Kiteworks

COMPLIANCE BRIEF

DATA PROTECTION LAW

Kiteworks Supports Ecuador's Organic Law on Personal Data Protection (LOPDP) Compliance

Addresses Encryption, Access Control, and Audit Documentation Under Ecuador's Data Protection Framework

Solution Highlights

- Strong double encryption
- SafeVIEW and SafeEDIT
- Data Policy Engine with ABAC and RBAC
- Vault-to-vault secure integration
- Consolidated audit log with SIEM integration
- Time-based access controls
- OpenTDF persistent encryption

Ecuador's Organic Law on Personal Data Protection (LOPDP), published by the National Assembly on May 26, 2021, sets data protection requirements for public and private organizations operating in Ecuador. It also reaches foreign organizations that process Ecuadorian residents' data when offering goods or services or monitoring behavior within Ecuador. Penalties range from public warnings and corrective measures to fines. Private sector infractions carry fines of 0.1% to 0.7% of prior-year business volume, net of VAT and directly related taxes (Art. 73). For public servants, the Reglamento General and Resolución SPDP-SPD-2025-0022-R set fines at 1–10 SBU (minor) and 10–20 SBU (serious), roughly $482–$4,820 and $4,820–$9,640 at the 2026 SBU of $482. Kiteworks supports LOPDP compliance. Here's how:

01

Data Encryption and Security Safeguards

Article 37 | Article 10(g)

LOPDP Article 37 requires controllers to implement appropriate security measures, citing anonymization, pseudonymization, and encryption as examples. Article 10(g) establishes the confidentiality principle, requiring data to be processed under a duty of secrecy and barring communication beyond the original purpose absent a lawful basis. Violations carry penalties. Kiteworks meets these obligations through encryption. The platform applies AES-256 encryption at rest with a double-encryption architecture that protects files at both the file system and individual file levels. In transit, it uses TLS 1.3 and 1.2, with optional FIPS 140-3 validated encryption. The hardened virtual appliance embeds network and web application firewalls that block unauthorized access, and OpenTDF enforces persistent encryption with embedded attribute-based access controls even when data leaves the organization.

02

Access Governance and Cross-Border Transfer Controls

Article 8 | Article 33 | Article 28

Articles 8 and 33 require consent management and data transfer controls, and the regulation governs international transfers requiring adequate protection or appropriate safeguards. Article 28 bars communicating credit data on economic, financial, banking, or commercial obligations once five years pass from when the obligation became due. Noncompliance can trigger serious infractions and penalties. Kiteworks provides granular access governance through its Data Policy Engine, combining RBAC and ABAC to enforce dynamic policies based on data attributes (folder paths, tags), user attributes (domain, profile), and actions. For international transfers, vault-to-vault integration creates secure connections between Kiteworks instances with full encryption and access logging, while geofencing and domain restrictions enforce cross-border limits. Time-based access controls and expiration policies automate retention under Article 28.

03

Audit Documentation and Accountability Requirements

Article 10(k) | Article 42 | Article 43 | Article 46 | Article 51

Article 10(k) requires demonstrated accountability. Article 43 requires breach notification to the Authority and ARCOTEL within 5 days and controller-to-processor within 2 days, while Article 46 requires notifying affected data subjects within 3 days. Article 51 governs National Registry information, and Article 42 mandates impact assessments for high-risk processing, including automated decision-making. Kiteworks provides a consolidated audit log capturing all data access and processing, with 632 distinct event types spanning user actions, administrative changes, and system activities. Real-time SIEM integration enables immediate breach detection. The platform generates compliance reports mapped to LOPDP, an audit log map for impact assessments, and automated reports with CSV export documenting databases, processing purposes, data categories, recipients, and retention periods for Article 51.

IN SUMMARY

Kiteworks gives organizations a unified platform to address Ecuador's LOPDP across data protection, control, and tracking. Double encryption at rest, TLS 1.3 in transit, hardened virtual appliance deployment, and OpenTDF address Article 37's security and Article 10(g)'s confidentiality requirements. The Data Policy Engine's combined RBAC and ABAC controls, vault-to-vault transfers, and automated retention policies support access governance, cross-border transfer restrictions, and Article 28's credit data limits. The consolidated audit log with 632 event types, real-time SIEM integration, and automated reporting help organizations meet Article 43's breach notification deadlines and Article 51's registry documentation requirements. Together, these capabilities position organizations to address LOPDP's data protection obligations while maintaining operational efficiency and compliance.