Kiteworks

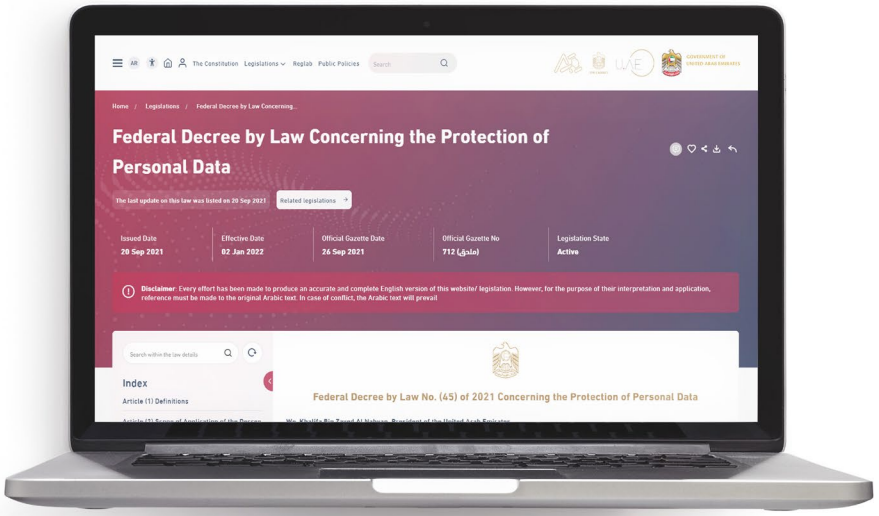
GUIDE

Navigating UAE Personal Data Protection Law With Kiteworks

How the Kiteworks Private Data Network Supports Personal Data Protection, Security, and Governance Requirements Under the UAE Personal Data Protection Law

Introduction

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. Promulgated by President Khalifa Bin Zayed Al Nahyan and effective as of 02 January 2022, the regulation aims to safeguard the privacy and confidentiality of personal data belonging to natural persons, while enabling lawful data processing activities that serve legitimate organizational, contractual, and public interest purposes. The UAE Data Bureau (the Bureau), established under Federal Decree by Law No. (44) of 2021, serves as the primary regulatory authority responsible for enforcement, oversight, and issuance of executive guidance.



The regulation applies to any Controller or Processor — whether residing inside or outside the UAE — that processes personal data of Data Subjects located within the State. It extends equally to Data Subjects residing in or conducting business from the UAE. Importantly, the law excludes government data, governmental entities, personal data held by security and judicial authorities, personal health data governed by separate legislation, banking and credit data with dedicated regulatory frameworks, and companies operating within free zones that maintain their own data protection regimes. The Bureau retains authority to grant partial or full exemptions to establishments processing limited volumes of personal data.

Controllers and Processors carry distinct but complementary obligations. Controllers must implement appropriate technical and organizational measures to protect personal data throughout its life cycle, maintain comprehensive processing records, appoint qualified Processors capable of meeting the law's standards, and conduct Data Protection Impact Assessments before deploying technologies that pose elevated privacy risks. Processors must operate strictly within the scope defined by the Controller, erase data upon completion of processing, and immediately notify the Controller of any breach. Both parties must report data breaches to the Bureau with detailed documentation — including breach descriptions, corrective actions, and potential impacts — and must directly notify affected Data Subjects when breaches threaten their privacy and confidentiality.

The law mandates appointment of a Data Protection Officer (DPO) where processing involves high privacy risks, large volumes of sensitive personal data, or systematic profiling and automated decision-making. The DPO ensures regulatory compliance, advises on risk assessments, receives data subject complaints, and liaises with the Bureau. Controllers and Processors must actively support the DPO's independence, provide necessary resources, and refrain from imposing penalties related to the DPO's lawful performance of duties.

GOVERNMENT OF
UNITED ARAB EMIRATES

Data Subjects hold substantive rights under the law, including rights to access, correct, erase, restrict, and port their personal data, as well as the right to object to direct marketing, automated processing decisions, and unlawful processing. Cross-border data transfers require Bureau approval and are permissible only to jurisdictions with equivalent data protection standards or under specific contractual safeguards, bilateral agreements, or explicit Data Subject consent.

The Council of Ministers, acting on recommendations from the Bureau's General Director, determines the administrative penalties applicable to violations, which the Bureau imposes following complaint investigation and verification. Stakeholders may submit grievances against Bureau decisions within 30 days of notification, with resolution required within 30 days of submission. Controllers and Processors were required to regularize their compliance status within six months of the Executive Regulations' issuance, with the Council of Ministers holding authority to extend that period. Complementary frameworks include the UAE Credit Information Law, the Health Sector ICT Law, and the Central Bank Financial Regulation, all of which intersect with this decree's data protection obligations.

