

Where your data lives — jurisdiction and the cloud

Onshore doesn't mean untouchable, offshore doesn't mean lawless — how it actually works

The key idea: geography matters, but law matters more

“Your data is stored in Australia” sounds like the end of the story. It isn't. What matters is the combination of **where data sits** and **which laws reach it** and those are different questions. This sheet corrects both directions of misunderstanding: onshore-is-safe complacency and cloud panic.

How the cloud actually stores things

Cloud services spread data across data centres, the physical buildings this series' companion sheets describe. Major providers now operate Australian regions, so data can be kept onshore. But storage location is only one fact about a service: who operates it, who can be compelled to hand data over and where support staff sit all shape who can actually reach it.

The jurisdiction reality

Data stored in Australia by a foreign-owned provider may still be reachable by that provider's home government in some circumstances; several countries assert legal reach over their companies' data wherever it's held. Equally, Australian law (privacy, consumer protection, notifiable data breach rules) applies to services offered to Australians, wherever the servers are. **Onshore ≠ out of reach; offshore ≠ lawless.** The honest question is which laws apply and what the contract says.

How government handles it

The Australian Government's own approach is instructive: a **hosting certification framework** classifies providers by ownership, control and security arrangements and sensitive workloads must use certified providers. The lesson transfers: sovereignty of data is achieved by *verifiable arrangements* (certification, contracts, encryption, audit), not by an address.

What good practice looks like

- Providers state plainly where data is stored, who can access it and under which laws.
- Sensitive community and government data held under certified or contractually protected arrangements.
- Encryption and key control explained: who can read the data, not just who stores it.
- “Data stays in Australia” claims backed in the contract, not just the brochure.

Questions to ask

Where is our data stored and who owns and operates the facility? Which governments could lawfully compel access? Who holds the encryption keys? What does the contract, not the marketing, actually promise?

Want to know more? The Digital Transformation Agency publishes the hosting certification framework; the OAIC covers privacy rights; the ACSC publishes cloud security guidance. This sheet is general information, not legal advice; check the named sources for current detail.