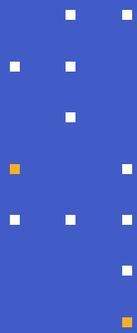


GUIDE

Kiteworks' Guide to the Saudi Arabia Data & AI Authority Personal Data Protection Law

**Navigating Compliance and Protecting
Privacy Rights in the Kingdom**





3 Introduction

4 The Kiteworks Secure File Sharing and Governance Platform

5 The Kiteworks Platform and Saudi Arabia Data & AI Authority Personal Data Protection Law

5 Articles 1-31

Introduction

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 data protection 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. Personal data is defined as any information that relates to an identified or identifiable natural person. The law covers various industries, including healthcare, finance, telecommunications, e-commerce, and any other sector that collects, stores, or processes personal data.

Under the PDPL, data controllers and processors must adhere to several key principles and regulations. These include lawfulness, fairness, and transparency in data processing; purpose limitation; data minimization; accuracy; storage limitation; integrity; and confidentiality. Data controllers are required to obtain explicit consent from data subjects for the collection and processing of their personal data, unless another legal basis applies. The law grants data subjects several rights, such as the right to access, rectify, and erase their personal data, object to processing, and data portability. Data controllers must respond to data subject requests within a specified time frame and provide clear information about their data processing activities. In certain cases, data controllers are obligated to appoint a Data Protection Officer (DPO) to oversee compliance with the PDPL and act as a point of contact for data subjects and the supervisory authority. Data Protection Impact Assessments (DPIAs) must be conducted for high-risk processing activities, and data breaches must be reported to the supervisory authority and affected data subjects within specified time frames.

The PDPL also regulates cross-border data transfers, allowing personal data to be transferred outside of Saudi Arabia only if the recipient country provides an adequate level of data protection or if other specified conditions are met. Special provisions apply to the processing of sensitive personal data, such as health data, biometric data, and data revealing religious or philosophical beliefs. Noncompliance with the PDPL can result in significant penalties and fines. The SDAIA has the power to impose fines of up to SAR 5 million (approximately USD 1.3 million) for violations of the law. In addition to financial penalties, noncompliant organizations may face reputational damage and loss of customer trust. To ensure compliance with the PDPL, organizations operating in Saudi Arabia or processing data related to Saudi residents must review and update their data protection policies, procedures, and practices. This may involve conducting data audits, implementing technical and organizational security measures, training employees, and establishing mechanisms for handling data subject requests and breaches.

This guide showcases how Kiteworks can support entities operating in Saudi Arabia that are working to comply with PDPL requirements to protect personal data.



SDAIA
الهيئة السعودية للبيانات
والذكاء الاصطناعي
Saudi Data & AI Authority

The Kiteworks Secure File Sharing and Governance Platform

Kiteworks' FedRAMP- and FIPS-140-2-compliant file sharing and governance platform enables public entities to share sensitive information quickly and securely while maintaining full visibility and control over their file sharing activities. The Kiteworks platform provides:

Secure File Sharing

Kiteworks is ISO 27001, ISO 27017, and ISO 27018 certified and enables public entities to access and share personal data securely, reducing the risk of data breaches, malware attacks, and data loss.

Governance and Compliance

Kiteworks supports the Saudi Data & AI Authority (SDAIA) Personal Data Protection Law (PDPL) compliance and provides comprehensive reports on file activity and access.

Simplicity and Ease of Use

Kiteworks enables secure file sharing and collaboration among public entities, individuals, and third-party organizations.

Data Collection

Kiteworks' secure web forms and data collection mechanisms provide a robust solution for organizations to obtain explicit consent from users for the collection and use of their personal information, in compliance with data protection regulations.



