Kiteworks

COMPLIANCE BRIEF

Kiteworks Supports Uruguay Law No. 18.331 on Personal Data Protection

Encryption, Access Control, and Audit Documentation Under Uruguay's Data Privacy Framework

Uruguay's Law No. 18.331 on Personal Data Protection, promulgated August 2008, establishes comprehensive data privacy requirements for all data controllers and processors operating in Uruguay, including both public and private sector entities across all industries such as telecommunications, healthcare, finance, retail, and government services. The law applies throughout Uruguay, and as amended by Law 19.670 of October 2018 and regulated by Decree 64/020 of February 2020, introduces extraterritorial application to any organization processing Uruguayan residents' personal data when offering goods or services to Uruguay inhabitants or monitoring their behavior. Organizations face administrative sanctions imposed by the Data Protection Control Unit (Unidad Reguladora y de Control de Datos Personales), including observation, warning, fines up to 500,000 indexed units (UI), suspension of database operations for up to five days, or database closure. Kiteworks supports organizations working toward compliance with Law No. 18.331. Here's how:

Data Encryption and Security Infrastructure Obligations

Articles 10, 12, and 20 of Law No. 18.331 mandate that data controllers implement necessary technical measures to ensure data security and confidentiality, preventing unauthorized access, alteration, or loss of personal information. Article 12 specifically requires proactive responsibility including privacy by design, privacy by default, and impact assessments. The Kiteworks platform addresses these requirements through its hardened virtual appliance deployment architecture with multiple security layers. Files undergo double encryption at rest using AES-256 standards, while TLS 1.3 and 1.2 protocols secure data in transit. The platform incorporates AI-based intrusion detection systems that maintain pattern libraries for identifying suspicious network activities and potential threats. Built-in antivirus scanning (F-Secure/WithSecure Atlant) automatically examines files on upload and download, including content passing through the Email Protection Gateway (EPG). An embedded Web Application Firewall provides zero-maintenance protection against SQL injection, known attack signatures, and command-and-control attempts. The platform offers comprehensive TLS certificate validation to prevent man-in-the-middle attacks and real-time threat intelligence notifications when security risks are identified.

Solution Highlights

- **Strong double encryption**
- **Data Policy Engine with ABAC and RBAC**
- **Data sovereignty and geofencing**
- **Consolidated audit logs with SIEM feeds**
- **Secure Data Forms**
- **Compliance Report**

Access Governance and Cross-Border Transfer Controls

Articles 7, 8, 9, 13, 14, 15, 17, 21, 22, and 23 establish strict requirements for data collection consent, purpose limitation, data subject rights fulfillment, and international transfer restrictions. Kiteworks implements these controls through its Data Policy Engine featuring both role-based access controls (RBAC) and attribute-based access controls (ABAC). The platform enforces principle of least privilege, where users receive no default permissions until explicitly granted through user profiles and data owner invitations. Dynamic policies evaluate three attributes: data asset properties like folder paths or tags, user attributes including domain or profile, and specific actions being performed. For consent management, Secure Data Forms provides authentication options for public or private submissions, while Terms of Service policies present mandatory review and acceptance screens before data access. The REST API and SCIM support enable integration with identity management systems for automated user provisioning, modification, and deletion to fulfill data subject requests. International transfer controls utilize geofencing technology that restricts data storage and routing based on assigned user locations through LDAP or SAML attributes, blocking access from prohibited IP addresses or countries.

Audit Documentation and Accountability Requirements

Articles 12, 16, 18-BIS, 20, and 28 require comprehensive documentation of data processing activities, impact assessments for biometric data, telecommunications audit trails, and database registry compliance. Kiteworks maintains a consolidated audit log that captures all data and administrative events including file movements, file access, access-control changes, privilege changes, on/off-boarding, logins, and AV/ATP/DLP scan results. The platform generates real-time SIEM feeds through standard syslogs supporting multiple concurrent feeds to systems like ArcSight, QRadar, Splunk, and LogRhythm. Compliance summary reports demonstrate adherence to various regulatory frameworks including dedicated GDPR reports for data protection accountability. The Compliance Report enables compliance administrators to verify policy enforcement by filtering events for specific policies and time frames. For automated decision-making under Article 16, the MCP Server enables secure AI interactions with governance controls. Administrative reporting capabilities export detailed CSV files for regulatory submissions, while audit logs maintain integrity through cryptographic hashes and support configurable retention periods to meet regulatory timelines.

The Kiteworks platform delivers comprehensive technical controls that align with Uruguay Law No. 18.331's multifaceted data protection requirements. For data security obligations, Kiteworks provides hardened virtual appliances with double encryption, intrusion detection, antivirus scanning, and embedded Web Application Firewalls that protect personal data from unauthorized access or alteration. To address access governance and cross-border transfer controls, the platform implements RBAC and ABAC through its Data Policy Engine, enforces least-privilege principles, manages consent through Secure Data Forms, and restricts international transfers via geofencing technology. For audit documentation and accountability requirements, Kiteworks maintains consolidated audit logs capturing all data and administrative events, generates real-time SIEM feeds, produces compliance summary reports, and controls AI interactions through dedicated gateways. As organizations navigate Uruguay's data protection landscape, Kiteworks serves as a unified platform that addresses security infrastructure, access governance, and compliance documentation requirements through integrated technical controls and automated policy enforcement.