrastructure Assets, in accordance with the requirements in Part 2 of the SOCI Act;
- Organisations must notify the Australian Signals Directorate ("**ASD**") of actual or imminent cyber security incidents with an actual or likely relevant impact within 72 hours of the organisation becoming aware, in accordance with the requirements set out in Part 2B of the SOCI Act; and
- Organisations must implement and comply with a "risk management program", in accordance with the requirements in Part 2A of the SOCI Act and the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023.

Generally, organisations to whom the SOCI Act applies or those that provide services to relevant organisations should ensure that any terms and conditions deal with compliance with the obligations under the SOCI Act.

Consumer Data Right

The Commonwealth Government is in the implementation phases of the Consumer Data Right (“**CDR**”) following a number of policy reviews including the Productivity Commission's "Data Availability and Use" report and the "Review into Open Banking in Australia".

The CDR allows a consumer to obtain certain data held about that consumer by a third party and require data to be given to accredited third parties for certain purposes. By requiring businesses to provide public access to information on specified products they have on offer, it is intended that consumers' ability to compare and switch between products and services will be improved, as well as encouraging competition between service providers, which could lead to better prices for customers and more innovative products and services. In this way, the CDR provides a mechanism for accessing a broader range of information within designated sectors than is provided for by APP 12 in the Privacy Act, given it applies not only to data about individual consumers but also to business consumers and related products.

The CDR rules have been implemented in respect of the banking and energy sector in Australia. The non-bank lending sector is the next to be added to the CDR. Other sectors across the economy will be added to the CDR over time.

The CDR regime addresses competition, consumer, privacy and confidentiality issues. As such, it is regulated by the Australian Competition and Consumer Commission as well as the OAIC.

DEFINITIONS

Definition of personal data

Personal data (referred to as "personal information" in Australia) means 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 material form or not.

The Privacy Act currently contains an exemption for “employee records”, such that any records containing personal information which an employer makes in connection with a current or former employment relationship are exempt from the Privacy Act. However there are some further carve outs to this (for example, the exemption does not apply to contractors or unsuccessful applicants), and it is widely anticipated that the employee records exemption will be removed from the Privacy Act as a result of the ongoing review of the Privacy Act (see Enforcement).

Definition of sensitive personal data

Sensitive personal data (referred to as "sensitive information" in Australia) means information or an opinion about:

- 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;
- Criminal record that is also personal information;
- 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 identification or verification; and / or
- Biometric templates.

NATIONAL DATA PROTECTION AUTHORITY

The Information Commissioner, under the Office of the Australian Information Commissioner ("**OAIC**") is the national data protection regulator responsible for Privacy Act oversight.

175 Pitt Street
Sydney NSW 2000

T 1300 363 992

F +61 2 9284 9666

REGISTRATION

There is no registration requirement in Australia for data controllers or data processing activities. Under the Privacy Act, organizations are not required to notify the Information Commissioner of any processing of personal information.

DATA PROTECTION OFFICERS

Organizations are not required to appoint a data protection officer. However, the Information Commissioner has issued guidance recommending that organizations appoint a data protection officer as good practice.

COLLECTION & PROCESSING

Organizations may not collect personal information unless the information is reasonably necessary for one or more of its business functions or activities.

Under the Privacy Act, organizations must take reasonable steps to ensure that personal information collected is accurate and up-to-date.

At or before the time organizations collect personal information, or as soon as practicable afterwards, they must take reasonable steps to provide individuals with notice of:

- The Organization’s identity and contact information;
- Why it is collecting (or how it will use the) information about the individual;
- The entities or types of entities to which it might give the personal information;
- Any law requiring the collection of personal information;
- The main consequences (if any) for the individual if all or part of the information is not provided;
- The fact that the organization’s privacy policy contains information about how the individual may access and seek correction of their personal information, how they may make a complaint about a breach of the APPs and how the organization will deal with such complaint; and
- Whether the organization is likely to disclose their personal information to overseas recipients and, if so, the countries in which such recipients are likely to be located.

Organizations should comply with these notification requirements by preparing a “collection statement” or “privacy notice” for each significant collection of personal information, and providing this to individuals prior to collecting their personal information.

This notification requirement applies in addition to the requirement for organisations to maintain a broader privacy policy, which details the general personal information handling processes of the organisation. APP 1 lists the information which is required to be included in a privacy policy.

In practice, a major Privacy Act compliance issue often arises because organizations fail to recognize that the mandatory notice requirements outlined above also apply to any personal information collected from a third party. Organizations must provide individuals with required notice on receipt of personal information from a third party, even though they did not collect personal information directly from the individual. Unlike Europe, Australian privacy law does not distinguish between "data processors" and "data controllers".