The Kiteworks Platform and Saudi Arabia Data & AI Authority Personal Data Protection Law

Personal Data Protection Law	Control Description	Kiteworks Solution
Article 4	<p>Data Subject shall have the following rights pursuant to this Law and as set out in the Regulations:</p> <ol style="list-style-type: none"> 1. The right to be informed about the legal basis and the purpose of the Collection of their Personal Data. 2. The right to access their Personal Data held by the Controller, in accordance with the rules and procedures set out in the Regulations, and without prejudice to the provisions of Article (9) of this Law. 3. The right to request obtaining their Personal Data held by the Controller in a readable and clear format, in accordance with the controls and procedures specified by the Regulations. 4. The right to request correcting, completing, or updating their Personal Data held by the Controller. 5. The right to request a Destruction of their Personal Data held by the Controller when such Personal Data is no longer needed by Data Subject, without prejudice to the provisions of Article (18) of this Law. 	<p>Kiteworks' secure web forms allow organizations to obtain explicit consent for data collection and use. Users can request deletion of their personal information, which is securely removed from the system. Compliance dashboards and activity logs enable tracking and auditing of user actions, including file deletions, to demonstrate compliance. These features, along with data collection mechanisms and versioning, help organizations inform data subjects about the legal basis and purpose of data collection, allowing access to and correction of personal data, and facilitating data deletion requests.</p>
Article 5	<ol style="list-style-type: none"> 1-Except for the cases stated in this Law, neither Personal Data may be processed nor the purpose of Personal Data Processing may be changed without the consent of the Data Subject. The Regulations shall set out the conditions of the consent, the cases in which the consent must be explicit, and the terms and conditions related to obtaining the consent of the legal guardian if the Data Subject fully or partially lacks legal capacity. 2-In all cases, Data Subject may withdraw the consent mentioned in Paragraph (1) of this Article at any time; the Regulations determines the necessary controls for such case. 	<p>Kiteworks' secure web forms and data collection mechanisms enable them to obtain explicit consent from users for the processing of their personal data. These features allow organizations to clearly communicate the purpose of data collection and obtain informed consent from Data Subjects, ensuring compliance with the Regulations. Kiteworks' consent management capabilities enable organizations to handle consent withdrawal requests effectively.</p>

Personal Data Protection Law	Control Description	Kiteworks Solution
Article 8	<p>Subject to the provisions of this Law and the Regulations regarding the Disclosure of Personal Data, the Controller shall only select Processors providing the necessary guarantees to implement the provisions of this Law and the Regulations. The Controller shall also monitor the compliance of said Processors with the provisions of this Law and the Regulations. This shall not prejudice the Controller's responsibilities towards the Data Subject or the Competent Authority as the case may be. The Regulations shall set out the provisions necessary in this regard, including provisions related to any subsequent contracts conducted by the Processor.</p>	<p>Kiteworks provides a secure platform for sending, receiving, and storing information with robust security, tracking, and policy controls. The platform enables organizations to define their business processes to meet the requirements of the law. Kiteworks also generates comprehensive, standardized log data for security and compliance-related activities, which can be easily integrated with an organization's existing SIEM tools. This allows organizations to monitor and analyze potential security threats and demonstrate compliance with the PDPL.</p>
Article 9	<p>1-The Controller may set time frames for exercising the right to access Personal Data stated in Paragraph (2) of Article (4) herein as stipulated in the Regulations. The Controller may limit the exercise of this right in the following cases:</p> <p>a) If this is necessary to protect the Data Subject or other parties from any harm, according to the provisions set forth in the Regulations.</p> <p>b) If the Controller is a Public Entity and the restriction is required for security purposes, required by another law, or required to fulfill judicial requirements.</p> <p>2-The Controller shall prevent the Data Subject from accessing Personal Data in any of the situations stated in Paragraphs (1, 2, 3, 4, 5) and (6) of Article (16) herein.</p>	<p>Kiteworks provides features that allow Controllers to set time frames and limit access to personal data when necessary. The platform enables Controllers to delete file previews if not accessed within a specified number of days, and to set retention periods for folders and files. This ensures that personal data is not retained longer than needed. Additionally, Kiteworks allows Controllers to recover deleted files within a specified grace period, enabling them to fulfill Data Subject access requests while still protecting the data from unauthorized access.</p>

