

# Enabling Compliance With the Saudi Personal Data Protection Law

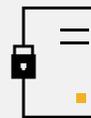
**Leverage Kiteworks' Features for Consent Management, Data Security, and Data Minimization to Ensure Compliance With the PDPL**

The Saudi Data & AI Authority (SDAIA) introduced the Personal Data Protection Law (PDPL) in September 2021, which came into effect on March 23, 2022. This comprehensive legislation aims to regulate the processing of personal data within Saudi Arabia and protect the privacy rights of individuals residing in the country. The PDPL applies to any entity, whether public or private, that processes personal data related to individuals in Saudi Arabia, regardless of the entity's location. Key principles include lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality. Data controllers must obtain explicit consent, grant data subject rights, appoint Data Protection Officers when necessary, and conduct Data Protection Impact Assessments for high-risk processing activities. The PDPL also regulates cross-border data transfers and imposes significant penalties for noncompliance. Organizations operating in Saudi Arabia or processing data related to Saudi residents must review and update their data protection policies, procedures, and practices to ensure compliance with the PDPL.

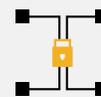
## Empowering Consent Management and Data Subject Rights

Consent management and data subject rights are central to the Saudi Data & AI Authority PDPL, and the Kiteworks platform provides a range of features to help entities comply with these requirements. Article 5 of the PDPL states that personal data cannot be processed or have its purpose changed without the explicit consent of the data subject, and Kiteworks' secure web forms and data collection mechanisms enable organizations to obtain this consent while clearly communicating the purpose of data collection (Article 13). These customizable forms allow entities to include relevant legal disclaimers, privacy policies, and hyperlinks to additional information, ensuring that data subjects are fully informed before providing their consent (Article 12). Additionally, Kiteworks empowers data subjects to exercise their rights under Article 4 of the PDPL, such as the right to access, rectify, and erase their personal data. The platform's features allow data subjects to request the deletion of their personal information, which is then securely removed from the system (Article 15). Kiteworks also facilitates the correction, completion, and updating of personal data, with notifications to alert relevant parties of any changes (Article 17). The platform maintains a comprehensive audit log of all user activities, including data access, modification, and deletion, enabling organizations to demonstrate compliance with data protection regulations and support investigations related to data subject requests (Articles 21 and 31).

## Solution Highlights



**Secure web forms**



**Granular access controls**



**Encryption at rest and in transit**



**Detailed audit logs**

## Safeguard Personal Data via Access Control and Encryption

The PDPL places great emphasis on the importance of data security and protection. Article 19 requires controllers to implement necessary organizational, administrative, and technical measures to protect personal data, including during data transfers. Kiteworks employs strong encryption for data at rest and in transit, as well as a hardened virtual appliance with embedded firewalls and intrusion detection systems. The platform also maintains detailed audit logs to track user activity and data access, enabling the detection and investigation of unauthorized access (Article 19). In the event of a data breach or illegal access to personal data, Kiteworks' proprietary patterns can detect suspicious activities, allowing organizations to promptly identify and notify the Competent Authority and affected data subjects, as mandated by Article 20.

Kiteworks' advanced access control features, such as role-based access controls and least-privilege defaults, ensure that access to sensitive information, including health data (Article 23) and credit data (Article 24), is restricted to authorized users only. The platform's granular tracking capabilities empower organizations to maintain strict control over the copying of official documents where data subjects are identifiable, as stipulated in Article 28. When it comes to cross-border data transfers, Article 29 requires that there be an adequate level of protection for personal data outside the Kingdom. Kiteworks addresses this by utilizing a double encryption mechanism to protect data even in the event of a breach, demonstrating a commitment to maintaining an adequate level of protection for personal data during transfers. By leveraging Kiteworks' robust security features and detailed audit logs, entities can effectively safeguard personal data, detect and respond to security incidents, and demonstrate compliance with the data security and protection requirements of the PDPL.

## Verify Consent With Web Forms and Audit Logs

The PDPL also emphasizes the importance of data minimization and purpose limitation in protecting personal data. Article 11 states that the content of personal data collected should be appropriate and limited to the minimum amount necessary to achieve the purpose of collection. Kiteworks supports this principle by enabling organizations to restrict access to personal data to authorized individuals through its advanced access control features, such as role-based access controls and least-privilege defaults. Additionally, the platform ensures that data is securely destroyed when no longer needed, in line with Article 11's requirement to cease collection and destroy previously collected personal data when it is no longer necessary for the purpose for which it was collected. Kiteworks' secure deletion feature ensures that once a user deletes a file, it is permanently removed from the system, including all storage locations and backup systems, and cannot be recovered (Article 18).

Article 10 allows controllers to collect and process personal data for purposes other than those for which it was initially collected only under specific circumstances, such as obtaining the data subject's consent or when the data is not to be recorded or stored in a form that makes it possible to directly or indirectly identify the data subject. Kiteworks supports compliance with granular tracking capabilities, including its comprehensive audit log of all user activities. Article 31 obligates controllers to maintain records of their personal data processing activities, including the purpose of processing, categories of data subjects, and any cross-border data transfers. Kiteworks' detailed logging feature captures this essential information, allowing organizations to easily access and provide these records to the Competent Authority upon request, demonstrating their adherence to the PDPL's data minimization and purpose limitation principles. By utilizing Kiteworks' features for access control, secure deletion, granular tracking, and detailed logging, entities can ensure that they collect and process only the minimum amount of personal data necessary for the specified purpose, securely destroy it when no longer needed, and maintain accurate records of their data processing activities, ultimately achieving compliance with the PDPL's data minimization and purpose limitation requirements.

Kiteworks provides a robust platform for entities operating in Saudi Arabia to comply with the Personal Data Protection Law. By offering secure web forms for obtaining explicit consent, advanced access controls and encryption for data protection, and comprehensive audit logs for tracking data processing activities, Kiteworks empowers organizations to meet the key requirements. The platform's features enable companies to effectively manage consent, safeguard personal data, and adhere to data minimization and purpose limitation principles, ultimately reducing the risk of noncompliance and demonstrating a strong commitment to protecting the privacy rights of individuals in Saudi Arabia.