Organizations must not use or disclose personal information about an individual unless one or more of the following applies:

- The personal information was collected for that purpose (the primary purpose) or a different (secondary) purpose which is related to (and, in the case of sensitive information, directly related to) the primary purpose of collection and the individual would reasonably expect the organization to use or disclose the information for that secondary purpose.
- The individual consents.
- The information is not sensitive information and disclosure is for direct marketing and it is impracticable to seek the individual’s consent and (among other things) the individual is told that they can opt out of receiving marketing from the organization.
- A "permitted general situation" or "permitted health situation" exists; for example, the entity has reason to suspect that unlawful activity relating to the entity's functions has been engaged in, or there is a serious threat to the health and safety of an individual or the public.
- It is required or authorized by law or on behalf of an enforcement agency.

In the case of use and disclosure for the purpose of direct marketing, organizations are required to ensure that:

- Each direct marketing communication provides a simple means by which the individual can opt out
- The individual has not previously requested to opt out of receiving direct marketing communications

The above direct marketing requirements apply to all forms of direct marketing. Additionally, specific requirements for commercial electronic messaging are outlined in Electronic Marketing.

The Privacy Act affords additional protections when processing involves sensitive information. Organizations are prohibited from collecting sensitive information from an individual unless certain limited requirements are met, including one or more of the following:

- The individual has consented to the collection and the collection of the sensitive information is reasonably necessary for one or more of the entity's functions or activities.
- Collection is required or authorized by law or a court / tribunal order.
- A "permitted general situation" or "permitted health situation" exists; for example, the entity has reason to suspect that unlawful activity relating to the entity's functions has been engaged in, or there is a serious threat to the health and safety of an individual or the public.
- The entity is an enforcement body and the collection is reasonably necessary for that entity's functions or activities.
- The entity is a nonprofit organization and the information relates to the activities of the organization and solely to the members of the organization (or to individuals who have regular contact with the organization relating to its activities).

Organizations must provide individuals with access to their personal information held by the organization upon an individual’s request. Additionally, individuals have a right to correct inaccurate, out-of-date, and irrelevant personal information held by an organization. Under certain circumstances, the organization may limit the extent to which it provides an

individual with access or correction rights, including in emergency situations, specified business imperatives, and law enforcement or other public interests.

Further, organizations must provide individuals with the option to not identify themselves, or use a pseudonym, when dealing with the organization, unless it is impractical to do so or the organization is required or authorized by law to deal with identified individuals.

TRANSFER

Unless certain limited exemptions under the Privacy Act apply, personal information may only be disclosed to an organization outside of Australia where the entity has taken reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the personal information. The disclosing / transferring entity will generally remain liable for any act(s) done or omissions by that overseas recipient that would, if done by the disclosing organization in Australia, constitute a breach of the APPs. However, this provision will not apply where any of the following apply:

- The organization reasonably believes that the recipient of the information is subject to a law or binding scheme which effectively provides for a level of protection that is at least substantially similar to the Privacy Act, including as to access to mechanisms by the individual to take action to enforce the protections of that law or binding scheme. There can be no reliance on contractual provisions requiring the overseas entity to comply with the APPs to avoid ongoing liability (although the use of appropriate contractual provisions is a step towards ensuring compliance with the 'reasonable steps' requirement).
- The individual consents to the transfer. However, under the Privacy Act the organization must, prior to receiving consent, expressly inform the individual that if he or she consents to the overseas disclosure of the information the organization will not be required to take reasonable steps to ensure the overseas recipient does not breach the APPs.
- A "permitted general situation" applies.
- The disclosure is required or authorized by law or a court / tribunal order.

SECURITY

An organization must have appropriate security measures in place (i.e. take reasonable steps) to protect any personal information it retains from misuse and loss and from unauthorized access, modification or disclosure. The Information Commissioner has issued detailed guidance on what it considers to be reasonable steps in the context of security of personal information, which we recommend be reviewed and implemented. Depending on the organization, and how and by which government agency it is regulated, as noted above specific requirements or expectations may also exist and with which organizations should be familiar. An organization must also take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for the purpose(s) for which it was collected.

BREACH NOTIFICATION

Entities with obligations to comply with the Privacy Act must comply with the mandatory data breach notification regime under the Privacy Act.

The mandatory data breach notification includes data breaches that relate to:

- Personal information
- Credit reporting information
- Credit eligibility information
- Tax file numbers

In summary, the regime requires organizations to notify the OAIC and affected individuals of "eligible data breaches" (in accordance with the required contents of a notice). Where it is not practicable to notify the affected individuals individually, an organization that has suffered an eligible data breach must make a public statement on its website containing certain information as required under the Privacy Act, and take reasonable steps to publicise the contents of the statement.

An "eligible data breach" occurs when the following conditions are satisfied in relation to personal information, credit reporting information, credit eligibility information or tax file information:

All of the following conditions are satisfied:

- There is unauthorized access to, or unauthorized disclosure of, or loss of the information;
- A reasonable person would conclude that the access or disclosure, or loss would be likely to result in serious harm to any of the individuals to which the information relates; and
- Prevention of the risk of serious harm through remedial action has not been successful.

