

The RoPA is the artefact every privacy programme actually maintains, and the one an auditor opens first. The role column is the important one: it decides whether Table A.1 (controller) or Table A.2 (processor) controls apply to that activity. Table A.3 shared security controls apply either way.

REF	PROCESSING ACTIVITY	OUR ROLE	PII CATEGORIES	PII PRINCIPALS	PURPOSE	LAWFUL BASIS / APP RELIED ON	SOURCE	RECIPIENTS AND PROCESSORS	CROSS-BORDER TRANSFER	RETENTION	SECURITY CONTROLS	OWNER
P-01	Employee records and payroll	PII controller	Name, address, TFN, bank details, superannuation, emergency contacts	Employees	Employment administration and statutory obligations	Required by law (Fair Work, ATO); APP 3	Direct from employee	Payroll provider (processor), superannuation funds, ATO	No	7 years after employment ends	Role-based access, encryption at rest, quarterly access review	Head of People
P-02	Recruitment and applicant tracking	PII controller	Name, contact details, CV, work rights, interview notes	Job applicants	Assessing suitability for employment	Consent at application; APP 3 and APP 5	Direct from applicant and recruiters	Applicant tracking SaaS (processor)	Yes — vendor hosts in Singapore	12 months for unsuccessful applicants unless consent to retain	Access limited to hiring panel, automatic purge job	Head of People
P-03	Customer account administration	PII controller	Name, business email, phone, role	Customer staff (our direct users)	Providing and supporting the service, billing	Necessary for the contract; APP 3 and APP 6	Direct from customer	Billing platform, support desk (processors)	Yes — support desk hosted in the United States	Duration of contract plus 7 years for financial records	MFA enforced, audit logging, least privilege	Chief Operating Officer
P-04	Customer end-user data hosted in the platform	PII processor	Whatever the customer uploads — may include sensitive information	Our customers' end users	Processing on documented instructions from the customer	Determined by the customer as controller; we act on instruction	From the customer	Sub-processors listed in the DPA	Yes — primary AU region, backup in Singapore	Deleted 30 days after contract end, or on instruction	Tenant isolation, encryption in transit and at rest, no production access without approval	Chief Technology Officer
P-05	Support tickets and correspondence	PII processor	Contact details plus whatever a user includes in a ticket	Customers' end users and staff	Resolving support requests	On instruction from the customer	From the requester	Support desk provider (sub-processor)	Yes — United States	24 months	Redaction guidance for agents, access logging	Support Manager
P-06	Marketing and prospect list	PII controller	Name, business email, company, engagement history	Prospects and subscribers	Direct marketing of related services	Consent, with opt-out in every message; APP 7	Web forms, events, opt-in	Marketing automation platform (processor)	Yes — United States	Until opt-out, then suppression list only	Consent timestamps retained, opt-out honoured within 48 hours	Head of Marketing
P-07	Website analytics	PII controller	IP address, device and usage data, cookie identifiers	Website visitors	Understanding and improving site performance	Consent for non-essential cookies; APP 3 and APP 5	Collected automatically	Analytics provider (processor)	Yes — United States	14 months	IP truncation enabled, consent banner gating non-essential cookies	Head of Marketing
P-08	Security monitoring and incident logs	PII controller	User identifiers, IP addresses, access and event logs	Employees and end users	Detecting and investigating security incidents	Legitimate function; APP 11 security obligation	Generated by systems	SIEM provider (processor)	Yes — Australia region	12 months hot, 12 months archive	Restricted to the security team, tamper-evident storage	Security Lead
P-09	Vendor and contractor management	PII controller	Contact details, contract terms, insurance and clearance evidence	Vendor personnel	Managing the supply chain and third-party risk	Necessary for the contract	From the vendor	Contract management system (processor)	No	7 years after contract end	Access restricted to procurement and legal	Chief Operating Officer
P-10	Privacy request handling	PII controller	Requester identity, the request, the response	Any PII principal	Meeting access and correction obligations	Required by law; APP 12 and APP 13	From the requester	None	No	7 years	Case file access restricted to the privacy team	Privacy Officer

Free to use and adapt. This template is published in full by [Aegentra Academy](#), an official PECB authorised training partner in Australia. Get the rest of the set and the course it accompanies at [aegentra.com.au/academy/iso-27701-lead-implementer](#).