Personal Data Protection Law	Control Description	Kiteworks Solution
<p>Article 10</p>	<p>The Controller may only collect Personal Data directly from the Data Subject and may only process Personal Data for the purposes for which they have been collected. However, the Controller may collect Personal Data from a source other than the Data Subject and may process Personal Data for purposes other than the ones for which they have been collected in the following situations:</p> <p>1-The Data Subject gives their consent in accordance with the provisions of this Law.</p> <p>2-Personal Data is publicly available or was collected from a publicly available source.</p> <p>3-The Controller is a Public Entity, and the Collection or Processing of the Personal Data is required for public interest or security purposes, or to implement another law, or to fulfill judicial requirements.</p> <p>4-Complying with this may harm the Data Subject or affect their vital interests.</p> <p>5-Personal Data Collection or Processing is necessary to protect public health, public safety, or to protect the life or health of specific individuals.</p> <p>6-Personal Data is not to be recorded or stored in a form that makes it possible to directly or indirectly identify the Data Subject.</p> <p>7-Personal Data Collection is necessary to achieve legitimate interests of the Controller, without prejudice to the rights and interests of the Data Subject, and provided that no Sensitive Data is to be processed.</p> <p>The Regulations shall set out the provisions, controls, and procedures related to what is stated in paragraphs (2) to (7) of this Article.</p>	<p>The Kiteworks Enterprise Connect feature allows organizations to access content from external repositories while applying the access controls of the third-party system, ensuring that personal data is collected and processed in accordance with the law. Additionally, Kiteworks maintains a comprehensive audit log of all user activities, including data access and modification. This audit log can be used to detect and investigate unauthorized access to personal data, demonstrate compliance with data protection regulations, and ensure that personal data is collected and processed only for the purposes for which it was obtained.</p>

Personal Data Protection Law	Control Description	Kiteworks Solution
Article 11	<p>1-The purpose for which Personal Data is collected shall be directly related to the Controller's purposes, and shall not contravene any legal provisions.</p> <p>2-The methods and means of Personal Data Collection shall not conflict with any legal provisions, shall be appropriate for the circumstances of the Data Subject, shall be direct, clear, and secure, and shall not involve any deception, misleading, or extortion.</p> <p>3-The content of the Personal Data shall be appropriate and limited to the minimum amount necessary to achieve the purpose of the Collection. Content that may lead to specifically identifying Data Subject once the purpose of Collection is achieved shall be avoided. The Regulations shall set out the necessary controls in this regard.</p> <p>4-If the Personal Data collected is no longer necessary for the purpose for which it has been collected, the Controller shall, without undue delay, cease their Collection and destroy previously collected Personal Data.</p>	<p>The platform's comprehensive audit logging functionality allows organizations to track all user activities, including data access and modification. This enables them to detect and investigate any unauthorized access to personal data, ensuring that the collection methods are secure and do not involve deception or extortion. The audit logs serve as evidence of compliance with data protection regulations, demonstrating that personal data is collected only for the specified purposes and destroyed when no longer necessary.</p>
Article 12	<p>The Controller shall use a privacy policy and make it available to Data Subjects for their information prior to collecting their Personal Data. The policy shall specify the purpose of Collection, Personal Data to be collected, the means used for Collection, Processing, Storage and Destruction, and information about the Data Subject rights and how to exercise such rights.</p>	<p>Kiteworks enables organizations to create and display privacy policies to Data Subjects prior to collecting their personal data. The platform allows organizations to customize the branding and text on their web forms, including the addition of custom legal disclaimers and privacy policies. These policies can specify the purpose of data collection, the types of personal data collected, the means used for collection, processing, storage, and destruction, as well as information about Data Subject rights and how to exercise them.</p>

Personal Data Protection Law	Control Description	Kiteworks Solution
<p>Article 13</p>	<p>When collecting Personal Data directly from the Data Subject, the Controller shall take appropriate measures to inform the Data Subject of the following upon Collection:</p> <ol style="list-style-type: none"> 1-The legal basis for collecting their Personal Data. 2-The purpose of the Collection, and shall specify the Personal Data whose Collection is mandatory and the Personal Data whose Collection is optional. The Data Subject shall be informed that the Personal Data will not be subsequently processed in a manner inconsistent with the Collection purpose or in cases other than those stated in Article (10) of this Law. 3-Unless the Collection is for security purposes, the identity of the person collecting the Personal Data and the address of its representative, if necessary. 4-The entities to which the Personal Data will be disclosed, the capacity of such entities, and whether the Personal Data will be transferred, disclosed, or processed outside the Kingdom. 5-The potential consequences and risks that may result from not collecting the Personal Data. 6-The rights of the Data Subject pursuant to Article (4) herein. 7-Such other elements as set out in the Regulations based on the nature of the activity done by the Controller. 	<p>Customizable web forms enable organizations to provide the necessary information to Data Subjects during data collection. Using Kiteworks' features, organizations can tailor the text on their web forms to include the legal basis for data collection, the purpose of collection, and specify which data is mandatory or optional. They can also inform Data Subjects about the entities to which their data will be disclosed, potential consequences of not providing the data, and their rights under Article 4. Additionally, Kiteworks allows the inclusion of hyperlinks to direct users to privacy policies or other relevant information.</p>

