Kiteworks

COMPLIANCE BRIEF

DATA PROTECTION LAW · LAW NO. 8968

Kiteworks Supports Protection of Persons Against the Processing of Their Personal Data Law, Law No. 8968

SafeVIEW and the Data Policy Engine Turn Costa Rica's Access Rights Into Executable Controls

SOLUTION HIGHLIGHTS

- Strong Double Encryption
- Embedded Web Application Firewall
- Intrusion and anomaly detection
- SafeVIEW and SafeEDIT
- Secure Data Forms
- Data Policy Engine with ABAC
- Immutable audit log

OVERVIEW

Costa Rica's Protection of Persons Against the Processing of Their Personal Data Law, Law No. 8968, was promulgated on July 7, 2011, and published in La Gaceta No. 170 on September 5, 2011. Under Article 1, this law protects individuals regardless of nationality, residence, or domicile. Article 2 establishes the material scope: the law applies to personal data contained in automated or manual databases of public or private organizations. Article 28 establishes a three-tier penalty structure: minor offenses carry fines up to five base salaries, serious offenses from five to twenty base salaries, and very serious offenses from fifteen to thirty base salaries of an auxiliary judicial position, plus suspension of the database's operation for one to six months for very serious offenses. Kiteworks supports organizations working toward compliance with Costa Rica's data protection law. Here's how:

01 — SECURITY ARCHITECTURE

Protect Data With an Assumed-Breach Architecture

Article 10 mandates that database controllers adopt technical and organizational measures necessary to protect the security of personal data and prevent alteration, accidental or unlawful destruction, loss, unauthorized processing, or access. Kiteworks implements assumed-breach architecture through file and disk double encryption that minimizes attack surfaces even if intruders gain operating system access. The platform's embedded Web Application Firewall operates as a zero-management barrier against non-Kiteworks activity including suspicious network traffic, known attack signatures, SQL injection, exfiltration, and command-and-control attempts. AI-based intrusion and anomaly detection maintains an evolving library of patterns to detect suspicious activities on the network and within the Kiteworks virtual appliance. These layered defenses align with NIST Cybersecurity Framework standards to protect personal data against the full spectrum of threats specified in Article 10.

02 — DATA SUBJECT RIGHTS

Data Subject Rights Through Eight Control Articles

Articles 5, 6, 7, and 14 establish comprehensive data subject rights requiring explicit consent, data quality controls, access and rectification rights, and transfer restrictions. Kiteworks Secure Data Forms generates unique HTTPS endpoints for each form instance, enabling compliant consent collection with authentication options for public or SSO-based submission, creating human-readable PDF files for each submission stored in secure shared folders. The platform's SCIM 2.0 compliance enables centralized identity management for maintaining data accuracy per **Article 6**'s exactitude requirements. SafeVIEW provides view-only access with optional watermarked downloads while SafeEDIT enables possessionless editing where documents never leave the secure Kiteworks environment, fulfilling **Article 7**'s access, rectification, suppression, and consent-to-assignment rights. For **Article 14**'s transfer controls, the platform enforces attribute-based access controls based on data asset attributes, user attributes, and requested actions, with secure file sharing through ACL-protected packages, expiration controls, authentication requirements, and fingerprint watermarks. Time-based access controls and retention cleanup scheduling ensure data currency per **Article 6**, while legal/admin file withdrawal capabilities with reason-tracked deletion support rectification rights.

03 — AUDIT TRAIL

Audit Trail Requirements Under Law 8968

While Law 8968 contains no explicit audit logging mandate, compliance depends on documentation that can be produced on demand. **Article 16** grants Prodhab inspection access to databases and processing protocols, **Article 7** requires organizations to demonstrate what data exists and how it has been processed, and **Article 25** establishes three-day complaint response deadlines. Kiteworks addresses these implicit recordkeeping obligations through a consolidated audit log capturing **632 distinct event types** — including file access, uploads, downloads, logins, admin actions, and MFT activities — exportable to any SIEM via syslog, with native integrations for Splunk, IBM QRadar, ArcSight, and LogRhythm. This comprehensive trail documents consent collection, data subject access responses, transfer authorizations, and system access in the format Prodhab inspectors require.

SUMMARY

Why Kiteworks for Law No. 8968

Kiteworks delivers the technical foundation Costa Rica's Law No. 8968 demands across three enforcement-critical dimensions. The platform's assumed-breach architecture — file and disk double encryption, embedded WAF, and AI-based anomaly detection — meets Article 10's comprehensive security mandate. Secure Data Forms, SCIM-compliant identity management, SafeVIEW, SafeEDIT, and attribute-based transfer controls operationalize the access, rectification, suppression, and consent-to-assignment rights guaranteed under Articles 5, 6, 7, and 14. And a consolidated audit log capturing 632 distinct event types, with real-time SIEM export, equips organizations to respond to Prodhab inspections, satisfy Article 7 processing transparency requirements, and meet Article 25's three-day complaint response deadlines. As organizations navigate Law No. 8968's three-tier penalty structure — fines up to thirty base salaries and database suspension for the most serious violations — Kiteworks serves as the unified platform where protection, control, and audit capabilities converge to safeguard personal data across all regulated operations.