Kiteworks

COMPLIANCE BRIEF

Support for Compliance With Colombia's Personal Data Protection Law

How Kiteworks Addresses the Security, Governance, and Accountability Requirements of Law 1581 of 2012

Colombia's Law 1581 of 2012 establishes a comprehensive personal data protection framework that governs how public and private entities collect, store, process, and circulate personal data, anchoring these obligations in the constitutional right to habeas data under Article 15 of the Colombian Constitution. The law applies to any entity processing personal data within Colombian territory, as well as foreign controllers and processors subject to Colombian jurisdiction through international agreements. It impacts all sectors of the Colombian economy, including financial institutions, commercial enterprises, healthcare providers, and government agencies that maintain personal databases. Entities had six months from the law's October 2012 promulgation to adapt their operations, with regulatory decrees issued in 2013 and 2015 further defining compliance obligations. Organizations that fail to comply face fines up to 2,000 monthly minimum wages, suspension of data processing activities for up to six months, and permanent closure of operations involving sensitive data. Kiteworks provides organizations with the technical controls and governance capabilities to assist in meeting Law 1581's requirements. Here's how:

Security Measures for Personal Data Integrity

Law 1581 requires data controllers and processors to apply the technical, human, and administrative measures necessary to prevent adulteration, loss, unauthorized consultation, and fraudulent access to personal data, as established under the security principle in Article 4(g) and the duty provisions of Articles 17 and 18. Kiteworks addresses these requirements through its hardened virtual appliance, which secures the underlying server infrastructure against external attack and misconfiguration, and double encryption at rest, which ensures that stored personal data remains unreadable without proper authorization. Each Kiteworks Secure Data Form automatically creates an associated secure shared folder, so that personal data submitted through the form is protected from the moment of collection. Kiteworks' Trusted Data Format (TDF) wraps sensitive data in persistent encryption and access controls that travel with the file regardless of where it is stored, shared, or processed, enforcing automatic data expiration policies and maintaining embedded audit trails that log all access attempts against protected content.

Solution Highlights

- Hardened virtual appliance
- Strong double encryption
- RBAC and ABAC
- Secure data forms
- Compliance audit logs

Governance of Personal Data Access and Circulation

The law additionally establishes that personal data may circulate only to authorized parties, that Data Subjects retain the right to know, update, and rectify their information, and that processing must serve a defined legitimate purpose as governed by Articles 4(b), 4(c), 8, 13, and 17. Data Controllers must restrict access to unauthorized persons and supply information to Data Subjects upon consultation request within 10 business days. Kiteworks supports these obligations through the Data Policy Engine (DPE), which enforces RBAC permissions that define which users may view, download, or collaborate on data stored in secure shared folders. ABAC risk policies apply dynamic access decisions based on file attributes, user department, and geographic context, ensuring personal data does not reach unauthorized parties. Kiteworks Secure Data Forms apply built-in field validation — enforcing email format, date range, numeric input, and file type rules — to ensure that only complete, accurate data enters the system, directly supporting the truthfulness and quality requirements of Article 4(a).

Audit, Retention, and Data Subject Rights Documentation

Data controllers and processors are required to maintain verifiable records of authorizations, process data subject consultations and claims within defined time frames, and demonstrate compliance with data quality and life-cycle obligations under Articles 7, 15, 17(b), 17(k), 18(f), and 19A. Organizations must keep proof of consent and evidence of their compliance measures so that regulators may audit these records during investigations. Kiteworks audit logs capture all user activity against personal data stored in the platform, creating a traceable record of who accessed, downloaded, or modified each file. Each form submission generates both a human-readable PDF and a machine-readable CSV file stored in the form's secure shared folder, producing structured documentation that supports data subject consultations and authorization verification requests. Persistent TDF encryption embeds audit trail metadata directly within protected files, ensuring access records travel with the data and remain available for regulatory review.

Kiteworks equips organizations operating under Colombia's Law 1581 of 2012 with the technical and operational controls needed to meet the law's security, governance, and accountability requirements across every stage of personal data processing. The platform's hardened virtual appliance and encryption architecture protect personal data at rest and in transit, while the Data Policy Engine applies role-based and attribute-based access controls that enforce the law's restricted circulation requirements. Secure Data Forms capture complete data and immediately place it under governed folder controls, supporting the quality principles that Law 1581 mandates from the point of collection. Comprehensive audit logs and structured submission records give data controllers and processors the verifiable documentation that regulators expect when assessing compliance with authorization, consultation, and claims-handling obligations.