Personal Data Protection Law	Control Description	Kiteworks Solution
<p>Article 15</p>	<p>The Controller may not Disclose Personal Data except in the following situations:</p> <ol style="list-style-type: none"> 1-Data Subject consents to the Disclosure in accordance with the provisions of the Law. 2-Personal Data has been collected from a publicly available source. 3-The entity requesting Disclosure is a Public Entity, and the Collection or Processing of the Personal Data is required for public interest or security purposes, or to implement another law, to fulfill judicial requirements. 4-The Disclosure is necessary to protect public health, public safety, or to protect the lives or health of specific individuals. 5-The Disclosure will only involve subsequent Processing in a form that makes it impossible to directly or indirectly identify the Data Subject. 6-The Disclosure is necessary to achieve legitimate interests of the Controller, without prejudice to the rights and interests of the Data Subject, and provided that no Sensitive Data is to be processed. <p>The Regulations shall set out the provisions, controls. and procedures related to what is stated in paragraphs (2) to (6) of this Article.</p>	<p>The platform allows users to request the deletion of their personal information at any time, ensuring that data is permanently and securely removed from the system. This feature can be used to fulfill Data Subject requests for erasure, as permitted by the law. Additionally, Kiteworks maintains a comprehensive audit log of all user activities, including data access, modification, and deletion. This audit log can be used to detect and investigate unauthorized access to personal data, demonstrate compliance with data protection regulations, and support investigations related to data disclosure.</p>
<p>Article 17</p>	<ol style="list-style-type: none"> 1-If Personal Data is corrected, completed, or updated, the Controller shall notify such amendment to all the other entities to which such Personal Data has been transferred and make the amendment available to such entities. 2-The Regulations shall set out the time frames for correction and updating of Personal Data, types of correction, and the procedures required to avoid the consequences of Processing incorrect, inaccurate, or outdated Personal Data. 	<p>Kiteworks facilitates the correction, completion, and updating of personal data. When a user submits a form to update their personal information, Kiteworks' notification feature can be used to alert designated recipients, ensuring that the relevant parties are immediately aware of the changes and can take appropriate action. Additionally, Kiteworks maintains a comprehensive, consolidated activity log that tracks all system activities, including file edits. This log can be searched, filtered, and sorted to identify changes made to personal data, as well as who made those changes.</p>

Personal Data Protection Law	Control Description	Kiteworks Solution
Article 18	<p>1-The Controller shall, without undue delay, Destroy the Personal Data when no longer necessary for the purpose for which they were collected. However, the Controller may retain data after the purpose of the Collection ceases to exist; provided that it does not contain anything that may lead to specifically identifying Data Subject pursuant to the controls stipulated in the Regulations.</p> <p>2-In the following cases, the Controller shall retain the Personal Data after the purpose of the Collection ceases to exist:</p> <p>a) If there is a legal basis for retaining the Personal Data for a specific period, in which case the Personal Data shall be destroyed upon the lapse of that period or when the purpose of the Collection is satisfied, whichever is longer.</p> <p>b) If the Personal Data is closely related to a case under consideration before a judicial authority and the retention of the Personal Data is required for that purpose, in which case the Personal Data shall be destroyed once the judicial procedures are concluded.</p>	<p>Kiteworks enables secure and timely destruction of personal data when it is no longer necessary for the purpose of collection. The platform 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. This action is logged, confirming the user's ID, file name, and time of deletion. Kiteworks also provides tools for securely wiping data from devices in case of loss or theft.</p>
Article 19	<p>The Controller shall implement all the necessary organizational, administrative, and technical measures to protect Personal Data, including during the Transfer of Personal Data, in accordance with the provisions and controls set out in the Regulations.</p>	<p>The platform maintains detailed audit logs to track user activity and data access, enabling the detection and investigation of unauthorized access. Kiteworks employs least-privilege access defaults to minimize the risk of unauthorized access, strong encryption for data at rest and in transit, and a hardened virtual appliance with multiple layers of protection, such as embedded firewalls and intrusion detection systems. The system also supports secure clustering and one-click updates to maintain security and integrity.</p>

