

Data Sovereignty Checklist for MSPs Handling Veteran Data

A practical control checklist for managed service providers who host, support or process the records of Australian veterans and former ADF members. Built from the Deep Tech Australia insights series by Shaune Irving, CTO of Keytech Intelligence.

1. Data classification and minimisation

- ☐ Classify veteran medical files, service records and DVA claim documents as sensitive information under the Privacy Act 1988.
- ☐ Identify protected ADF identifiers (PMKeyS numbers, unit, deployment and security details) and tag them as a separate high risk class.
- ☐ Collect only the fields each service needs. Remove or redact identifiers that are not required.
- ☐ Set a documented retention period for every record type and delete on schedule.
- ☐ Never use real veteran data in test, development or vendor demonstration environments.

Read more: <https://ausdeeptech.org/insights/veteran-medical-data-protection-what-to-ask-your-advocate>

2. Sovereign residency and custody

- ☐ Store primary data, backups and replicas in Australian data centres operated by an Australian owned provider.
- ☐ Confirm that no administrator, support desk or subprocessor outside Australia can access data in clear text.
- ☐ Hold encryption keys in Australia under your own or the client's control, not the platform vendor's.
- ☐ Map the full data path, including logging, telemetry, email and AI services, and prove each hop stays onshore.
- ☐ Prefer IRAP assessed hosting for any workload that touches government or DVA related data.

Read more: <https://ausdeeptech.org/insights/keytech-intelligence-macquarie-cloud-partnership>

3. Reference architecture

- ☐ Separate environments into zones: edge, identity, application, sensitive data and management.
- ☐ Place the sensitive data zone behind a dedicated boundary with no direct internet path.
- ☐ Run a separate management plane for administration, isolated from client workloads.
- ☐ Encrypt data in transit and at rest with modern ciphers and documented key rotation.
- ☐ Load test and fail test the architecture before onboarding real veteran records.

Read more: <https://ausdeeptech.org/insights/msp-reference-architecture-veteran-data-sovereignty>

4. Identity and access governance

- ☐ Enforce phishing resistant MFA (FIDO2 or passkeys) for every staff and administrator account.

- [] Use just in time and time limited privileged access. No standing admin rights.
- [] Apply least privilege by role and review access every quarter.
- [] Log every access to veteran records and retain logs in Australia for at least 12 months.
- [] Revoke access the same day a staff member or contractor leaves.

Read more: <https://ausdeeptech.org/insights/zero-trust-architecture-australia>

5. Third party and supply chain risk

- [] Maintain a register of every subprocessor that can touch veteran data, with location and ownership.
- [] Require contractual breach notification within 24 hours from every supplier.
- [] Assess supplier security each year against the Essential Eight and ISO 27001 controls.
- [] Remove suppliers that cannot show Australian residency for sensitive data.
- [] Test your own exposure if a supplier is breached, as the GoTo Health incident showed.

Read more: <https://ausdeeptech.org/insights/goto-health-breach-veteran-data-sovereign-governance>

6. AI and automated decisions

- [] List every system that uses personal information to make, or substantially assist, decisions about veterans.
- [] Update privacy policies before 10 December 2026 to disclose automated decision making.
- [] Keep AI models and inference that process veteran data inside sovereign infrastructure.
- [] Keep a human reviewer accountable for any decision that affects entitlements or care.
- [] Record model versions, inputs and outputs so decisions can be explained and audited.

Read more: <https://ausdeeptech.org/insights/privacy-act-10-december-2026-automated-decision-ai-transparency>

7. Assurance, testing and response

- [] Reach at least Essential Eight Maturity Level Two and track progress toward Level Three.
- [] Commission independent penetration testing at least once a year and after major change.
- [] Keep a tested incident response plan that covers the Notifiable Data Breaches scheme.
- [] Run a breach tabletop exercise with the client at least once a year.
- [] Publish a plain English privacy policy that states where data is stored and who can see it.

Read more: <https://ausdeeptech.org/insights/building-governable-ai-systems>

Deep Tech Australia, ausdeeptech.org. Author: Shaune Irving, CTO, Keytech Intelligence. General guidance only, not legal advice.