Due diligence checklist: Privacy Act and the APPs

Privacy Act 1988 and the Australian Privacy Principles. OAIC, Australia.

Regime	Privacy Act and the APPs
Regulator	OAIC
Country	Australia
Regulator's page	https://www.oaic.gov.au/privacy/australian-privacy-principles
Prepared	9 November 2026
Current version	https://www.vederca.com/market-scan/due-diligence/au-privacy

What it is

Personal information goes only to suppliers that handle it under the APPs, with cross-border disclosures accounted for.

Who it applies to

Applies to every financial institution in Australia.

What to ask a vendor, and the evidence to request

#	Ask the vendor for	Evidence to request	Received
1	Handling of personal information under the Australian Privacy Principles, by contract	Conformance test results or a written statement of conformance against the standard, with the version supported.	
2	Where data is hosted and processed, and any disclosure outside Australia (APP 8)	The hosting regions and a data flow description naming every country data is stored in or processed from, and the transfer mechanism for anything leaving the country.	
3	Cooperation with the Notifiable Data Breaches scheme, including timely notice of eligible breaches	The incident notification clause and procedure: what counts as an incident, who is told, within what time, and a record of a past notification if one exists.	

In every case

- A named contact at the vendor responsible for this regime, and how the vendor tracks changes to it.
- Which named customers the vendor already serves under this regime, as references you may call.

This checklist is a starting point for a procurement team, not legal advice. Read it with the regulator's own page, your institution's policies and your legal and risk teams; the regime may have changed since the date on this document.