Personal Data Protection Law	Control Description	Kiteworks Solution
Article 20	<p>1-The Controller shall notify the Competent Authority upon knowing of any breach, damage, or illegal access to personal data, in accordance with the Regulations.</p> <p>2-The Controller shall notify the Data Subject of any breach, damage, or illegal access to their Personal Data that would cause damage to their data or cause prejudice to their rights and interests, in accordance with the Regulations.</p>	<p>The platform maintains an evolving library of proprietary patterns that detect suspicious activities on the network and within the Kiteworks application code. These patterns match various indicators, such as network traffic, known attack signatures, exfiltration attempts, and unauthorized code changes. The system's multiple layers of protection and tripwires make it difficult for attackers to hide intrusion attempts. Kiteworks logs all activity related to intrusion attempts and detected anomalies, enabling organizations to promptly identify and notify the Competent Authority and affected Data Subjects of any breach, damage, or illegal access to personal data, in accordance with the Regulations.</p>
Article 21	<p>The Controller shall respond to the requests of the Data Subject pertaining to their rights under this Law within such period and in such method as set out in the Regulations.</p>	<p>The platform gives users control over their personal identification information, allowing them to choose what information to provide and request its deletion at any time. Kiteworks maintains a complete audit log of all user activity, including the submission of personal identification information. This audit log records who has submitted information, when it was submitted, and from where, enabling organizations to track Data Subject requests and demonstrate compliance with data protection regulations.</p>

Personal Data Protection Law	Control Description	Kiteworks Solution
Article 23	<p>Without prejudice to this Law, the Regulations shall set out additional controls and procedures for the Processing of Health Data in a manner that ensures the privacy of the Data Subject and protects their rights under this Law. Such additional controls and procedures shall include the following:</p> <p>1-Restricting the right to access Health Data, including medical files, to the minimum number of employees or workers and only to the extent necessary to provide the required Health Services.</p> <p>2-Restricting Health Data Processing procedures and operations to the minimum extent possible of employees and workers as necessary to provide Health Services or offer health insurance programs.</p>	<p>Kiteworks provides advanced access control features that ensure the privacy of Data Subjects and protect their rights when processing Health Data. The platform supports various authentication methods, including multi-factor authentication, SSO, and integration with existing identity providers, ensuring that only authorized users can access sensitive information. Kiteworks employs role-based access controls and adheres to the principle of least privilege, automatically granting users the minimum permissions necessary to perform their tasks. This approach allows organizations to restrict access to Health Data, including medical files, to the minimum number of employees or workers required to provide Health Services.</p>
Article 24	<p>Without prejudice to this Law, the Regulations shall set out additional controls and procedures for the Processing of Credit Data in a manner that ensures the privacy of the Data Subject and protects their rights under this Law and the Credit Information Law. Such controls and procedures shall include the following:</p> <p>1-Implementing appropriate measures to verify that the Data Subject has given their explicit consent to the Collection of the Personal Data, changing the purpose of the Collection, or Disclosure or Publishing of the Personal Data in accordance with the provisions of this Law and the Credit Information Law.</p> <p>2-Requiring that the Data Subject be notified when a request for Disclosure of their Credit Data is received from any entity.</p>	<p>The platform provides secure web forms and data collection mechanisms that enable them to obtain explicit consent from Data Subjects for the collection, change of purpose, disclosure, or publishing of their Credit Data. These customizable forms allow organizations to include relevant legal disclaimers, privacy policies, and hyperlinks to additional information, ensuring that Data Subjects are fully informed before giving their consent. Kiteworks also requires authentication for users verifying consent, and maintains immutable audit logs and optional archiving for eDiscovery, demonstrating compliance with data protection regulations.</p>

