Data. Protection. Adding Value.

Data Protection Laws - Australia

Legislation

The key legislative instrument in Australia which regulates data privacy and protection is the federal Privacy Act 1988 (Cth) ("**Privacy Act**") which includes the Australian Privacy Principles ("**APPs**"). Several Australian states and territories also have their own privacy legislation which oversees the information handling practices of public sector agencies and certain organisations that handle health information.

Scope: The Privacy Act (including the APPs) applies to "APP Entities" which broadly are Australian federal government agencies and private sector organisations incorporated in Australia with an annual turnover of more than AUD $3 million. A foreign corporation or body will be also regulated under the Privacy Act where the organisation carries on business in Australia.

Exemptions: Small businesses (i.e. with an annual turnover of AUD $3 million or less) are exempt from the requirements of the Privacy Act. The handling of employee records by private sector organisations is also excluded from the Privacy Act although this exemption has been narrowly applied.

Risk Level: High

Enforcement

Powers: The OAIC has the power to investigate organisations, request information regarding compliance where there has been a data breach, accept enforceable undertakings, make determinations, issue infringement notices, share information with other enforcement bodies, publish information, and apply for injunctions or civil penalties.

Fines: Civil penalties for "serious or repeated interference with privacy" may be up to:

- AUD $2.5 million for individuals; or
- For corporations, the greater of: (i) AUD 50 million, (ii) 3 times the value of the benefits obtained, if it is quantifiable; or (iii) where the benefit cannot be determined, 30% of the corporations 'adjusted turnover' during the 'breach turnover period'.

Data Processing

Legal Basis for Processing: APP 6 provides that an APP Entity may only use or disclose personal information for the primary purpose for which it was collected however there are certain exceptions to this general rule. Specifically, an APP Entity may also use or disclose personal information in the following circumstances:

i. where the use or disclosure is for another secondary purpose which is related to the primary purpose for collection (or directly related, in the case of sensitive information), and the individual would reasonably expect the entity to use or disclose the information for that secondary purpose;
ii. the relevant individual has consented to the use or disclosure;
iii. where the use or disclosure is for direct marketing, provided the personal information is not sensitive information and the APP Entity satisfies certain conditions, including enabling the individual to opt-out of receiving direct marketing;
iv. there is a 'permitted general situation' or 'permitted health situation' (e.g. unlawful activity or a serious threat to the life, health, safety of an individual); or
v. where the use or disclosure is required or authorised by law or on behalf of an enforcement agency.

Sensitive information: Sensitive information must be handled with a higher standard than personal information and may only be collected where reasonably necessary for the functions or activities of an organisation or agency (APP 3). Sensitive information is personal information that includes information or an opinion about an individual's race, religion, sexual orientation, health or genetic information, criminal record or political opinions.

Supervisory Authority

The Office of the Australian Information Commissioner ("**OAIC**") is the key independent national regulator responsible for overseeing compliance with the Privacy Act and protecting individuals' rights to access public information under Australia's Freedom of Information laws.

Data related matters may fall under the purview of other regulators such as the Australian Competition and Consumer Commission, Australian Tax Office, Australian Communications and Media Authority, Australian Prudential Regulation Authority, Australian Securities and Investments Commission and state or territory authorities.

Registration/Approval Requirements: There is no registration requirement for APP Entities in respect of the handling of personal information.

Australian Privacy Principles

An APP Entity that collect, use or disclose 'personal information' must comply with the APPs. These include:

- **Transparency:** APP entities must manage personal information in an open and transparent manner, including having an up to date privacy policy (APP 1);
- **Purpose limitation**: APP 6 provides that an APP entity that holds personal information about an individual can only use or disclose the information for a particular purpose for which it was collected (known as the 'primary purpose' of collection), unless an exception applies. The exceptions include: (i) where the use or disclosure is for another secondary purpose which is related to the primary purpose for collection (or directly related, in the case of sensitive information), and the individual would reasonably expect the entity to use or disclose the information for that secondary purpose; and (ii) the relevant individual has consented to the use or disclosure.
- **Accuracy:** An APP entity must take reasonable steps to ensure that the personal information it collects is accurate, up to date and complete (APP 10);
- **Security:** 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 (APP 11);
- **Access:** An APP entity must grant individuals the right to access their personal information that is in the possession of the APP entity (APP 12); and
- **Correction:** An APP entity must take reasonable steps to correct personal information it holds about individuals (APP 13).

pwc

Transparency Requirements

APP 1 ensures that APP Entities manage personal information in an open and transparent way, requiring an entity to have a clearly expressed in their privacy policy details of the kind of personal information held and collected, for what purposes, rights to access, avenues for complaint and extent of disclosure to third parties/overseas recipients. An APP Entity that collects personal information about an individual must also take reasonable steps to notify the individual, or otherwise ensure the individual is aware, of certain matters listed in APP 5.2 (which include the APP Entity's details and the purposes of collection).

