Kiteworks

COMPLIANCE BRIEF

Kiteworks and the UAE Federal Personal Data Protection Law

How the Kiteworks Private Data Network Supports Controller and Processor Compliance With Federal Decree by Law No. (45) of 2021

The UAE Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data establishes a comprehensive legal framework governing the collection, processing, storage, and transfer of personal data across the United Arab Emirates. The regulation applies to any Controller or Processor — whether based inside or outside the UAE — that handles personal data belonging to individuals located within the country, making it a global compliance obligation for organizations operating in or with the UAE. Financial services, healthcare, technology, and other data-intensive sectors must comply, though government entities, security and judicial authorities, and companies within free zones under their own data protection regimes are exempt. Controllers and Processors were required to regularize compliance within six months of the Executive Regulations' issuance, effective from January 2, 2022, with the UAE Data Bureau serving as the primary enforcement authority. Organizations that fail to comply face administrative penalties determined by the Council of Ministers. Kiteworks supports organizations in meeting these obligations through its Private Data Network. Here's how:

Hardened Infrastructure and Encryption Secure Personal Data Across All Processing States

Articles 5(6), 7(1), 8(2), 8(6), and 20 require Controllers and Processors to apply appropriate technical and organizational measures that preserve the confidentiality, integrity, and security of personal data across all processing states, aligned with internationally recognized standards. These measures must address the full range of processing risks, including unauthorized access, destruction, alteration, and disclosure, at every stage from design through operation. The Kiteworks hardened virtual appliance prevents direct access to the underlying operating system and database, while double encryption at rest using AES-256 is applied at both the file and disk levels with customer-owned keys. Data in transit is secured with TLS 1.3, and optional FIPS 140-3 validated cryptographic modules support deployments requiring the highest encryption standards. Embedded firewalls, Fail2Ban IP blocking, and AI-based intrusion detection protect the processing environment, while antivirus, DLP, advanced threat protection, and content disarm and reconstruction scanning inspect all content entering or leaving the system.

Solution Highlights

- **Hardened virtual appliance**
- **AES-256 double encryption**
- **Customer-owned keys**
- **Data Policy Engine with RBAC and ABAC**
- **Real-time audit log with SIEM integration**

Data Policy Engine, RBAC, ABAC, and Geofencing Enforce Purpose Limitation and Transfer Controls

Access governance and cross-border transfer obligations sit at the core of the UAE law. Articles 7(2), 7(3), 18(3), and 23(1)(a) require Controllers and Processors to limit personal data processing to its defined purpose, apply privacy-by-design principles at the point of collection, protect data subjects when automated processing occurs, and enforce contractual controls over cross-border transfers where adequate protection laws are absent. The Kiteworks Data Policy Engine applies role-based access control (RBAC) and attribute-based access control (ABAC) dynamically across all processing activities, including automated workflows, evaluating user identity, data sensitivity, and requested action to restrict operations to authorized personnel only. SafeVIEW and SafeEDIT allow data to be accessed without ever leaving the secure environment, preventing extraction during automated handling. Data sovereignty and geofencing controls enforce cross-border movement restrictions by routing and storing personal data within assigned country boundaries, directly supporting the contractual compliance obligations under Article 23(1)(a).

Unified Audit Logs and Compliance Reports Support Personal Data Record Obligations

Maintaining verifiable records of every processing activity is a distinct and enforceable obligation under the UAE law. Articles 7(4), 8(7), 11(1)(c), and 20(1)(d) require Controllers and Processors to document authorized access, processing purposes, retention periods, erasure mechanisms, and cross-border transfer details — and to submit these records to the UAE Data Bureau upon request. The Kiteworks unified, real-time audit log captures every data interaction across all channels — including who accessed what, when, from where, and what action was taken — and feeds directly into SIEM systems for continuous monitoring. Role-based and attribute-based access controls document which users hold authorization for specific processing activities, while configurable retention, expiration, and deletion policies record and enforce processing timeframes and erasure mechanisms. Compliance reports aggregate this information into exportable, structured outputs ready for submission to the Bureau whenever requested.

Kiteworks equips organizations operating under the UAE Federal Decree by Law No. (45) of 2021 with a unified, technically rigorous platform that addresses the law's most demanding obligations. Its hardened infrastructure and layered encryption architecture secure personal data across every processing state, meeting the confidentiality and integrity requirements the decree places on both Controllers and Processors. Dynamic access governance enforces purpose limitation and restricts processing to authorized personnel, while data sovereignty and geofencing controls operationalize the law's cross-border transfer obligations without relying solely on contractual commitments. Comprehensive audit logging and structured compliance reporting give organizations the verifiable, submission-ready records the UAE Data Bureau can request at any time. Across protection, control, and record-keeping, Kiteworks transforms UAE PDPL compliance from a legal obligation into a defensible, operational posture.