Kiteworks

COMPLIANCE BRIEF

Kiteworks Enables Support for Paraguay's Personal Data Protection Law (Law No. 7593/2025)

How Kiteworks Helps Organizations Operationalize Paraguay's Data Protection Obligations Before the November 2027 Compliance Deadline

Paraguay's Law No. 7593/2025 on Personal Data Protection in the Republic of Paraguay, promulgated on November 27, 2025, establishes comprehensive data protection requirements that take effect 24 months (November 2027) from official publication. The law applies cross-sectorally to public and private controllers and processors, regardless of industry, including (illustratively) healthcare, finance, telecommunications, retail, education, and public administration. The regulation covers any processing of personal data within Paraguay's jurisdiction and includes provisions for international data transfers, requiring adequate protection levels for cross-border data flows. While the law establishes the National Agency for the Protection of Personal Data as the supervisory authority -- a deconcentrated unit within the Ministry of Information and Communication Technologies with functional autonomy (Article 34), headed by a Director General and Deputy Director appointed by Executive Decree from a shortlist proposed by MITIC after public competition (Article 37) -- with powers to impose administrative sanctions including warnings, fines ranging from 20 to 2,500 minimum daily wages for general violations (Article 46), up to 5,000 minimum daily wages for violations involving sensitive data, and up to 10,000 minimum daily wages for violations involving sensitive data of children and adolescents, as well as suspension of data processing activities, specific monetary penalties vary based on violation severity and other factors outlined in Article 47. Fines are calculated in jornales mínimos (minimum daily wages), set periodically by MTESS resolution at ₲ 111,502 as of July 2025 under MTESS Resolution 677/2025. Kiteworks supports organizations working toward compliance with Law No. 7593/2025. Here's how:

Securing Personal Data Against Unauthorized Access and Breach

Articles 4 and 16 mandate technical and organizational measures to prevent data breaches, requiring controllers to periodically implement and monitor security safeguards that protect against unauthorized access, alteration, or loss of personal data. Article 9 further requires data controllers to demonstrate compliance through appropriate security controls based on processing risks. Article 22 specifically addresses video surveillance data, establishing that recordings containing evidence of acts against the integrity of persons or property must be provided to competent authorities within 72 hours of becoming aware of their existence.

Solution Highlights

- Hardened virtual appliance with double encryption
- Data Policy Engine with ABAC and RBAC
- Data sovereignty and geofencing
- Comprehensive audit logs with SIEM integration
- OpenTDF Standard Implementation
- Time-based retention and expiration controls
- Secure Data Forms

Kiteworks addresses these protection requirements through its hardened virtual appliance deployment model with multiple defense layers including double encryption that encrypts customer files at rest to minimize attack surfaces. The platform implements enterprise-grade encryption standards through its embedded network firewall blocking unused ports and embedded web application firewall providing automated protection against web-based threats. For persistent data protection, Kiteworks implements the OpenTDF Standard providing strong encryption with embedded attribute-based access control policies that remain with the data throughout its life cycle. The platform's comprehensive DevSecOps practices include shift-left security testing and one-click updates for maintaining current security patches, while risky settings detection alerts administrators to potential security misconfigurations requiring remediation.

Permissions, Cross-Border Transfers, and Data Sovereignty

Articles 19 and 25 establish strict requirements for international data transfers and data exchanges between public institutions, mandating adequate protection levels for cross-border flows and legitimate purposes for inter-agency data sharing. Articles 23, 24, and 30 require specific controls: Article 23 governs processing of data on criminal matters; Article 24 addresses the balance between public information access and data protection; and Article 30 establishes the right of data subjects to object to processing for reasons related to their particular situation. Articles 4, 6, and 7 mandate privacy-by-design principles, transparent consent mechanisms, and special protections for children's data. Kiteworks enforces these control requirements through the Data Policy Engine (DPE) combining ABAC runtime policies and RBAC controls that govern access based on user roles, data attributes, and contextual factors. The platform's data sovereignty capabilities restrict data storage and routing to assigned geographic locations through LDAP or SAML attributes, while geofencing controls limit access based on user location determined by IP address. For consent management, Secure Data Forms enables organizations to collect structured data with configurable authentication requirements and terms of service policies that users must accept before accessing protected data. The platform enforces the principle of least privilege, with users receiving only necessary permissions through assigned profiles and explicit data invitations.

Audit Logging, Retention, and Data Subject Rights

Article 17 requires breach notification to supervisory authorities within 72 hours, necessitating comprehensive incident detection and reporting capabilities. Article 4 establishes principles of data minimization and limited retention periods, requiring data to be kept only as long as necessary for processing purposes with deadlines to be established by the supervisory authority. Articles 27, 28, and 33 grant data subjects specific rights: Article 27 establishes the right to information about how data is processed; Article 28 provides the right to access personal data and obtain copies; and Article 33 establishes the right to review and challenge automated decisions affecting their interests. Kiteworks fulfills these tracking obligations through comprehensive audit logs feeding real-time data to SIEM systems including QRadar, LogRhythm, ArcSight, and Splunk via syslog for immediate threat detection and regulatory reporting. The platform provides Threat Intelligence Notifications alerting administrators to security risks in real time through admin console banners. For retention compliance, time and expiration controls automatically delete files and folders after configured periods while maintaining anonymized audit logs that protect privacy through UUID substitution. End-users access tracking information through the information and tracked activity pane showing who accessed their data and what actions were performed, with exportable audit logs including timestamps for all file and email interactions across internal and external users.

Kiteworks addresses Law No. 7593/2025's multifaceted requirements through integrated capabilities spanning the regulation's three core compliance domains. For data protection obligations under Articles 4, 9, and 16, Kiteworks deploys hardened virtual appliances with double encryption, embedded firewalls, and OpenTDF Standard implementation to safeguard personal data against unauthorized access and breaches. To meet access control mandates in Articles 19, 23, 25, and 30, the platform enforces granular permissions through its DPE combining ABAC and RBAC controls, while data sovereignty features and geofencing restrict cross-border transfers and ensure appropriate jurisdictional controls.

For tracking and retention requirements outlined in Articles 17, 22, and 27-33, Kiteworks provides comprehensive audit logs with real-time SIEM integration, automated retention policies, and user-accessible activity tracking that enables both regulatory reporting and data subject rights fulfillment. As organizations prepare for the law's implementation within the 24-month transition period, Kiteworks delivers a unified platform that transforms Paraguay's complex data protection obligations into operationalized security controls, positioning enterprises to meet their compliance deadlines while maintaining secure collaboration across all regulated data exchanges.