DENTONS

Data protection, privacy and artificial intelligence laws

Grow | Protect | Operate | Finance

2024

Data protection, privacy and artificial intelligence laws

1. Privacy

Legislation and regulation

Australia has both federal and state and territory legislation governing the use of personal information.

At the federal level, the Australian Privacy Act 1988 (Cth) (**Privacy Act**), applies to acts and practices, whether occurring in Australia or overseas, by any organisation with an Australian "link". Businesses that target and sell to persons in Australia and collect their personal information are likely to be considered to have an Australian link. The Privacy Act is set to be significantly reformed in 2024-2025.

For some states and territories, there is additional specific legislation regulating processing of health information by private sector organisations. Also, generally, more stringent and broader requirements apply for government agencies and companies that provide services to them.

The federal government have publicly stated that they intend to reform Australia's privacy and cyber security laws and the regime regulating artificial intelligence and announced their intention to implement new laws in the next year or so for mandatory ransomware payment reporting, reviewing data retention requirements in legislation and making further changes to the federal Privacy Act and the federal Security of Critical Infrastructure Act.

Key definitions

"**Personal information**" is defined in the Privacy Act as information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not that information or opinion is true or not or is recorded in a material form or not.

"**Sensitive information**" is a special category of personal information which includes information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record or health, genetic and biometric information or biometric templates.

The Office of the Information Commissioner (**OAIC**) is the national regulatory body responsible ensuring compliance with the Privacy Act.

Australian Privacy Principles

The Privacy Act establishes thirteen Australian Privacy Principles (set out in Schedule 1 of the Privacy Act) (**APP**s) which must be followed by entities who are collecting, using, disclosing, handling, dealing with or processing personal information.

The Privacy Act does not currently differentiate between processors (being entities that ultimately control personal information) and processors (those that handle personal information on behalf of a controller). It is expected that the reforms to be enacted by the Australian Government in 2024 will introduce controller and processor concepts.

The Australian Privacy Principles address the open and transparent management of personal information, its collection, use and disclosure, the responsibility to maintain the integrity and security of personal information and the right of individuals to request access to or correction of their personal information. Entities covered by the Privacy Act must have a clearly expressed and update to date privacy policy freely available to the individuals whose information it collects or processes. Any collection of personal information must be reasonably necessary for an entity's functions or activities.

Entities must not use or disclose any personal information that they hold for any purpose other than for the purpose it was collected unless the individual has consented to the other uses or disclosures, or the other purpose is related to the original purpose (or *directly* related in the case of sensitive information). In each case, the individual must reasonably expect the entity to use or disclose for that other purpose.

Sensitive information is subject to stricter restrictions on processing and must not be collected without the consent of the individual.

Entities must take reasonable steps to maintain the security of personal information which they hold.

There are additional rules for entities that process the tax file numbers and other government related identifiers of individuals and credit information.

Cross border transfers

Although there are some exceptions, when transferring personal information from Australia to a recipient in another country, entities are required to take reasonable steps to ensure that the overseas recipient complies with the APPs and the entity may be liable for any breaches of the Privacy Act by that overseas recipient in certain circumstances.

Employee records exemption

A private sector employer's handling of employee records in relation to current and former employment relationships is exempt from the Australian Privacy Principles in certain circumstances. The exemption may apply if the organisation's act or practice is directly related to an employment relationship between the employer and the individual or an employee record held by the organisation relating to the individual. This exemption is expected to be significantly amended by the federal government as part of their reform agenda for 2024-2025.

Small business exemption

In some circumstances small businesses with turnover of less than AU$3 million are exempt from the Australian Privacy Principles. However, this exemption is not available to all small businesses. For example, a business that provides health services, trades in personal information, is a contractor that provides services under a Commonwealth contract or is a credit reporting body is required to comply with the Australian Privacy Principles.

This exemption is expected to be significantly amended by the federal government as part of their reform agenda for 2024-2025.

Data breach notification

Under the Privacy Act, if there has been unauthorised access to, or unauthorised disclosure of, personal information held by an organisation or personal information has been lost in circumstances where unauthorised access to, or unauthorised disclosure of, that personal information is likely to occur, and this would likely result in serious harm to the individual, then that organisation will have suffered an "**eligible data breach**".

Where an entity is aware of reasonable grounds to suspect that they may have suffered an eligible data breach, they must carry out a reasonable and expeditious assessment of those grounds to determine whether an eligible data breach has occurred, which must be completed within 30 days. This data breach notification regime is expected to be significantly amended by the federal government as part of their reform agenda for 2024-2025.

Subject to some exceptions, where an eligible data breach has occurred, the entity must submit a statement to OAIC notifying them of the eligible data breach as soon as practicable after it becomes aware of the breach. The entity must also notify the affected individuals as soon as practicable after preparing the statement for OAIC, subject to limited exceptions.

Penalties

The OAIC can impose penalties for a serious interference, or repeated interferences, with the privacy of an individual under the Privacy Act of up to the greater of:

a. A$50 million;

b. three times the value of the benefit derived from the interference/s with privacy, or

c. if the value of the benefit cannot be ascertained, then 30 per cent of the company's adjusted turnover.

If a business's privacy policy is not accurate or is misleading (either expressly or by silence), it could also face action by the Australian Consumer and Competition Authority (**ACCC**) (the consumer protection regulator in Australia) for making false or misleading representations and the penalties that may apply are similar to the penalties for a serious interference, or repeated interferences, with privacy.

