

Kiteworks Supports Australia's Privacy and Other Legislation Amendment Act 2024

A Unified Platform for Personal Information Handling Under the OAIC's Strengthened Privacy Framework

Solution Highlights



FIPS 140-3 Validated Encryption



Role-Based Access Controls



Attribute-Based Access Controls



Comprehensive Audit Logging



Data Residency and Geofencing

The Privacy and Other Legislation Amendment Act 2024 (No. 128, 2024), assented to on 10 December 2024 and registered on the Federal Register of Legislation under identifier C2024A00128, reforms Australia's privacy framework administered by the OAIC. The Act amends the Privacy Act 1988 and applies to Australian Government agencies and private sector organizations that handle personal information; the small business exemption (AU\$3 million turnover or less, covering roughly 95% of Australian businesses) is unchanged by this Act and remains a proposed second-tranche reform with no legislated timetable. It introduces a three-tier civil penalty regime — up to AU\$50 million for serious or repeated interferences (section 13G), with mid-tier and administrative penalties of approximately AU\$3.3 million and AU\$330,000 (sections 13H and 13K) — plus a direct court remedy for individuals under section 80UA. A statutory tort for serious invasions of privacy (Schedule 2, commenced 10 June 2025) and new criminal doxxing offences (Criminal Code sections 474.17C and 474.17D, up to 6 and 7 years' imprisonment) sit outside the OAIC's direct role, enforced through the courts and the justice system respectively. Automated-decision transparency obligations for APP privacy policies take effect 10 December 2026. Kiteworks supports organizations working toward compliance with the Act. Here's how:

Safeguarding Personal Information Under APP 11

Schedule 1, Part 5 of the Act amends clause 11 of Schedule 1 to the Privacy Act 1988, confirming that protecting personal information must "include technical and organisational measures" — codifying APP 11 as a security-by-design obligation. Kiteworks supports this with encryption at rest and in transit: the platform double-encrypts customer files to minimize the attack surface available to an intruder who has gained access to the operating system, uses TLS 1.2+ for encryption in transit, and applies AES-256 encryption by default at both the disk and file level. A hardened virtual appliance adds an embedded network firewall, web application firewall, intrusion detection, and file integrity monitoring as further defense-in-depth layers.

Access Governance and Cross-Border Disclosure Under APP 8

Schedule 1, Part 6 introduces a new APP 8.3 mechanism for disclosing personal information to overseas recipients in countries or binding schemes with protections "at least substantially similar" to the Australian Privacy Principles. Kiteworks supports this and the Act's broader access-governance requirements through role-based and attribute-based access controls: RBAC assigns a set of permissions to a user that control access to features and resources, while ABAC policies govern each data access dynamically based on attributes of the data, the user, and the attempted action. Kiteworks also supports data residency, storing a user's data only in their assigned country and routing it accordingly, and geofencing through blocked IP address ranges, blocked countries, and allowed IP address ranges.

Accountability and Recordkeeping for OAIC Oversight and Enforcement

The Act also strengthens OAIC oversight — expanded monitoring and investigation powers, the penalty regime above, and compliance notices under section 80UC — and adds automated-decision transparency requirements for APP privacy policies (Schedule 1, Part 15, in force 10 December 2026). Not every obligation sits with the OAIC: the statutory tort is pursued through the courts, and the doxxing offences are criminal matters outside its remit. Kiteworks supports recordkeeping and documentation by logging every file upload, download, folder creation, and access attempt with full context and user attribution, and by applying retention, file lifetime, and folder expiration controls.

The Privacy and Other Legislation Amendment Act 2024 raises the bar for how Australian entities safeguard, control, and account for the personal information they handle under the OAIC's strengthened framework. The reforms carry real consequences: a three-tier civil penalty regime under sections 13G, 13H, and 13K; a new individual right to seek court-ordered compensation under section 80UA; a statutory tort for serious invasions of privacy under Schedule 2, in force since 10 June 2025; new criminal doxxing offences under the Criminal Code; and automated-decision transparency obligations that take effect 10 December 2026. Kiteworks gives organizations a foundation for protecting personal information through encryption and access controls, for governing how they collect, use, and disclose it under the amended framework, and for demonstrating accountability to the OAIC on demand through comprehensive audit logging and recordkeeping. Kiteworks stands ready as a unified platform — one policy engine, one audit trail, built in rather than bolted on later.

Ready to Strengthen Compliance with Australia's Privacy Act?

www.kiteworks.com

Kiteworks



Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.