The Kiteworks Secure File Sharing and Governance Platform

The Kiteworks Private Data Network empowers organizations to share sensitive data with trusted parties by email, file sharing, file transfer, and other channels at the highest levels of security, governance, and compliance while maintaining full visibility and control over their file sharing activities. The Kiteworks platform provides:

Protection of Unstructured Data

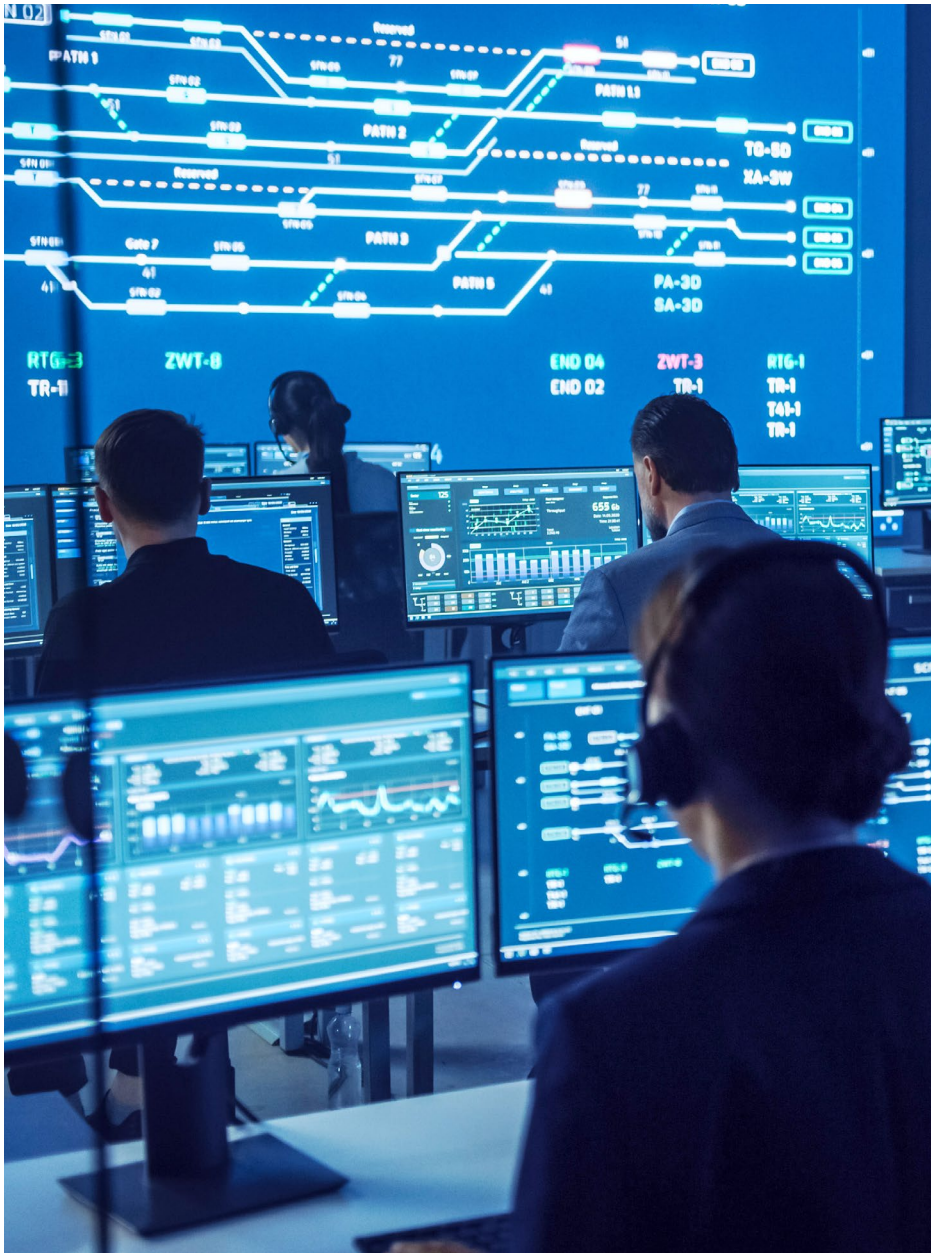
Kiteworks provides comprehensive protection for unstructured data through its advanced firewall and zero-trust file sharing capabilities that ensure sensitive unstructured data remains secure throughout its life cycle, whether at rest or in transit across various communication channels.

Governance and Compliance

Kiteworks reduces compliance risk and cost by consolidating advanced data governance capabilities into a single platform. Whether employees send and receive data via email, file share, automated file transfer, APIs, or web forms, it's covered.

Simplicity and Ease of Use

Kiteworks offers a user-friendly interface that simplifies secure file sharing and collaboration, enabling users to easily send, receive, and manage sensitive data without compromising security. The platform's intuitive design and seamless integration with existing workflows ensures high user adoption rates and minimizes the learning curve for organizations implementing robust data protection measures.



