Kiteworks

COMPLIANCE BRIEF

Kiteworks Helps Private Organizations Meet Mexico's LFPDPPP

Support for Data Protection, Consent Management, and Regulatory Accountability Under Mexico's Federal Privacy Law

Mexico's Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP), published March 20, 2025, establishes a comprehensive framework governing how private organizations collect, process, store, and transfer personal data. This law applies across all of Mexico and affects every private sector organization, including companies in financial services, healthcare, technology, retail, and any industry that processes personal data of Mexican residents. The law took effect immediately upon publication, with a November 14, 2025, reform aligning procedural provisions with Mexico's National Code of Civil and Family Procedures. Organizations that fail to comply face financial penalties reaching up to 640,000 times the Unit of Measure and Update for sensitive data violations, criminal prosecution carrying up to 10 years of imprisonment for offenses involving sensitive personal data, and civil liability claims from affected individuals. Kiteworks enables organizations to meet LFPDPPP requirements through secure data management capabilities. Here's how:

Data Protection and Security Measures

Mexico's LFPDPPP requires every controller to establish and maintain administrative, technical, and physical security measures that protect personal data against damage, loss, alteration, destruction, and unauthorized access or processing. Articles 18 and 13 mandate that these measures meet no lower standard than those the controller applies to its own information. Kiteworks addresses this requirement through its hardened virtual appliance architecture, which layers multiple security controls including an embedded network firewall, an embedded Web Application Firewall (WAF), file and disk double encryption using AES-256, and TLS 1.3 encryption in transit. Role-based access control and attribute-based access control enforce fine-grained access decisions based on user attributes, file classification, and contextual factors including location and device. An intrusion detection system monitors for advanced persistent threats, and comprehensive audit logs feed continuously to SIEM systems for forensic analysis and real-time incident detection.

Solution Highlights

- **Hardened virtual appliance architecture**
- **Role-based and attribute-based access control**
- **File expiration and retention controls**
- **SafeVIEW**
- **Comprehensive audit logs and SIEM integration**
- **Strong double encryption**

Consent Management and Access Control

The LFPDPPP requires controllers to obtain and manage data subject consent precisely, including establishing mechanisms that allow consent revocation at any time without retroactive effect under Article 7. When a data subject withdraws consent, the controller must cease processing. Kiteworks supports this requirement through several standard platform controls. Administrators can revoke user access to shared folders and files immediately by removing user permissions through role-based access controls, with access changes reflected in real time. Time-based expiration controls automatically terminate file and folder access after administrator-defined dates, and geofencing restricts access based on a user's current geographic location. For email-based data sharing, Kiteworks enables senders to withdraw protected email attachments and message bodies after sending via webmail, supporting revocation obligations across both individual and shared mailboxes.

Data Retention and Tracking

Articles 10 and 32 of the LFPDPPP require controllers to keep personal data accurate and updated, delete data once it no longer serves its stated purpose, and ensure data subjects can access their information in a usable format. Controllers must also delete data related to contractual breaches within 72 months. Kiteworks addresses retention and access tracking requirements through configurable file expiration controls that automatically delete files after a set number of days or upon folder expiration, with folder owners able to set manual expiration dates within administrator-defined limits. For access fulfillment under Article 32, Kiteworks SafeVIEW provides controlled view-only access to files without enabling editing, copying, or download beyond watermarked versions, creating a documented access event that supports ARCO right fulfillment and compliance audit requirements.

Kiteworks provides private sector organizations with a technically rigorous compliance platform that addresses LFPDPPP obligations across data protection, consent management, retention, and access control. Rather than requiring organizations to assemble multiple disconnected tools, Kiteworks delivers layered security architecture, dynamic policy enforcement, and granular access management within a single hardened environment. Organizations gain the ability to respond to data subject rights requests, enforce data life-cycle policies, and maintain continuous audit documentation that demonstrates regulatory accountability to the Secretariat of Anti-Corruption and Good Governance. As Mexico's enforcement mechanisms carry significant financial penalties and criminal exposure for violations involving sensitive personal data, Kiteworks equips compliance teams with the technical controls and audit evidence needed to meet LFPDPPP obligations with confidence.