While "serious" harm is not defined in the legislation, the OAIC has released guidance on how serious harm may be interpreted and assessed by organizations. There are a number of key criteria to examine when determining if "serious" harm is likely to result from a breach which should be assessed holistically and take into account: the kinds of information, sensitivity, security measures protecting the information, the nature of the harm (i.e. physical, psychological, emotional, financial or reputational harm) and the kind(s) of person(s) who may obtain the information.

The regime also imposes obligations on organizations to assess within 30 calendar days whether an eligible data breach has occurred where the organization suspects (on reasonable grounds) that an eligible data breach has occurred, but that suspicion does not amount to reasonable grounds to believe that an eligible data breach has occurred.

There are various exceptions to the requirement to notify affected individuals and / or the OAIC of a data breach notification including in instances where law enforcement related activities are being carried out or where there is a written declaration by the Information Commissioner.

The introduction of the regime has resulted in many organizations requiring detailed contractual obligations with third party suppliers in relation to cybersecurity and the protection of personal information of their customers / clients. Complimenting this regime, the OAIC has also released several guidance notes relating to the regime which include topics such as the security of personal information and whilst these are not legally binding, they are considered industry best practice.

Further, organizations may have additional obligations to notify other regulators of data breaches in certain circumstances including under the Prudential Standard CPS 234 Information Security ("**CPS 234**") which aims to strengthen APRA-regulated entities' resilience against information security incidents (including cyberattacks), and their ability to respond swiftly and effectively in the event of a breach. CPS 234 applies to all APRA-regulated entities who among other things, are required to notify APRA within 72 hours "after becoming aware" of an information security incident and no later than 10 business days after "it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner".

ENFORCEMENT

The Information Commissioner is responsible for the enforcement of the Privacy Act and will investigate an act or practice if the act or practice may be an interference with the privacy of an individual and a complaint about the act or practice has been made. Generally, the Information Commissioner prefers mediated outcomes between the complainant and the relevant organization. Importantly, where the Information Commissioner undertakes an investigation of a complaint which is not settled, it is required to ensure that the results of that investigation are publicly available. Currently, this is undertaken by disclosure through the OAIC website of the entire investigation report.

The Information Commissioner may also investigate any "interferences with the privacy of an individual" (i.e. any breaches of the APPs) on its own initiative (i.e. where no complaint has been made) and the same remedies as below are available. With a number of large scale, high profile data breaches occurring in Australia recently, the Information Commissioner appears to be adopting a more proactive and more publicised approach to investigation and enforcement action, and it seems likely that the review and likely revision of the Privacy Act will strengthen the Information Commissioner's powers with respect to investigation and enforcement.

After investigating a complaint, the Information Commissioner may dismiss the complaint or find the complaint substantiated and make declarations that the organization rectify its conduct or that the organization redress any loss or damage suffered by the complainant (which can include non-pecuniary loss such as awards for stress and / or humiliation). The maximum penalties that may be sought by the Information Commissioner and imposed by the Courts for serious or repeated interferences with the privacy of individuals were increased significantly to the greater of (i) AUD50M, (ii) three times the benefit of a contravention, or (iii) (where the benefit cannot be determined) 30% of domestic turnover.

ELECTRONIC MARKETING

The sending of electronic marketing (referred to as "commercial electronic messages" in Australia) is regulated under the Spam Act 2003 (*Cth*) (“**Spam Act**”) and enforced by the Australian Communications and Media Authority.

Under the Spam Act, a commercial electronic message (which includes emails and SMS's sent for marketing purposes) must not be sent without the prior opt-in consent of the recipient.

In addition, each electronic message (which the recipient has consented to receive) must identify the sender and contain a functional unsubscribe facility to enable the recipient to opt out of receiving future electronic marketing. Requests to unsubscribe must be processed within 5 business days.

A failure to comply with the Spam Act (including unsubscribing a recipient that uses the unsubscribe facility) may have costly consequences, with repeat offenders facing penalties of up to AU$2.2 million per day.

ONLINE PRIVACY

There are no laws or regulations in Australia specifically relating to online privacy, beyond the application of the Privacy Act, the Spam Act and State and Territory privacy laws relating to online / e-privacy, and other specific laws regarding the collection of location and traffic data. Specifically, the are no specific legal requirements regarding the use of cookies (or any similar technologies). If the cookies or other similar technologies collect personal information of a user the organization must comply with the Privacy Act in respect of collection, use, disclosure and storage of such personal information. App developers must also ensure that the collection of customers' personal information complies with the Privacy Act and the Information Commissioner has released detailed guidance on this.

KEY CONTACTS

Nicholas Boyle
Partner
T +61 2 9286 8479
nicholas.boyle@dlapiper.com

Sarah Birkett
Special Counsel
DLA Piper Australia
T +61 3 9274 5464
sarah.birkett@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.