Personal Data Protection Law	Control Description	Kiteworks Solution
Article 25	<p>With the exception of the awareness-raising materials sent by Public Entities, the Controller may not use personal means of communication, including the post and email, of the Data Subject to send advertising or awareness-raising materials, unless:</p> <p>1-Obtaining the prior consent of the targeted recipient for such materials.</p> <p>2-The sender of the material shall provide a clear mechanism, as set out in the Regulations, that enables the targeted recipient to request stopping receiving such materials if they desire so.</p> <p>3-The Regulations shall set out the provisions concerning the aforementioned advertising and awareness-raising materials, as well as the conditions and situations concerning the consent of the recipient to receive aforementioned materials.</p>	<p>The platform's secure web forms and data collection mechanisms allow organizations to obtain explicit consent from users, with customizable branding, legal disclaimers, and hyperlinks to relevant information, such as privacy policies. Kiteworks also provides a tracking feature that enables senders to monitor recipient engagement with the materials, ensuring that they can provide a clear mechanism for recipients to request stopping the receipt of such materials, as required by the Regulation.</p>
Article 28	<p>It is not permissible to copy official documents where Data Subjects are identifiable, except where it is required by law, or when a competent public authority requests copying such documents pursuant to the Regulations.</p>	<p>The platform logs a wide range of user activities, including file access, uploads, downloads, edits, deletions, and sharing. This detailed audit log allows organizations to track who has accessed or copied specific documents, when the action occurred, and from which location. By leveraging these features, organizations can ensure that official documents are only copied when required by law or requested by a competent public authority pursuant to the Regulations. The granular tracking capabilities of Kiteworks empower organizations to maintain strict control over the copying of sensitive documents.</p>

Personal Data Protection Law	Control Description	Kiteworks Solution
<p>Article 29</p>	<p>1-Subject to the provisions of Paragraph (2) of this Article, a Controller may Transfer Personal Data outside the Kingdom or disclose it to a party outside the Kingdom, in order to achieve any of the following purposes:</p> <p>A. If this is relating to performing an obligation under an agreement, to which the Kingdom is a party.</p> <p>B. If it is to serve the interests of the Kingdom.</p> <p>C. If this is to the performance of an obligation to which the Data Subject is a party.</p> <p>D. If this is to fulfill other purposes as set out in the Regulations.</p> <p>2-The conditions that must be met when there is a Transfer or Disclosure of Personal Data, according to what is stated in Paragraph (1) of this Article, are as follows:</p> <p>A. The Transfer or Disclosure shall not cause any prejudice to national security or the vital interests of the Kingdom.</p> <p>B. There is an adequate level of protection for Personal Data outside the Kingdom. Such level of protection shall be at least equivalent to the level of protection guaranteed by the Law and Regulations, according to the results of an assessment conducted by the Competent Authority in coordination with whomever it deems appropriate from the other relevant authorities.</p> <p>C. The Transfer or Disclosure shall be limited to the minimum amount of Personal Data needed.</p> <p>3-Paragraph (2) of this Article shall not apply to cases of extreme necessity to preserve the life or vital interests of the Data Subject or to prevent, examine, or treat disease.</p> <p>4-The Regulations shall set out the provisions, criteria, and procedures related to the implementing of this Article, including applicable exceptions for Controllers regarding conditions referred to in Subparagraphs (b) and (c) of Paragraph (2) of this Article, as well as controls and procedures for such exemptions.</p>	<p>The platform employs a role-based access control system with least-privilege defaults, guaranteeing that users are only granted the minimum permissions necessary to perform their assigned tasks. This granular approach to access management allows organizations to maintain strict control over who can access and transfer personal data, minimizing the risk of unauthorized disclosure.</p> <p>Kiteworks also supports advanced data residency controls, enabling organizations to restrict user access based on the country of origin determined by the user's IP address. This feature empowers organizations to limit the transfer or disclosure of personal data to the minimum amount required. By ensuring that personal data is only transferred or disclosed when absolutely necessary, Kiteworks helps organizations safeguard the privacy of Data Subjects and protect the vital interests of the Kingdom.</p> <p>In addition to these access controls, Kiteworks utilizes a double encryption mechanism to protect data even in the event of a breach. This multilayered approach to data security ensures that personal data remains protected during cross-border transfers, minimizing the risk of unauthorized access and demonstrating a commitment to maintaining an adequate level of protection for personal data outside the Kingdom.</p>

