Topic	Privacy Act 1988 (Cth)	GDPR
Personal Data	The Privacy Act governs the handling of 'personal information', defined as "information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not." (s6(1)).	**Articles 17 and 20:** Any information: (a) Relating to an identified or identifiable natural person; (b) An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Subject	'Individual' is defined as "a natural person" (s6(1)). Regulator guidance indicates that a deceased person is not a natural person (APP Guidelines para. B95).	Relating to an identified or identifiable natural person.
Controller	The Privacy Act does not distinguish between controllers and processors. Instead, the APPs apply to any APP entity that collects personal information. The definition of 'APP entity' includes: • most Australian Government agencies • all private sector and not-for-profit organisations with an annual turnover of more than AUS $3 million • all private health service providers, and • some small businesses (ie, that trade in personal information for a benefit, are a contracted service provider to the Australian Government, or are a credit reporting body; ss 6(1), 6A).	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or member state law, the controller or the specific criteria for its nomination may be provided for by Union or member state law.
Processor		A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. However, GDPR does also have a definition for "third party": A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.
Consent	'Consent' is defined as "express consent or implied consent" (6(1)). Regulator guidance indicates that the four key elements of consent are: • the individual is adequately informed before giving consent • the individual gives consent voluntarily	**Article 4:** (11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Topic	Privacy Act 1988 (Cth)	GDPR
	• the consent is current and specific • the individual has capacity to understand and communicate consent (APP Guidelines para. B. 35).	

Sensitive Data	'Sensitive information' is a subset of personal information and is defined as:
	• information or an opinion (that is also personal information) about an individual's:
	  ○ racial or ethnic origin
	  ○ political opinions
	  ○ membership of a political association
	  ○ religious beliefs or affiliations
	  ○ philosophical beliefs
	  ○ membership of a professional or trade association
	  ○ membership of a trade union
	  ○ sexual orientation or practices, or
	  ○ criminal record
	• health information about an individual
	• genetic information (that is not otherwise health information)
	• biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or
	• biometric templates (s 6(1)).
	
	APP 3 provides that sensitive information about an individual must not be collected unless the individual consents and the collection is reasonable necessary for an APP entity's functions or activity, or a listed exception applies.
		Article 9:
		Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
		
		Listed exceptions apply.

Topic	Privacy Act 1988 (Cth)	GDPR
Transfer of Personal Data to third countries or international organizations	APP 8 provides that, before disclosing personal information outside of Australia, a business must take reasonable steps to ensure that the recipient does not breach the APPs in relation to the information, unless a listed exception applies. An APP entity that discloses personal information to an overseas recipient is accountable for a breach of the APPs by the recipient in relation to the information (s 16C; exceptions apply).	Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if the conditions laid down in Article 44 – 50 are complied with by the controller and processor to ensure that the level of protection of natural persons guaranteed by the GDPR. Transfers on the basis of an adequacy decision and methods such as BCR, Contract Clauses, etc. or in the case of EU-US transfer, the Privacy Shield.
Right to restriction of processing	**No equivalent.**	**Article 18:** "The data subject shall have the right to obtain from the controller restriction of processing [where a specified ground applies]".
Right to be forgotten	**No equivalent.** APP 11.2 requires that APP entities must destroy or deidentify personal information that they no longer require for a lawful business purpose. However, individuals have no express right to require APP entities to destroy or deidentify the information that they hold about them.	**Article 17:** "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay [where a specified ground applies]".
Data Portability	**No direct equivalent.** APP 12.1 provides that if an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information. APPs 12.2 and 12.3 list exceptions. APP 12.5 provides that the entity must take reasonable steps to give access in a way that meets the needs of the entity and the individual.	**Article 20:** "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided".
Data breach notification	Amendments to the Privacy Act to introduce a mandatory data breach notification requirement will come into force on 22 February 2017. APP entities that experience an 'eligible data breaches' (that generate a "likely risk of serious harm" to affected individuals) must give a statement in a prescribed format to the Information Commissioner as soon as practicable (s26WK), and to affected individuals (26WL).	**Article 33:** "…the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority…" **Article 34:**

Topic	Privacy Act 1988 (Cth)	GDPR
	If it is unclear whether a breach is eligible, APP entities must conduct an assessment within 30 days of becoming aware of the breach (s26WH).	Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural personas, the controller shall communicate the personal data breach to the data subject without undue delay".
Penalty	A breach of the APPs is an 'interference with privacy (s13). Serious or repeated interferences with privacy may be subject to a civil penalty of up to AUD $2.1 million for companies (s13G).	Under **Article 83:** • Up to 10 000 000 EUR, or in the case of an undertaking, up to 2 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher for infringements of obligations such as controllers and processors, the certification body, and the monitoring body. • Up to 20 000 000 EUR, or in the case of an undertaking, up to 4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher for infringements of obligations such as principles of processing, conditions for consent, data subject's rights, transfer beyond EU, etc. Under Article 84, each member state can lay down the rules on other penalties applicable to infringements of GDPR in particular for infringements which are not subject to Article 83, and can take all measures necessary to ensure that they are implemented.