Kiteworks

COMPLIANCE BRIEF

Complying With Saudi Data and Artificial Intelligence Authority (SDAIA) National Data Governance Interim Regulations

Kiteworks Supports Data Classification, Protection, Sharing, and Open Data

The Saudi Data and Artificial Intelligence Authority (SDAIA) oversees data and AI governance in Saudi Arabia. In 2020, they published interim regulations to control data collection, processing, and management nationally. The rules provide a framework for classifying, protecting, and sharing data produced by public entities, while upholding accountability and transparency. They cover data classification, personal data protection, sharing between government bodies, freedom of information requests, and open data standards. The SDAIA enforces compliance through binding and voluntary measures. The regulations aim to increase the value of data through ethical, responsible use that respects privacy. By regulating data at a national level, the SDAIA seeks to enable data-driven decision-making that benefits society while safeguarding individual rights. Kiteworks supports their interim regulations. Here's how:

Data Classification With Access Controls and Tagging

Data Classification regulations mandate classifying data based on sensitivity, applying the highest protection to unstructured data, and restricting access through role-based controls and least-privilege principles. Kiteworks helps comply by seamlessly integrating classification schemas with access controls, providing flexible and customizable categories tailored to an organization's needs, and logging all data classification actions for complete auditability. Granular user permissions limit data access on a need-to-know basis while administrative roles prevent privilege overlap. Kiteworks allows organizations to define their own classifications with associated criteria, then control corresponding access automatically based on that tagging. The unified, comprehensive audit log records the entire life cycle of data classification, from initial tagging to any reclassifications that may occur over time. This ensures full visibility into how each data asset is protected over its lifetime. By directly linking granular classification to access controls and maintaining detailed immutable records, Kiteworks provides the capabilities needed to implement layered data security policies aligned with Saudi regulations.

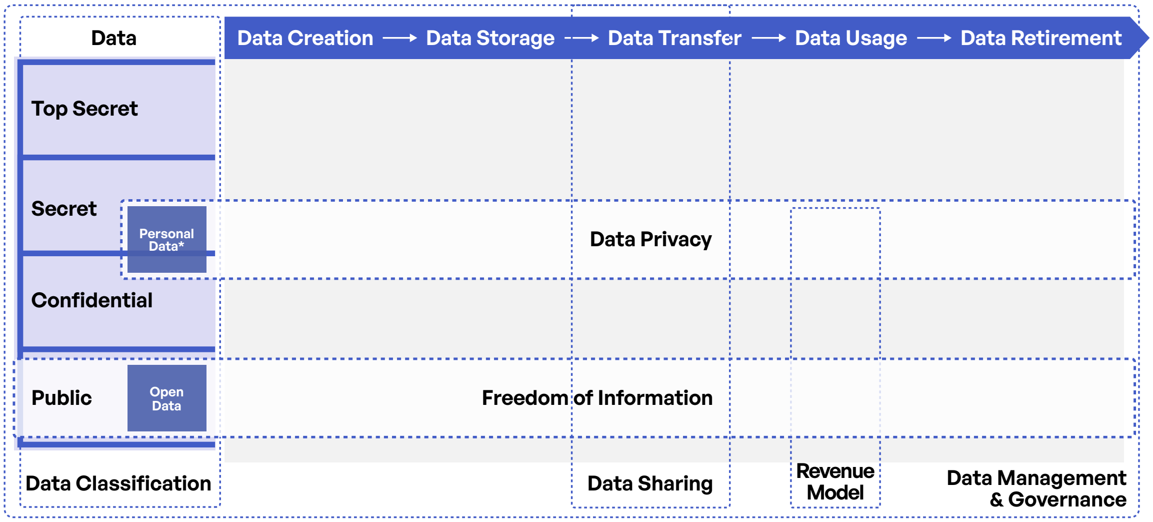
Personal Data Protection With Encryption and Security Controls

The Personal Data regulations require consent, data minimization, limited use and disclosure to authorized parties only, and mandatory deletion protocols to safeguard personal information. Kiteworks facilitates compliance through AES-256 encrypted storage, granular access controls, and immutable audit logs recording all access and modification events in detail. This provides full accountability while upholding privacy rights. Deleted personal data is permanently removed in a cryptographically secure manner, with logs documenting the removal process. Consent is obtained via customizable web forms with built-in data minimization, only collecting information expressly permitted. Encryption secures personal data end-to-end both in transit and at rest, mitigating unauthorized exposure risks even in the event of interception. Granular access controls implemented at an individual role level restrict personal data sharing to only authorized third parties, preventing uncontrolled proliferation. Detailed activity logging provides

Solution Highlights

- Flexible data classification
- Role-based access
- Secure web forms
- Least-privilege defaults
- Robust audit logs

complete visibility into internal handling and external sharing of personal data across the organization to demonstrate regulatory compliance. With its multilayered security model and meticulous audit logs, Kiteworks provides organizations with the capabilities required to responsibly manage personal data in alignment with Saudi privacy regulations.



(*) May be classified as Top Secret

Figure 1: Relationship and interdependencies of data-specific policies and regulations

Data Sharing via Authorized Accessibility

Data Sharing regulations stipulate authorized, accountable data sharing backed by stringent security controls to maintain confidentiality and integrity. Kiteworks delivers this through role-based access controls, granular permissions, detailed activity logging, and robust encryption. Role-based access ensures only properly authorized personnel can access shared data based on justified need. Comprehensive, tamper-proof audit logs record all data access events and transfers, providing transparency and accountability into how data is handled by all parties. This detailed visibility enables compliance monitoring, incident investigation, and policy refinement. By restricting data accessibility to only authorized purposes, providing end-to-end visibility into all interactions, and cryptographically protecting information, Kiteworks supports Saudi requirements for ethical, controlled, responsible data sharing.

Open Data With Visibility and Tracking

The Saudi regulations advise publishing open data in structured machine-readable formats to power transparency and innovation. Kiteworks can assist compliance through unified, standardized audit logs capturing all user and admin actions across the platform. The consistent, cleaned log data can be exported in accessible formats. This enables easy ingestion into analytics tools like Splunk to gain data insights. The comprehensive, immutable logs provide complete visibility into platform interactions as required for open data accountability. Data access events, transfers, and modifications are logged in a complete tamper-proof chain. By exporting these standardized logs in common formats, entities can meet open data stipulations for transparency while respecting privacy via strict data minimization. With holistic visibility into all interactions and interoperable machine-readable formats, Kiteworks gives organizations the foundational toolset needed to fulfill open data sharing regulations with appropriate security controls.

Ultimately, the Kiteworks platform provides the capabilities needed to manage data ethically and compliantly across the entire life cycle. By automating policy-driven data governance, enabling secure collaboration, and providing transparency through detailed audit logs, Kiteworks allows organizations to harness the power of data responsibly. Whether classifying sensitive data, safeguarding personal information, controlling sharing, or publishing open data, Kiteworks has the tools to help organizations comply with Saudi regulations while leveraging data securely to drive innovation. With Kiteworks, entities gain both data protection and data-driven agility.

Kiteworks