Kiteworks

COMPLIANCE BRIEF

Protecting Personal Data in Chile With Kiteworks

Kiteworks Helps Organizations Meet the Requirements of Law 21.719

Chile's Law No. 21.719 establishes a personal data protection framework that governs how natural and legal persons, including public bodies, collect, process, store, and share personal data of identified or identifiable individuals. The law applies to any entity processing data of persons located in Chile, regardless of where the controller operates, extending its reach globally to organizations offering goods or services to Chilean residents or monitoring their behavior. All industry sectors face compliance obligations, from financial services and healthcare to technology companies and public institutions. The law enters into force on December 1, 2026, 24 months after its publication in Chile's Diario Oficial on December 13, 2024. Organizations that fail to comply face fines up to 20,000 monthly tax units for very serious violations, operational suspensions, and civil liability for damages caused to data subjects. Kiteworks provides organizations with the secure content communication capabilities needed to meet Law 21.719's requirements. Here's how:

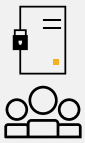
Hardened Virtual Appliance and Encryption for Data Security

Law 21.719 establishes in Articles 3(f), 14(4), and 14(5) that controllers must apply appropriate technical and organizational measures ensuring the confidentiality, integrity, availability, and resilience of processing systems, protecting personal data against unauthorized access, destruction, loss, leakage, or accidental alteration. These measures must account for the nature of the data processed and the probability and severity of risk. Kiteworks addresses these obligations through its hardened virtual appliance, which delivers a purpose-built, enterprise-grade server infrastructure with an embedded zero-maintenance network firewall, Web Application Firewall (WAF), and multiple intrusion detection layers. Double encryption at rest ensures stored personal data remains protected against unauthorized access or tampering, while TLS Certificate Validation secures data in transit by terminating connections that fail certificate verification. Each Kiteworks Secure Data Forms automatically associates with a secure shared folder governed by the platform's centralized security policies, protecting submitted personal data from the point of collection through the full data life cycle.

Solution Highlights

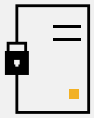
Hardened virtual appliance

TLS certificate validation



Data Policy Engine with ABAC

Role-based access control



Secure Data Forms

Compliance audit log with SIEM integration

Data Policy Engine and RBAC for Access Governance

Controllers are required to apply privacy-by-design and privacy-by-default measures under Article 14(4), process only data strictly necessary for each specific purpose, implement mechanisms enabling data subjects to exercise their rights under Article 10, and enforce consent and purpose limitations governing data assignment under Articles 15 and 15(2). Controllers that fail to restrict processing to authorized purposes or that carry out assignment without required consent face serious infringement classification under Article 34(3). Kiteworks supports these requirements through the Data Policy Engine (DPE), which allows administrators to centrally define attribute-based access controls (ABAC) — known as risk policies — across all data exchange channels. These runtime policies evaluate data file attributes, user attributes, and requested actions simultaneously to enforce purpose-limited access. Role-based access control (RBAC) restricts folder access to defined user profiles, while the DPE's folder invitation policies govern data sharing and transfer permissions. The machine-readable CSV export generated by each Secure Data Forms supports data portability requests under Article 9, enabling structured, operable delivery of personal data to subjects upon request.

Compliance Audit Log and SIEM Integration for Breach Readiness

Law 21.719 requires controllers under Article 14(6) to report security breaches to the Personal Data Protection Agency without undue delay when there is reasonable risk to the rights and freedoms of data subjects, to maintain records describing the nature of each breach, categories of affected data, approximate number of subjects involved, and remediation measures taken. When breaches involve sensitive personal data or data of children under 14, controllers must also notify affected individuals directly. Kiteworks supports these obligations through its comprehensive compliance audit log, which captures and normalizes security- and compliance-related activity across the platform into a single, standardized data stream. Kiteworks can feed this audit log in real time to external SIEM systems via syslog, enabling security teams to detect anomalous activity, generate breach documentation, and respond to Agency notification requirements. Each Secure Data Forms submission produces both a human-readable PDF and a machine-readable CSV record stored in the form's secure shared folder, providing structured evidentiary records that support subject notification and regulatory reporting obligations.

Kiteworks equips organizations with a unified platform designed to meet the technical and organizational demands of Chile's Law 21.719. Its hardened virtual appliance and layered encryption architecture directly address the security principle obligations that the law establishes for controllers and processors alike. The Data Policy Engine enforces data limitation and access governance at runtime, ensuring that personal data flows only to authorized parties for authorized purposes. Secure Data Forms captures structured, machine-readable records from the point of collection onward. The compliance audit log and real-time SIEM integration give security teams the breach detection and documentation capabilities that the notification obligations demand. Taken together, these capabilities allow organizations to demonstrate accountability to the Personal Data Protection Agency with confidence and precision.