Kiteworks

COMPLIANCE BRIEF

Kiteworks Supports Panama's Law No. 81 on Personal Data Protection

Enable Data Security, Access Control, and Transfer Documentation Across Panama's Data Protection Framework

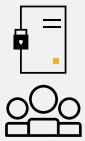
Law No. 81 on Personal Data Protection, enacted by the National Assembly of Panama on March 26, 2019, establishes comprehensive data protection requirements for organizations operating within Panama. This law applies to all data controllers and processors in both public and private sectors, including government entities, financial institutions, healthcare providers, telecommunications companies, retail businesses, and any organization maintaining databases containing personal data of Panamanian nationals or foreign residents. The law governs databases located in Panama and extends to organizations domiciled in the country, regardless of where their data is stored. Organizations face monetary sanctions ranging from B/.1,000.00 to B/.10,000.00, with additional measures including citations for minor violations and suspension or closure of data processing operations for serious infractions, with enforcement by the National Authority for Transparency and Access to Information (ANTAI). The law became effective two years after promulgation on March 29, 2021. Kiteworks supports organizations working toward compliance with Law No. 81. Here's how:

Data Encryption and Security Infrastructure Requirements

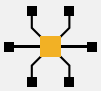
Article 2 of Law No. 81 establishes the security principle requiring data controllers to implement technical and organizational measures to guarantee data security, with heightened obligations for sensitive data. Article 7 obliges controllers to establish protocols, processes, and procedures for secure data management and transfer, and subjects them to ANTAI fiscalization. Article 26 extends these requirements to public network operators and communication service providers, who must adopt technical measures to protect personal data. The Kiteworks platform addresses these requirements through its hardened virtual appliance architecture featuring enterprise-grade double encryption at rest, TLS 1.3 encryption in transit, and an embedded network firewall that blocks all unused ports from outside traffic. The platform's embedded Web Application Firewall (WAF) operates in parallel with the network firewall, while AI-based intrusion and anomaly detection maintains an evolving library of patterns to detect suspicious network activities. For organizations handling sensitive data, Kiteworks implements zero-trust architecture and comprehensive audit logs with SIEM feeds to enable security monitoring and breach response. The Email Protection Gateway evaluates all email traffic based on policies and logs metadata, ensuring protection extends to email communications containing personal data.

Solution Highlights

Double encryption at rest



Data Policy Engine with ABAC and RBAC



Comprehensive audit logs with SIEM feeds

Time-based retention controls

AI-based intrusion detection

Rest API with SCIM support

Access Control and Data Processing Governance

Articles 2, 6, 11, and 13 establish lawful processing conditions requiring explicit consent, purpose limitation, and special authorization for sensitive data transfers. Article 15 enumerates the rights of access, rectification, cancellation, opposition, and portability. Articles 16 and 17 establish response time frames and procedures for modification or blocking, which must be fulfilled within specified time frames. Article 19 restricts automated decision-making that produces legal effects on data subjects. Kiteworks enables compliance through its Data Policy Engine (DPE), combining role-based access control (RBAC) and attribute-based access control (ABAC) to enforce dynamic policies based on data asset attributes, sender and recipient user attributes, and specific actions being taken. The platform's Secure Data Forms feature allows organizations to configure public or private submission requirements with authentication options for consent collection. For data subject rights, the REST API and SCIM support enable programmatic access for data retrieval, modification, and deletion operations within the law's required 10-business-day response period. The MCP Server ensures AI operations respect governance frameworks by inheriting authenticated user roles and permissions, preventing unauthorized automated processing. Time-based expiration controls automatically delete files after configured retention periods, while the withdrawal feature allows users to revoke access to protected email attachments after sending.

Audit Trail and Transfer Documentation Obligations

Article 31 requires data controllers to maintain a registry of all personal data transfers to third parties, making these records available to ANTAI upon request. Article 26 mandates comprehensive security monitoring for public network operators, while Article 32 specifies detailed documentation requirements for data transfer requests including requester identification, purpose, time limits, and data subject notifications. Kiteworks consolidates all user, data, and system activities into a single audit log tracking successful and failed logins, uploads, downloads, views, send activities, and receive activities. The platform logs intrusion attempts and detected anomalies, with the Email Protection Gateway capturing metadata for all inbound and outbound email traffic. For MFT operations, the platform provides detailed flow logging with comprehensive connection insights displayed through a graphical dashboard interface showing dependencies and file transfer statistics. The MCP Server generates detailed audit trails for AI operations including every file upload, download, folder creation, and access attempt. These comprehensive logs support both internal compliance monitoring and regulatory reporting to ANTAI, while the Trusted Data Format (TDF) implementation tracks every access attempt to protected files regardless of their location.

The Kiteworks platform addresses Law No. 81's data encryption and security infrastructure requirements through its hardened virtual appliance architecture featuring double encryption, embedded firewalls, AI-based intrusion detection, and comprehensive security monitoring capabilities that protect personal data across all communication channels. For access control and data processing governance, Kiteworks enables compliant consent management and data subject rights fulfillment through its Data Policy Engine, combining RBAC and ABAC controls, REST API for programmatic access, automated retention controls, and governed AI operations that respect user permissions. To meet audit trail and transfer documentation obligations, the platform consolidates all data activities into comprehensive logs tracking access attempts, transfer operations, and security events while providing detailed reporting capabilities for regulatory compliance with ANTAI. Kiteworks unifies these protection, control, and tracking capabilities into a single solution that enables organizations to maintain continuous compliance with Panama's comprehensive data protection requirements while facilitating secure collaboration and communication.