2. Direct marketing

Businesses undertaking direct marketing activities including targeted advertising, email or other messaging platform campaigns and telemarketing are regulated under the Privacy Act, *Spam Act 2003* (Cth) (**Spam Act**) and *Do Not Call Register Act 2003* (Cth) (**Do Not Call Register Act**).

The Australian Communications and Media Authority (**ACMA**) is the regulator responsible for compliance and enforcement of anti-spam and telemarketing laws.

Anti-Spam Law

The *Spam Act 2003* (Cth) regulates commercial electronic messages and prohibits businesses from sending commercial electronic messages which offer, advertise or promote goods and services without the consent of the recipient. The sender of a commercial electronic message must also comply with certain requirements such as providing recipients with the opportunity to opt out from receiving further messages.

Telemarketing

Voice calls (including using recorded or synthetic voice) are governed the *Do Not Call Register Act 2003* (Cth). Voice calls are not permitted to phone numbers listed on the Do Not Call Register unless the persons have consented to receiving such calls. The *Telecommunications (Telemarketing and Research Calls) Industry Standard 2017* (Cth) sets out the requirements that persons conducing telemarketing must comply with including identifying themselves and only calling within certain permitted timeframes.

Use of personal information for the purpose of direct marketing

Additionally, under the Privacy Act, a business may use an individual's personal information for the purpose of direct marketing if:

a. the business collected the personal information from the individual;

b. the individual would reasonably expect the business to use their personal information for direct marketing purposes; and

c. the business has provided a simple means to opt out of direct marketing messages and the individual has not so opted out.

Penalties

The maximum penalty for a company making unsolicited commercial electronic messages in breach of the Spam Act is A$2.75 million for each day the company contravenes the penalty regimes under the Spam Act.

The maximum penalty for a company making unsolicited telemarketing calls in breach of the Do Not Call Register Act is A$2.75 million for each day the company contravenes the penalty regimes under the Do Not Call Register Act, and the maximum penalty for contraventions of the Telemarketing Standard may be up to A$250,000 for each infringement.

Where direct marketing activities also interferes with an individual's privacy a business may also be liable for penalties for breach of the Privacy Act as described in the previous section.

3. Consumer Data Right

Australia has a Consumer Data Right since the enactment of the federal legalisation called the *Laws Amendment (Consumer Data Right) Act 2019* (Cth). The Consumer Data Right is a right of consumers to data portability - and the right is to be rolled out across the entire Australian economy on a sector-by-sector basis. The banking sector and the energy sector have been required to implement the Consumer Data Right. The non-bank lending and telecommunications sectors have been designated as the next sectors in which the Consumer Data Rights will be rolled out.

The Consumer Data Right seeks to enhance competition and give customers more control and choice over data held about them in the regulated sectors by enacting stricter privacy requirements for the collection and disclosure of personal information as well implementing a new right for consumers and certain small businesses to data portability. The geographic scope of the law is broad as it will apply to data generated or collected both in Australia and outside Australia in the designated sectors.

Technical standards for the consumer data right and for how data is to be shared are being developed by a newly appointed data standards body, Data 61. The ACCC will be the lead regulator with support from Data 61 and the OAIC.

4. Industry specific data protection regulations

There are industry specific data protection laws and regulations that apply in Australia. Some examples of industries with specific regulatory obligations include:

- Critical infrastructure
- Banking and financial services
- Health services
- Telecommunications

5. Government interceptions laws and security of critical infrastructure

The *Telecommunications (Interception and Access) Act 1979* (Cth) permits Australian law enforcement and security agencies to intercept communications, access stored communications and authorise the disclosure of data by telecommunications providers for national security or law enforcement purposes.

The *Telecommunications Act 1997* (Cth) (**Telecommunications Act**) establishes a regime whereby various Australian law enforcement agencies can request or compel designated communications providers to provide certain types of access or assistance to the agency. A designated communications provider is defined broadly such that it includes telecommunications network and internet service providers but also any person that supplies goods or services to those providers, as well as any business operating a website, messaging application or service delivered using the internet in Australia. The Telecommunications Act has extra territorial reach and applies to anyone providing a website or information technology equipment or services in Australia.

There are severe consequences for not complying with the Telecommunications Act or for breaching its provisions aimed to keep secret the requests made to businesses for cooperation with Australian law enforcement and security agencies to intercept communications, access stored communications or disclose data.

See also section 2.11 regarding the regulation of the security of critical infrastructure assets. The SOCI Act also requires, amongst other obligations, entities regulated by it to cooperate with interventions by the Australian Government security agencies.

6. Artificial intelligence

Presently there is no specifical law regulating the use of artificial intelligence (**AI**) but instead there is a patchwork of laws regulating privacy, critical infrastructure, intellectual property, product liability, consumer protection, discrimination, workplace safety and negligence and data security.

In 2024, the federal Australian government announced an intention to implement specific laws aimed to ensure safe and responsible use of AI.

ABOUT DENTONS

Across over 80 countries, Dentons helps you grow, protect, operate and finance your organization by providing uniquely global and deeply local legal solutions. Polycentric, purpose-driven and committed to inclusion, diversity, equity and sustainability, we focus on what matters most to you.

www.dentons.com

CSBrand-153608-Doing Business in Australia Guide-Chapter 11 — 02/11/2024