Kiteworks

COMPLIANCE BRIEF

Kiteworks Enables Kazakhstan Personal Data Law Compliance

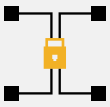
Address Data Encryption, Access Governance, and Audit Documentation Under Kazakhstan's Personal Data Protection Framework

Kazakhstan's Law on Personal Data and Their Protection, dated 21 May, 2013 (as amended through 2025), establishes comprehensive data protection requirements for controllers and processors operating within Kazakhstan, including state bodies, private companies, and third-party data handlers. The law applies to organizations collecting or processing personal data within Kazakhstan's territory, though it excludes certain activities such as personal and family needs, archive documents, state secrets, and intelligence operations. Organizations face responsibility for noncompliance under the Laws of the Republic of Kazakhstan, with enforcement through the authorized body (central executive body responsible for supervising the personal data protection field) and local executive authorities responsible for overseeing data protection compliance. The law mandates strict controls over personal data collection, processing, storage within Kazakhstan borders, consent management, cross-border transfers, and subject rights including access to information and requirements for correction, blocking, and deletion within one business day. Kiteworks supports organizations working toward compliance with Kazakhstan's Personal Data Law. Here's how:

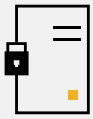
Data Encryption and Security Obligations

Kazakhstan's Personal Data Law requires comprehensive protection measures under Article 22 (as amended through 2023), which mandates prevention of unauthorized access, timely detection of unauthorized access attempts, and minimization of adverse consequences from security incidents. Article 23 requires protection of electronic information resources containing personal data in compliance with the legislation on informatization. The Kiteworks platform addresses these protection requirements through multiple layers of security. The system employs AES-256 file and disk double encryption at rest to safeguard stored data, while TLS 1.3 and 1.2 protocols protect data in transit. The hardened virtual appliance architecture incorporates an embedded network firewall that blocks all unused ports, an embedded Web Application Firewall (WAF) with automated rules updates, and Zero-Trust Mode that blocks all IP addresses by default except those explicitly allowed. AI-based intrusion and anomaly detection maintains an evolving library of patterns to identify suspicious activities, with all intrusion attempts and detected anomalies logged for security analysis.

Solution Highlights



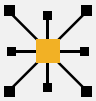
AES-256 double encryption



Data Policy Engine with ABAC and RBAC

Data sovereignty and geofencing

Comprehensive audit logging



Real-time SIEM integration

Automated data modification and blocking

Trusted Data Format revocation

The platform provides REST API access and Node Health API endpoints for system monitoring, enabling implementation of security measures while maintaining data protection through comprehensive audit logs that feed real-time to SIEM systems including QRadar, LogRhythm, ArcSight, and Splunk.

Access Governance and Cross-Border Controls

Articles 7 and 8 establish strict consent requirements for personal data collection and processing, including consent given in writing, via a state service, a non-state service, or in another manner enabling confirmation of consent, with specific content requirements. Article 10 mandates that access be determined by consent conditions, while Article 16 specifically governs cross-border transfers requiring protection equivalent to Kazakhstan law. Article 12 requires data storage within Kazakhstan territory with retention periods determined by the date of achievement of purposes of collection and processing. The Kiteworks platform implements comprehensive access governance through its Data Policy Engine (DPE), which combines role-based access control (RBAC) and attribute-based access control (ABAC) frameworks. RBAC assigns permissions based on predefined roles—owner, manager, collaborator, downloader, and viewer—while ABAC enables dynamic policies based on data attributes, user attributes, and actions taken. For cross-border compliance under Article 16, the platform's Data Sovereignty feature configures distributed systems to store users' data only in their assigned country, with geofencing controls that restrict sign-ins based on IP addresses at user, profile, or system levels. OAuth 2.0 authentication with refresh token support ensures secure authorization, while Secure Data Forms enables configurable authentication options for data collection. The platform enforces time-based access controls and folder expiration policies, with administrators able to block or require approval for folder member invitations.

Audit Documentation and Subject Rights

Article 25 requires organizations to provide information to individuals upon request within time frames stipulated by legislation and to execute specific actions within one business day, including changing or supplementing personal data based on relevant documents, blocking data when violations are detected, destroying illegally collected data, and notifying the competent authority about security breaches. Article 24 grants subjects rights to information about their data processing, while Articles 18 and 19 establish requirements for data destruction and transfer notifications. The Kiteworks platform fulfills these tracking obligations through its consolidated audit logging system that appends all activities to a single log with consistent formatting and terminology. The comprehensive audit documentation covers 632 events across 22 categories, tracking all user authentication attempts, file and folder access, permission changes, and administrative actions. For subject rights management, the Information & Tracked Activity Pane provides end-users with direct visibility into their data interactions, showing who accessed files or folders and what actions were taken. The platform supports rapid response to subject requests through SCIM-compliant APIs for data updates and Time and Expiration policies for automated data retention and deletion. Legal hold and eDiscovery access controls enable compliance with court-ordered data preservation, while compliance reporting capabilities generate regulation-specific reports for GDPR, HIPAA, and CMMC 2.0, with role-based access ensuring appropriate data visibility. Real-time SIEM integration ensures continuous monitoring and rapid incident response, while the platform's tracking features enable organizations to demonstrate compliance with Kazakhstan's requirements for data modification, blocking, and destruction under Article 25.

Kiteworks delivers comprehensive technical controls that enable organizations to work toward compliance with Kazakhstan's Personal Data Law through a unified platform approach. For data encryption and security obligations, the platform provides multi-layered protection including AES-256 double encryption, hardened virtual appliance architecture, AI-based intrusion detection, and real-time SIEM integration to fulfill Article 22's prevention and detection requirements. For access governance and cross-border controls, Kiteworks implements RBAC and ABAC frameworks through its Data Policy Engine, enforces data sovereignty with geofencing controls for Article 16 cross-border transfer requirements, and provides infrastructure that supports organizations' consent workflow implementation.

For audit documentation and subject rights, the platform maintains comprehensive logging of 632 event types, provides end-user visibility through tracked activity interfaces, and supports Article 25's one-business-day requirements for data changes, blocking, and destruction through SCIM APIs and automated retention policies. By consolidating data protection, access control, and compliance tracking into a single secure content platform, Kiteworks positions organizations to meet Kazakhstan's stringent personal data protection requirements while maintaining operational efficiency across their data governance programs.