Kiteworks

COMPLIANCE BRIEF

Kiteworks and Dominican Republic Law No. 172-13: Personal Data Protection

How Kiteworks Enables Secure Data Handling, Access Rights, and Cross-Border Controls Under the Dominican Republic's Personal Data Protection Framework

Law No. 172-13 on Protection of Personal Data, enacted by the Dominican Republic's Congress on December 13, 2013, and published in the Official Gazette No. 10737 on December 15, 2013, establishes comprehensive data protection requirements for all public and private entities processing personal data within Dominican territory. The law applies to government agencies, private companies across all sectors including finance, healthcare, telecommunications, and retail, as well as Credit Information Companies (Sociedades de Información Crediticia) that handle credit history data. The regulation covers the entire Dominican Republic and applies to any organization maintaining databases, public registries, or technical data processing systems containing personal information. Organizations face administrative sanctions for noncompliance, including fines ranging from 10 to 100 times the national minimum wage, and for serious violations, criminal penalties including imprisonment of six months to two years. The Superintendency of Banks is designated as the control body for Credit Information Companies under Article 29, though no equivalent authority exists for organizations outside the credit reporting sector. Kiteworks supports organizations working toward compliance with Law No. 172-13. Here's how:

Secure Personal Data in Transit and at Rest

Article 5 establishes that data controllers must implement technical, organizational, and security measures to safeguard personal data and prevent unauthorized alteration, loss, or access. Article 13 reinforces this requirement, mandating that organizations maintain information under necessary security conditions to prevent tampering, loss, or unauthorized consultation. Article 54 requires Credit Information Companies to present security manuals to the Superintendency of Banks detailing minimum security measures for data transport, physical security, logistics, and communications protection, while Article 63 requires SICs to adopt necessary security and control measures and protect their algorithms and technologies. Kiteworks deploys as a hardened virtual appliance containing all necessary files and software within multiple protection layers that minimize the attack surface. The platform implements double encryption for customer files at rest, encrypting both individual files and the underlying disk storage to protect against intruders who gain operating system access. For data in transit, Kiteworks employs TLS 1.2+ encryption protocols with AES-256 encryption by default.

Solution Highlights

- Strong double encryption
- TLS 1.2+ encryption
- Multi-factor authentication
- RBAC and ABAC access controls
- Comprehensive audit logs with SIEM integration
- Geofencing and data sovereignty controls

The embedded network firewall blocks all unused ports from outside traffic, while built-in F-Secure antivirus scanning quarantines malware on upload and download. Authentication mechanisms include credential-based authentication, certificate-based authentication (CBA), multi-factor authentication (MFA), and SAML 2.0 Single Sign-on integration with Microsoft Entra ID.

Manage Access Control and Data Subject Rights

Articles 8, 10, and 14 grant data subjects rights to access, rectify, update, and request deletion of their personal data, while Articles 11 and 12 establish specific procedures for Credit Information Companies to provide credit reports within five business days. Article 21 requires organizations to maintain proper tracking during habeas data proceedings. Article 13 mandates that access to information be restricted only to authorized persons. Kiteworks enables these requirements through its REST API, allowing organizations to develop custom applications for managing data subject requests and integrating with existing workflows. The System for Cross-domain Identity Management (SCIM) 2.0 compliance enables centralized account management through external Identity Management solutions, facilitating prompt updates and deletions. Secure Data Forms collects structured data while leveraging centralized security policies and unified audit logging. For access procedures, the platform generates unique HTTPS endpoints for each form instance, supporting both authenticated and unauthenticated public form submissions where configured. Role-based access control (RBAC) ensures AI operations inherit authenticated user permissions, preventing access beyond authorization levels. Attribute-based access control (ABAC) evaluates file attributes, user attributes, and contextual attributes to enforce fine-grained access decisions. The comprehensive audit log system automatically cleans, normalizes, standardizes, and aggregates all security and compliance-related activities into a single stream, with automatic tagging of data files as they enter the system through web uploads, email, APIs, or plugins.

Control Cross-Border Data Transfers

Article 6 (numeral 20) defines international data transfers as processing that involves transmission of data outside Dominican territory, while Article 6 (numerals 13 and 15) defines data importers and exporters. Article 80 establishes the conditions under which such transfers are permitted, including adequacy requirements for the recipient country and the data owner's free and conscious authorization. Article 27 establishes exceptions for health data processing and dissociation procedures. Kiteworks implements these controls through its Data Policy Engine, which enforces dynamic policies based on data asset attributes, sender and recipient user attributes, and user actions. For international transfers, the platform provides geofencing capabilities that restrict sign-ins based on geographic settings at individual user, profile, or system levels. The MFT Server connects to storage repositories, cloud file shares, and enterprise applications while supporting direct Kiteworks-to-Kiteworks integration that bypasses less secure intermediary protocols. For healthcare data under Article 27's medical cooperation exceptions, Kiteworks' Trusted Data Format (TDF) enables secure transfers between hospitals, clinics, researchers, and insurance companies while supporting HIPAA-aligned controls through OpenTDF-based persistent encryption and ABAC. This provides persistent encryption with embedded attribute-based access control policies, enabling senders to define access based on security clearance, organizational affiliation, location, or operational role. For financial transfers, TDF secures financial transaction data, records, and audit logs between institutions, regulators, and partners with granular control. The platform's audit logs maintain privacy standards while allowing administrator review when detailed verification is required.

Kiteworks provides organizations with comprehensive capabilities to address Law No. 172-13's multifaceted requirements across data protection, access control, and transfer management. For protection obligations, the platform delivers hardened security through double encryption at rest, TLS encryption in transit, and multi-factor authentication including biometric options required for Credit Information Companies.

For control requirements, Kiteworks enables data subject rights through REST APIs and SCIM 2.0 integration while enforcing granular access through RBAC and ABAC frameworks with comprehensive audit logging. For cross-border processing, the platform implements geofencing, secure international transfers via MFT Server, and Trusted Data Format encryption with embedded access policies for healthcare and financial data exchanges. Through this unified platform approach, Kiteworks empowers organizations across Dominican Republic's public and private sectors to maintain compliance while securely managing personal data throughout its life cycle.