Personal Data Protection Law	Control Description	Kiteworks Solution
<p>Article 30</p>	<p>1-Without prejudice to the provisions of this Law and the powers of the Saudi Central Bank pursuant to applicable legal provisions, the Competent Authority shall be the entity in charge of overseeing the implementation of this Law and the Regulations.</p> <p>2-The Regulations shall identify the situations where the Controller shall appoint one or more persons as personal data protection officer(s), and shall set the responsibilities of any such person in accordance with the provisions of this Law.</p> <p>3-The Controller shall cooperate with the Competent Authority in performing its duties to supervise the implementation of the provisions of this Law and the Regulations, and shall take such steps as necessary in connection with the related matters referred to the Controller by the Competent Authority.</p> <p>4-The Competent Authority, in order to carry out its duties related to supervising the implementation of the provisions of the Law and Regulations, may:</p> <p>A. Request the necessary documents or information from the Controller to ensure its compliance with the provisions of the Law and Regulations.</p> <p>B. Request the cooperation of any other party for the purposes of support in accomplishing supervisory duties and enforcement of the provisions of the Law and Regulations.</p> <p>C. Specify the appropriate tools and mechanisms for monitoring Controllers' compliance with the provisions of the Law and the Regulations, including maintaining a national register of Controllers for this purpose.</p> <p>D. Provide services related to Personal Data protection through the national register referred to in Subparagraph (c) of this Paragraph or through any other means deemed appropriate. The Competent Authority may collect a fee for the Personal Data protection services it may provide.</p> <p>5-The Competent Authority may, at its discretion, delegate to other authorities the accomplishment of some of its duties that are related to supervision or enforcement of the provisions of the Law and Regulations.</p>	<p>The platform meticulously logs a wide array of user activities, including logins, uploads, downloads, views, and administrative actions, ensuring that the data is captured in a complete, detailed, timely, consolidated, and standardized manner. This level of granularity in tracking enables organizations to swiftly and thoroughly demonstrate compliance to auditors, providing them with the necessary evidence to support their adherence to the law.</p> <p>Kiteworks' tracking features empower the Competent Authority to effectively monitor Controllers' compliance with the Saudi PDPL. By granting access to these detailed logs, organizations can proactively assist the Competent Authority in identifying any potential breaches or noncompliant practices, thereby facilitating the enforcement of the law's provisions.</p> <p>Kiteworks also provides a range of compliance reports for various regulations, such as GDPR and HIPAA. These reports offer a clear and concise overview of an organization's compliance status, enabling them to identify areas for improvement and take corrective action where necessary.</p>

Personal Data Protection Law	Control Description	Kiteworks Solution
Article 31	<p>Without prejudice to Article (18) herein, the Controller shall maintain records, for such a period as required under the Regulations, of the Personal Data Processing activities, based on the nature of the activity carried out by the Controller. Such records are to be available whenever requested by the Competent Authority. The records shall contain the following information at a minimum:</p> <ul style="list-style-type: none"> 1-Contact details of the Controller. 2-The purpose of the Personal Data Processing. 3-Description of the categories of Personal Data Subjects. 4-Any other entity to which Personal Data has been, or will be, disclosed. 5-Whether the Personal Data has been or will be transferred outside the Kingdom or disclosed to an entity outside the Kingdom. 	<p>The platform logs a wide range of user activities, including logins, uploads, downloads, views, and administrative actions, in a complete, timely, and standardized manner. These logs can be easily accessed and provided to the Competent Authority upon request, demonstrating compliance with the law. Kiteworks' tracking features capture essential information such as the purpose of data processing, categories of Data Subjects, entities to which data has been disclosed, cross-border data transfers, and expected retention periods.</p>

The information provided on this page does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available on this page are for general informational purposes only. Information on this website may not constitute the most up-to-date legal or other information.