Individual Rights

Individuals have the following rights under the Privacy Act in relation to an APP Entity's processing of their personal information:

1. **Right to access:** individuals may request an APP Entity to provide access to personal information about them held by the APP Entity.
2. **Right to correction:** individuals may request an APP Entity to correct any personal information about them held by the APP Entity that is inaccurate, out-of-date, incomplete, or misleading.
3. **Right to deletion/be forgotten:** there is no specific 'right to erasure' but an APP Entity must take reasonable steps to destroy or de-identify the personal information if it is no longer needed for any purpose permitted under the Privacy Act.
4. **Right to opt out of direct marketing:** individuals have a right to opt out of use or disclosure of personal information from being used for marketing purposes without their consent.
5. **Right to anonymity:** individuals must be provided with the option of not identifying themselves, or of using a pseudonym, when dealing with an APP Entity.

Security & Data Breaches

Security Requirements: APP 11 requires an APP Entity to take such steps as are reasonable in the circumstances to protect personal information that the APP Entity holds from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Data Breaches: The Notifiable Data Breach (**NDB**) scheme in Part IIIC of the Privacy Act applies to APP Entities that have an obligation under APP 11 to protect personal information they hold. The NDB requires regulated APP Entities to notify impacted individuals and the OAIC if an 'eligible data breach' occurs (i.e. when personal information is accessed, disclosed or lost without authorisation and a reasonable person would conclude that this is likely to result in serious harm to any of the individuals to whom the personal information relates). However, if remedial action effectively prevents serious harm there will not be an 'eligible data breach' for the purposes of the Privacy Act, and notification will not be required.

Notification to individuals and supervisory authorities: The NDB scheme requires entities to notify affected individuals and the OAIC where they have reasonable grounds to believe there has been an 'eligible data breach and complete an assessment within 30 days.

Other Business Obligations

Data Protection Officer: The Privacy Act does not specifically require an APP Entity to appoint a data protection officer. However, the in its guidance, the OAIC recommends APP Entities should consider implementing governance mechanisms to ensure compliance with the APPs (including the appointment of a designated privacy officer).

Privacy Risk Assessment: While conducting a privacy impact assessment' is not an explicit requirement under the Privacy Act, it is a tool that can assist APP Entities in complying with their obligations under the Privacy Act. Specifically, a PIA can help an entity to ensure that it manages personal information in an open and transparent way (APP 1), identifies and mitigates risks to privacy (APP 1.2), and only collects personal information that is necessary for its functions or activities (APP 3).

APP 1.2 requires an APP entity to take reasonable steps 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 any binding registered APP code relevant to its activities. The OAIC's guidance recommends that the practices, procedures and systems that an APP Entity should consider implementing include regular staff training and information bulletins on how the APPs apply to the entity

Service Providers & Cross-Border Transfers

Cross-border data transfers: APP 8 requires that before an organisation discloses personal information to an overseas recipient, it must take "reasonable steps" to ensure that the overseas recipient will be able to handle this data in accordance with the APPs (other than APP 1). Alternatively, an APP entity may disclose to an overseas recipient without complying with APP 8.1 if the entity reasonably believes that the overseas recipient is subject to a law or binding scheme that has the effect of protection the information similar to the APPs, and mechanisms can be accessed to enforce that protection (APP 8.2(a)).

Localisation requirements: there are no specific data sovereignty or localisation requirements (such as governmental consent, approval or registration requirements) under the Privacy Act.

Upcoming reforms

On 28 September 2023, the Government released its response to the Privacy Act Review Report. The report considered 116 proposal, which if implemented, would involve the most dramatic change to the Australian privacy and data protection landscape since the introduction of the APPs. Key proposed reforms include expanding the scope of the definition of 'personal information', removal of the small business exemption and employee records exemption, stricter requirements in relation to notifying data breaches (including a 72 hour notification timeframe), and introducing a data controller-processor distinction).

Let's connect to discuss how we can help:

Jensen Li
Partner, PwC Australia

+61 433 942 706
jensen.li@au.pwc.com