Aegentra
ACADEMY

PII controller vs PII processor — who owes what

The role determination that decides which Annex A table applies

The role is decided per processing activity, not per organisation — most organisations are both. Under ISO/IEC 27701:2025 this determination selects Table A.1 (31 controller controls), Table A.2 (18 processor controls) or the shared Table A.3 (29 security controls).

OBLIGATION AREA	PII CONTROLLER OWES	PII PROCESSOR OWES	WHO AN AUDITOR ASKS FIRST	COMMON FAILURE
Determining purpose	Decides why and how PII is processed, and can be held to that purpose	Processes only on documented instruction; must not decide purpose	Controller	A processor quietly repurposing data for product analytics without instruction
Lawful basis	Establishes and records the basis for each activity	None — inherits the controller's basis	Controller	No recorded basis at all, only a general privacy policy
Transparency and notice	Provides collection notices to PII principals	Supports the controller; does not notify directly	Controller	Notices that do not match what the RoPA says is collected
PII principal rights	Answers access, correction and deletion requests	Assists the controller within agreed timeframes	Controller	No contractual timeframe for the processor to assist, so the controller misses its own deadline
Records of processing	Maintains a full RoPA for its own activities	Maintains records of processing carried out for each controller	Both, separately	One combined register that does not distinguish the two roles
Privacy risk assessment	Assesses risk to PII principals before processing	Assesses risk in how it processes on the controller's behalf	Controller	Assessment done once at project start and never revisited
Sub-processors	Approves and oversees the chain	Must not engage a sub-processor without authorisation, and remains liable	Processor	Sub-processor added with no notice to the controller
Cross-border transfer	Ensures the overseas recipient will not breach the APPs (APP 8)	Discloses transfer locations and does not move data without instruction	Controller, then processor	A backup region in another country that nobody documented
Security of PII	Takes reasonable steps to protect PII (APP 11)	Implements the agreed security measures and demonstrates them	Both — Table A.3 applies to each	Assuming the other party owns encryption
Breach handling	Assesses whether it is an eligible data breach and notifies the OAIC and individuals	Notifies the controller without undue delay so the controller can assess	Controller for the decision, processor for the timeline	No agreed notification window in the contract
Retention and disposal	Sets retention periods and disposes when no longer needed	Deletes or returns PII at the end of the contract on instruction	Controller for the schedule, processor for the execution	Backups retained past the deletion instruction with no record
Contracts	Puts written terms in place with every processor	Operates within them and can evidence compliance	Both	A DPA signed at onboarding and never reviewed against what actually happens