Kiteworks

COMPLIANCE BRIEF

Kiteworks Protects Personal Data Under Argentina's PDPL

Securing Personal Data Across Law 25.326

Argentina's Law 25.326, the Personal Data Protection Law (PDPL), establishes a comprehensive framework for protecting personal data held in public and private databases, registries, and data files across all sectors. The law applies exclusively within Argentina, covering all public institutions and private entities that collect, process, store, or transfer personal data about Argentine residents. Every industry that handles personal data falls under its scope, from financial services and healthcare to marketing firms and government agencies. Enacted on October 4, 2000, the law required existing data archives to register with the regulatory authority within 180 days of its implementing decree. Organizations that fail to comply face administrative sanctions ranging from formal warnings and operational suspensions to fines between $1,000 and $100,000 pesos, database cancellation, and criminal penalties including imprisonment for knowingly inserting false data or unlawfully accessing protected databases. Kiteworks provides organizations with the secure content governance capabilities needed to support the PDPL requirements. Here's how:

Technical and Organizational Security Measures

Argentina's PDPL requires controllers and data users to adopt the technical and organizational measures necessary to guarantee the security and confidentiality of personal data, prevent unauthorized access or alteration, and prohibit storage in systems lacking integrity and security conditions (Articles 9.1, 9.2, 21.2). Registered databases must also document the means used to guarantee data security and identify categories of personnel with access to data processing. Kiteworks addresses these requirements through its hardened virtual appliance, which delivers double encryption at rest for all stored data. Role-based access control (RBAC) ensures that only authorized users can access sensitive files at permission levels defined by the form builder, while attribute-based access control (ABAC) applies dynamic risk policies that evaluate file classification, user clearance, and contextual factors. TLS certificate validation protects data in transit by automatically terminating connections that fail certificate checks, preventing interception or spoofing attacks.

Solution Highlights

- **Hardened virtual appliance**
- **Strong double encryption**
- **Role-based access control (RBAC)**
- **Attribute-based access control (ABAC)**
- **TLS certificate validation**
- **Robust audit logs**

Access Governance and Data Life-Cycle Management

The PDPL requires that personal data be stored in a manner that allows data subjects to exercise their right of access, restricts transfers to parties with legitimate interests, prohibits transfers to countries lacking adequate protection, and mandates that data under review be blocked or flagged during rectification proceedings (Articles 4.6, 4.7, 11.1, 12.1, 16.6). Controllers must also destroy data that is no longer necessary for the purposes for which it was collected. Kiteworks supports these requirements through its Data Policy Engine (DPE), which enforces RBAC and ABAC permissions on every folder and file, ensuring access aligns with defined user roles and data sensitivity. The DPE's folder invitation policies allow administrators to block sharing with restricted domains or require approvals before transfers proceed, directly supporting cross-border transfer restrictions. The Direct Operator File Verification feature confirms, validates, and reviews files before deletion, ensuring data destruction follows a controlled and auditable process.

Audit, Retention, and Revocation Controls

The PDPL establishes that data subjects hold the right to rectification, deletion, updating, and confidentiality of their personal data, and that data must be retained only for legally or contractually defined periods. Third-party processors must destroy data upon contract completion, and individuals may request removal from advertising databases at any time (Articles 16.1, 16.7, 25.2, 27.3). Kiteworks supports these tracking and life-cycle requirements through its secure shared folder architecture, which stores all form submissions under defined retention conditions enforced by the Data Policy Engine. The Form Scheduling feature gives administrators precise control over when data collection is active, allowing immediate deactivation in response to withdrawal requests. The Direct Operator File Verification feature performs structured confirmation before any deletion executes, creating a defensible record of the action. Compliance officers can monitor all activities through Kiteworks' standard compliance reports and audit logs, providing evidence of timely response to data subject rights requests.

Kiteworks gives organizations operating under Argentina's Personal Data Protection Law a unified platform for support in meeting security, governance, and data life-cycle obligations across the law's full scope. Its hardened virtual appliance and layered encryption protect personal data at rest and in transit, while role-based and attribute-based access controls ensure that only authorized personnel reach sensitive content. The Data Policy Engine governs every file and folder according to defined permissions, enforcing cross-border transfer restrictions and blocking unauthorized sharing automatically. Form Scheduling and Direct Operator File Verification give compliance teams precise, auditable control over data collection activity and deletion workflows, enabling timely responses to data subject rights requests. Comprehensive audit logs and compliance reports create the evidentiary record organizations need to demonstrate accountability to Argentina's regulatory authority.