

# 6 steps to support privacy compliance & data security

New privacy law changes in Australia will impact how organisations handle personal data, with serious consequences for non-compliance. Our information transformation framework is a structured approach to modernising information management, helping you enhance security, innovation, and resilience—while ensuring compliance.



## Step 1:

### Discover

#### Identify risks & reduce data exposure

- Locate and document all personal data across digital and physical records.
- Map data flows to track how information is collected, used, and shared.
- Assess storage risks and potential breach points.
- Securely dispose of redundant, obsolete, or trivial ROT (redundant, obsolete, trivial) data.

**By discovering all data, you lower your risk of fines from unknown data breaches.**



## Step 2:

### Organise & secure data for compliance

### Unify

- Centralise data management to eliminate silos.
- Classify personal data based on privacy risks.
- Apply access controls to restrict unauthorised use.
- Embed privacy governance in daily operations.

**Centralising data allows for easier access and management, improving efficiency and reducing the risk of data silos.**



## Step 3:

### Govern

#### Establish clear privacy policies

- Set data retention and disposal policies aligned with regulations.
- Ensure legal processing of data, including valid consent.
- Implement a governance framework to adapt to evolving laws.
- Define workflows for handling data access, corrections, and deletion requests.

**Clear policies ensure compliance with regulations and build trust with customers.**



## Step 4:

### Streamline compliance & reduce risk

### Automate

- Use automation to manage data lifecycle and enforce privacy rules.
- Apply AI-driven tools to detect and mitigate privacy risks.
- Automate compliance reporting for Australian Privacy Act requirements and other relevant regulations.
- Reduce manual efforts while maintaining continuous compliance.

**Automation reduces manual errors and frees up staff for other tasks, while ensuring consistent compliance.**



## Step 5:

### Unlock

#### Enable secure & ethical data use

- Structure and govern data for responsible business use.
- Leverage privacy-enhancing technologies for compliant analytics.
- Balance privacy with business insights to unlock data value.
- Develop privacy-led innovation strategies for a competitive edge.

**Unlocking data value drives innovation and improves business outcomes while respecting customer privacy.**



## Step 6:

### Stay ahead of privacy threats

### Maintain

- Conduct regular privacy impact assessments and audits.
- Implement real-time monitoring for breaches and regulatory changes.
- Adapt privacy strategies to legal, tech, and business shifts.
- Train employees on evolving regulations to foster compliance culture.

**Continuous monitoring and improvement ensures ongoing compliance and reduces the risk of future breaches.**



## Confidently navigate regulations

Contact us for a consultation and transform your information management for greater security and compliance

