PROCUREMENT CHECKLIST | VOICE AI AGENTS AUSTRALIA

Voice AI Compliance Checklist

For legal, healthcare, accounting, financial services, and government procurement teams evaluating enterprise voice AI platforms.

VAAA -- Voice AI Agents Australia | voiceaiagents.com.au | May 2025

HOW TO USE THIS CHECKLIST

Complete this evaluation for any voice AI vendor you are assessing. A single FAIL in Category A should be treated as a disqualifying result for compliance-sensitive organisations. Share completed versions with your legal, IT, and procurement teams for sign-off.

CATEGORY A -- DATA RESIDENCY & SOVEREIGNTY (CRITICAL)

☐	#	Evaluation Question & Why It Matters	Cloud AI Result	VAAA Result
☐	A1	**Where is voice data processed -- on-premise or cloud?** Determines whether data leaves your network perimeter. On-premise = no egress. Cloud = data transmitted to vendor servers in foreign jurisdictions.	✗ FAIL Cloud hosted	✓ PASS 100% local
☐	A2	**Which countries is voice data transmitted to?** Australian Privacy Act cross-border disclosure obligations. US-hosted processing requires additional contractual safeguards cloud vendors rarely provide in full.	✗ FAIL US / EU servers	✓ PASS None -- no egress
☐	A3	**Which third-party subprocessors receive access to your data?** Cloud AI typically involves 3+ parties: vendor, cloud provider (AWS/ GCP/Azure), LLM provider (OpenAI etc.). Each is a potential data access and breach point.	✗ FAIL Multiple parties	✓ PASS Zero subprocessors
☐	A4	**Is model training opt-out enforced by architecture or by policy?** A policy can change with a terms-of-service update. Architecture cannot. If opt-out requires contractual agreement rather than a technical constraint, it is not enforceable at the data layer.	⚠ RISK Policy only	✓ PASS Architecture

CATEGORY B -- REGULATORY & PRIVILEGE COMPLIANCE

☐	#	Evaluation Question & Why It Matters	Cloud AI Result	VAAA Result
☐	B1	**Does processing voice conversations through this platform risk waiving legal professional privilege?** Third-party disclosure of privileged communications can constitute waiver under Australian law. Cloud voice AI creates this exposure for every client conversation handled through the platform.	✗ FAIL Privilege at risk	✓ PASS No waiver risk
☐	B2	**Does the platform meet OAIC health records handling guidelines?** Patient voice data constitutes health information. OAIC guidelines require the highest level of protection. Offshore processing without specific contractual frameworks fails this standard.	⚠ RISK Uncertain compliance	✓ PASS By design
☐	B3	**Can you produce a complete audit trail of all data accesses on demand?** Required for OAIC, ASIC, and legal privilege compliance. Cloud vendor audit logs are vendor-controlled -- you cannot independently verify, export, or produce them for your own regulators.	⚠ RISK Vendor-controlled	✓ PASS Full local log

CATEGORY C -- CAPABILITY & OPERATIONS

☐	#	Evaluation Question & Why It Matters	Cloud AI Result	VAAA Result
☐	C1	**Does the platform support autonomous agent execution (tool use, browser control, task delegation)?** IVR and voice menus are not AI agents. True autonomous agents execute multi-step tasks, use external tools, and adapt without human-in-the-loop for each action.	✗ FAIL Voice menus only	✓ PASS Full autonomous
☐	C2	**Does the platform support scheduled, unattended task automation?** True operational value requires agents that run tasks on schedule without human initiation -- daily reports, weekly follow-ups, monthly compliance checks, recurring reconciliation.	✗ FAIL Manual trigger only	✓ PASS Full cron scheduling
☐	C3	**Is pricing fixed-cost, or metered per call/minute/API request?** Cloud voice AI with per-minute billing creates unpredictable operational costs. Fixed-cost local deployment provides budget certainty and eliminates usage-based billing surprises at month-end.	⚠ RISK Metered billing	✓ PASS Fixed cost

SCORING GUIDE -- INTERPRETING RESULTS

All PASS	Platform meets minimum compliance bar. Proceed to technical evaluation and legal review.
Any ⚠ RISK	Escalate to legal and IT security for written risk assessment. Document mitigation controls before proceeding. Treat as conditional approval only.
Any FAIL in Cat. A	Disqualifying for compliance-sensitive organisations. Cloud deployment with data egress cannot be remediated through policy. Do not proceed without architectural change to local deployment.

✓ VAAA RESULT: ALL CATEGORIES -- FULL PASS

VAAA is the only enterprise voice AI platform in Australia that passes all Category A criteria by architecture. Local deployment eliminates data egress at the infrastructure level -- not through contractual promises. For compliance-sensitive organisations in legal, healthcare, accounting, financial services, and government, this is the only path to voice AI your legal and procurement teams will approve.

Ready to Validate VAAA Against Your Requirements?

Book a technical demo or start a free 14-day proof of concept on your own network. Zero cost, zero obligation.

voiceaiagents.com.au | hello@voiceaiagents.com.au | Perth, Western Australia