



Sovereign AI — questions to ask

The compiled checklist: for sovereignty claims, AI services and the facilities behind them

How to use this sheet

Each sheet in this series ends with questions; this one gathers the essentials. They work in council meetings, consultation sessions, procurement decisions and letters to proponents. None are hostile. A credible proponent, vendor or agency can answer all of them and evasion on any is itself an answer.

For any “sovereign” claim

- Which layer is claimed: data location, compute, model capability or operational control?
- Who owns and controls the asset and under which country's laws?
- What arrangement makes the claim verifiable: certification, contract, audit, ownership?
- What do Australians actually get that we couldn't get otherwise and who guarantees it?

For data and cloud services

- Where is our data stored, who operates the facility and who holds the encryption keys?
- Which governments could lawfully compel access to it?
- What does the contract promise about location and access and what happens on exit?

For AI systems making decisions

- Which laws and guidance does this system operate under and who is accountable?
- When did an automated decision affect me and how do I challenge it?
- What has been disclosed about automated decision-making under privacy rules?

For the facilities

- Is this facility a regulated critical asset under the SOCI framework?
- Is it built for training, inference or both and what does that mean for energy, water and grid support?
- Does its national-significance framing come with better coordination or just pressure for less scrutiny?

Want to know more? The full series: what sovereign AI means (01), where data lives (02), compute (03), regulation (04), security (05), open models (06). This sheet is general information, not legal advice; check the named sources for current detail.