Kiteworks

COMPLIANCE BRIEF

Supporting Compliance With Qatar's Personal Data Privacy Protection Law

Kiteworks' Comprehensive Solution for Secure Data Management and Governance

Qatar's Personal Data Privacy Protection Law No. 13 of 2016 establishes a comprehensive framework to safeguard personal data in the country. This law protects individuals' privacy rights while allowing legitimate data processing activities. It applies to electronically processed personal data, data prepared for electronic processing, or data processed through a combination of electronic and traditional methods. The law impacts all industries in Qatar that process personal data electronically, including healthcare, finance, telecommunications, e-commerce, and social media platforms. It also affects international companies engaged in cross-border data flows with Qatar. Organizations had to comply with the law by 2017, with possible extensions granted by the Council of Ministers. Noncompliance carries significant risks, including penalties up to 5 million Qatari Riyals (approximately $1.37 million), reputational damage, loss of customer trust, and potential legal action from affected individuals. Kiteworks offers a comprehensive solution to help organizations meet the requirements of Qatar's Personal Data Privacy Protection Law through its secure file sharing and governance platform. Here's how:

Rights of Individuals: Empowering User Control With Consent Management and Audit Logs

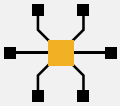
Chapter 2 of Qatar's Personal Data Privacy Protection Law focuses on individuals' rights regarding their personal data. It requires transparent, honest, and respectful data processing, empowering individuals to control their information. The law grants rights to consent, withdraw consent, object to unnecessary processing, request data erasure or correction, access personal data, and obtain copies for a fee. Organizations must implement technical controls to manage these rights effectively throughout the data life cycle.

Kiteworks' comprehensive audit logs and SIEM feeds track all data processing activities, including user consent actions. Granular access controls enable organizations to require explicit consent for data processing, while content-based policies enforce specific data type requirements. The platform's user self-service capabilities allow individuals to manage their consent preferences and request data corrections. File expiration settings support data erasure requirements. Automated notifications can alert users to data disclosures or inaccuracies. Secure file sharing features enable safe distribution of personal data copies upon request.

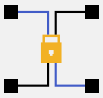
Solution Highlights

Granular access controls

Comprehensive audit logs



SIEM integration



Strong encryption

These functionalities collectively ensure that organizations can effectively manage consent, data access, correction, and erasure requests in line with the law's requirements.

Controller and Processor Liabilities: Secure Data Handling With Encryption and Audit Capabilities

Chapter 3 defines the responsibilities of data controllers and processors. It requires honest data processing, robust security measures, and strict adherence to privacy policies. The law mandates informing individuals about data processing details, ensuring data accuracy, implementing complaint management systems, and reporting breaches. It also emphasizes regular audits, staff training, and technologies that enable individual data rights.

The platform's hardened virtual appliance design, coupled with strong encryption and granular access controls, ensures legitimate data processing. Content-based risk policies and DevSecOps practices enable careful control design in data processing systems. Extensive audit logs, reporting capabilities, and file expiration settings verify data relevance, accuracy, and timely deletion. The system offers web forms and data correction request features to support individual rights. Kiteworks' breach detection and reporting capabilities, integrated with SIEM systems, facilitate effective breach notification. Secure file transfer protocols and DLP integration ensure lawful data disclosure and transfer. These features provide the necessary technical controls to protect personal data.

Special Nature Data Protection: Safeguard Sensitive Information via Risk Policies and Consent Workflows

Handling of sensitive personal data, including information related to ethnicity, children, health, religion, and criminal records, is paramount within Chapter 4. It requires stringent protection measures, including obtaining permission from the Competent Department before processing such data. The law emphasizes robust safeguards for children's data, mandating explicit guardian consent, transparency in data usage, and the right to request data deletion.

Kiteworks provides secure web forms for transparently collecting consent from parents for use of their child's information. Custom branding and text explain data practices and uses. Web forms sent to authenticated parent users then capture verified consent or non-consent for collecting and sharing data. Once consent is captured, parents can access, export, or delete their child's information anytime. Comprehensive audit logs create immutable records of all submission, access, and deletion activity for compliance reporting. Configurable notifications also alert designated staff of form submissions so they can take immediate action. Together, Kiteworks' encrypted web forms, access controls, detailed activity logs, and notifications empower organizations to provide the parental transparency, consent, and ongoing control over special nature data. Web forms give clear notice, capture affirmative consent, and enable access and deletion rights, while logs create records to demonstrate compliance.

Kiteworks provides a comprehensive solution for organizations seeking to comply with Qatar's Personal Data Privacy Protection Law. The platform's robust features address key requirements across individual rights, controller and processor liabilities, and special nature data protection. Through its advanced encryption, granular access controls, and content-based risk policies, Kiteworks ensures secure data processing and storage. The platform's audit logs, SIEM integration, and reporting capabilities enable thorough monitoring and breach detection. Web forms and workflow capabilities empower individuals to manage their data rights effectively. Kiteworks' flexible system allows organizations to adapt to specific exemptions while maintaining compliance. By implementing Kiteworks, organizations can confidently navigate the complex landscape of data protection in Qatar, mitigating risks and safeguarding personal information in line with the law's stringent requirements.