Kiteworks

COMPLIANCE BRIEF

Your Data, Brazil's Rules: Building LGPD Compliance With Kiteworks

How Controllers and Processors Can Meet Brazil's Most Comprehensive Data Protection Law Across Every Stage of the Data Life Cycle

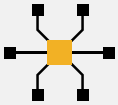
Brazil's Lei Geral de Proteção de Dados (LGPD), Law No. 13,709 enacted August 14, 2018, establishes a comprehensive personal data protection framework that applies to any organization processing the data of individuals located in Brazil, regardless of where that organization maintains its headquarters or where it stores its data. The law covers all sectors, including private companies, public bodies, financial institutions, healthcare providers, and research organizations, creating universal compliance obligations across industries. The National Data Protection Authority (ANPD) began enforcing administrative sanctions on August 1, 2021, and actively issues binding regulations. Noncompliant organizations face fines up to 2% of their Brazil-based revenue per infraction, capped at R$50,000,000, plus potential suspension or prohibition of data processing activities. Kiteworks equips controllers and processors with the technical and organizational capabilities required to satisfy the LGPD's core requirements. Here's how:

Technical Security and Data Protection

Brazil's LGPD places comprehensive security obligations on both controllers and processors under Articles 46 and 47, requiring technical and administrative measures to protect personal data from unauthorized access, destruction, loss, alteration, and improper processing. These obligations extend through the entire data life cycle, including after processing concludes, and Article 44 establishes liability for any failure to meet the security standard that data subjects reasonably expect. Kiteworks addresses these requirements through multiple layered technical controls. The platform's RBAC and ABAC Governance Controls evaluate file attributes, user clearance levels, and contextual factors in real time to enforce granular access decisions for every operation. Kiteworks applies TLS certificate validation and terminates connections that fail verification, blocking interception attacks. The Data-Centric Security Model binds protection to the data itself rather than infrastructure, ensuring security persists regardless of where data is stored or processed. Kiteworks applies AES-256 encryption for data at rest and TLS for encryption in transit.

Solution Highlights

RBAC and ABAC governance controls



Data-centric security model

Strong double encryption

Lawful Processing Controls and Purpose Limitation

Brazil's LGPD establishes strict requirements governing the lawful bases for personal data processing under Articles 7 through 10, requiring controllers to obtain specific, informed consent and process data only for explicitly defined purposes. Article 8 requires controllers to prove consent was properly obtained, while Articles 15 and 16 mandate that data processing ceases when its purpose concludes and that data is erased following termination. Kiteworks supports these control requirements through its Automatic Secure Shared Folder Storage, which uses the Kiteworks Data Policy Engine to set role-based access control permissions at the point of data collection, ensuring data flows only to authorized parties for defined purposes. The platform protects stored data through a hardened virtual appliance with double encryption at rest. Machine-readable CSV records and Downstream Workflow Enablement through folder sharing, email, MFT, SFTP, APIs, and MCP support structured data life-cycle management aligned to the law's processing purpose and termination requirements.

Transparency, Data Subject Rights, and Processing Records

Brazil's LGPD grants data subjects broad rights under Articles 18 and 19, including confirmation of processing existence, data access, correction of inaccurate data, erasure, portability, and consent revocation, with controllers required to respond within regulatory timelines. Article 37 requires controllers and processors to maintain records of all processing operations, and Article 9 requires controllers to make processing information clearly accessible to data subjects at the time of collection. Kiteworks supports these tracking requirements through several documented capabilities. The User Context and Authentication feature of the MCP Server provides verified access to authenticated user profiles, roles, and permission context, supporting transparent and traceable data interactions. Each form submission generates both a human-readable PDF and a machine-readable CSV record stored in a secure shared folder, creating auditable processing records that satisfy Article 37. The Downstream Workflow Enablement capability supports data portability requests through folder sharing, email, MFT, SFTP, and APIs.

Kiteworks gives organizations subject to Brazil's LGPD an integrated platform that addresses the law's three core compliance domains through a unified architecture designed for the full data processing life cycle. By combining persistent data-centric security with granular governance controls and comprehensive processing records, Kiteworks enables both controllers and processors to demonstrate the technical and organizational measures the ANPD requires. Organizations can show regulators that access decisions enforce purpose limitations, that security controls persist beyond infrastructure boundaries, and that processing records exist to support data subject rights requests. The platform's approach directly reduces the risk of the fines, suspension orders, and public disclosure penalties that the law authorizes. Controllers and processors that deploy Kiteworks gain a foundation that supports proactive compliance across the LGPD's requirements rather than reactive responses to enforcement actions.