	EU GDPR	AUSTRALIAN PRIVACY ACT
Who does this apply to?	Data processing activities of businesses, regardless of size, that are data processors or controllers	Most Australian Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses.
What does this apply to?	Personal data - any information relating to an identified or identifiable natural person: Art 4 (1)	Personal information (PI) - information or an opinion about an identified individual, or an individual who is reasonably identifiable: s 6(1)
Jurisdictional Link?	Applies to data processors or controllers: " with an establishment in the EU, or " outside the EU, that offer goods or services to individuals in the EU or monitor the behaviour of individuals in the EU: Art 3	Applies to businesses: " incorporated in Australia, or " that 'carry on a business' in Australia and collect PI from Australia or hold PI in Australia: s 5B
Accountability and Governance	Controllers generally must: " implement appropriate technical and organisational measures to demonstrate GDPR compliance and build in privacy by default and design: Arts 5, 24, 25 " undertake compulsory data protection impact assessments: Art 35 " appoint data protection officers: Art 37	APP entities must take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs and to enable complaints: APP 1.2 Businesses are expected to appoint key roles and responsibilities for privacy management and to conduct privacy impact assessments for many new and updated projects

	EU GDPR	AUSTRALIAN PRIVACY ACT
Consent	Consent must be: " freely given, specific and informed, and " an unambiguous indication of the data subject's wishes which, by a statement or by a clear affirmative action, signifies agreement to processing: Art 4(11)	Key elements: " the individual is adequately informed before giving consent, and has the capacity to understand and communicate consent " the consent is given voluntarily " the consent is current and specific: OAIC's APP GLs
Data Breach Notifications	Mandatory DBNs by controllers and processors (exceptions apply): Arts 33-34	From 22 February 2018, mandatory reporting for breaches likely to result in real risk of serious harm
Individual Rights	Individual rights include: " right to erasure: Art 17 " right to data portability: Art 20 " right to object: Art 21	No equivalents to these rights. However, business must take reasonable steps to destroy or de-identify PI that is no longer needed for a permitted purpose: APP 11.2. Where access is given to an individual's PI, it must generally be given in the manner requested: APP 12.5
Overseas Transfers	Personal data may be transferred outside the EU in limited circumstances including: " to countries that provide an 'adequate' level of data protection " where 'standard data protection clauses' or 'binding corporate rules' apply " approved codes of conduct or certification in place: Chp V	Before disclosing PI overseas, a business must take reasonable steps to ensure that the recipient does not breach the APPs in relation to the information: APP 8 (exceptions apply). The entity is accountable for a breach of the APPs by the overseas recipient in relation to the information: s 16C (exceptions apply)

	EU GDPR	AUSTRALIAN PRIVACY ACT
Sanctions	Administrative fines of up to €20 million or 4% of annual worldwide turnover (whichever is higher): Art 83	Powers to work with entities to facilitate compliance and best practice, and investigative and enforcement powers: Parts IV and V