The Kiteworks Platform and the UAE Federal Decree by Law Concerning the Protection of Personal Data

UAE Federal Decree by Law No. (45) of 2021 Concerning the Protection of Personal Data governs how Controllers and Processors collect, handle, secure, and transfer Personal Data across automated electronic systems. It establishes foundational processing principles including purpose limitation, data minimization, and accuracy, while requiring organizations to implement technical and organizational safeguards that protect data confidentiality and integrity throughout the processing life cycle. Controllers and Processors must maintain detailed activity records, apply privacy-by-design measures, secure all processing systems through encryption and pseudonymisation, and govern cross-border data transfers through enforceable contractual frameworks that replicate the Decree's protective standards.

Article Requirements	Kiteworks Solution
Article (5)(6) — Personal Data shall be kept securely, including protecting it from any violation, penetration, or illegal or unauthorized processing through the development and use of appropriate technical and organizational measures and procedures in accordance with the laws and legislation in force in this regard.	The Kiteworks Private Data Network (PDN) has a defense-in-depth architecture that protects personal data from breach and unauthorized access. The hardened virtual appliance prevents direct OS or database access, while embedded firewalls, Fail2Ban IP blocking, and AI-based intrusion detection guard the perimeter. Data is double-encrypted at rest with customer-owned keys, and zero-trust principles isolate internal services. A rigorous secure development life cycle — including penetration testing and continuous bounty programs — ensures vulnerabilities are caught before exploitation. Granular admin role separation, risky settings detection, and configurable data policies enforce procedural controls, with a real-time unified audit log feeding SIEM systems for continuous security monitoring.
Article (5)(7) — Personal Data shall not be kept after the purpose of its processing has been exhausted. It may be kept if the identity of the Data Subject has been concealed using the "Anonymization Mechanism."	Audit logs are anonymized by default to ensure that they follow privacy standards and regulations. Anonymization is performed using UUIDs and the administrator can convert UUIDs to email addresses if detailed information is required for the log verification.
Article (7)(1) — Take appropriate technical and organizational measures to implement the necessary standards to protect and secure Personal Data in order to preserve its confidentiality and privacy, and to ensure that it is not breached, destroyed, altered or tampered with, taking into account the nature, scope and purposes of processing and the possibility of risks to the confidentiality and privacy of the Data Subject's Personal Data.	Layered technical and organizational measures protect personal data across its full life cycle. Data is secured within a hardened virtual appliance using double encryption at rest, TLS 1.3 in transit, and embedded network and web application firewalls. Access is governed by role-based (RBAC) and dynamic attribute-based (ABAC) controls that enforce least privilege by default, evaluating user identity, data sensitivity, and requested action in real time. Multi-factor authentication, geofencing, IP blocking, and country-level restrictions further prevent unauthorized access, while SafeVIEW and SafeEDIT allow data to be used without ever leaving the secure environment. A unified, unthrottled audit log captures every action in real time, feeding SIEM systems and supporting compliance reporting. Antivirus, DLP, advanced threat protection, and intrusion detection continuously monitor for risks to confidentiality and integrity.

Article Requirements	Kiteworks Solution
Article (7)(4) — Maintain a special record for Personal Data, provided that such record shall include the data of both the Controller and the Data Protection Officer, a description of the categories of Personal Data, details of the persons authorized to access the Personal Data, processing times, limitations and scope, the mechanism for erasing, modifying or processing Personal Data, the purpose of processing, any data related to the cross-border movement and processing of such data, and the technical and organizational measures related to information security and processing. The Controller shall submit such record to the Bureau whenever requested to do so.	Kiteworks provides the underlying controls and audit infrastructure needed to populate and maintain a personal data record. The unified audit log captures every data interaction — including who accessed what, when, from where, and what action was taken — across all channels. Role-based and attribute-based access controls document which users are authorized to access specific data, while user profile assignments record processing permissions and limitations. Data sovereignty and geofencing controls track and enforce cross-border movement restrictions. Configurable retention, expiration, and deletion policies document and enforce processing time frames and erasure mechanisms. Compliance reports — including built-in GDPR reporting — aggregate this information into structured outputs that can be submitted to regulators upon request.
Article (8)(2) — Apply the appropriate technical and organizational procedures and measures to protect Personal Data at the design stage, whether during the identification of the means of processing or during the processing, taking into account the cost of implementing such procedures and the nature, scope and purposes of processing.	Kiteworks supports compliance by embedding technical and organizational safeguards directly into its architecture. The hardened virtual appliance, double encryption at rest, TLS 1.3 in transit, and embedded firewalls are foundational to every deployment. The principle of least privilege is enforced from the outset — users start with no permissions and are granted only what their role requires. The Data Policy Engine applies RBAC and ABAC controls at the point of data interaction, ensuring protection is embedded into every processing activity. A secure development life cycle incorporating threat modeling, code review, penetration testing, and bounty programs ensures privacy considerations are addressed before release. Configurable retention, expiration, and access controls allow organizations to align data handling with the specific nature, scope, and purpose of each processing activity.
Article (8)(6) — Protect and secure data processing, the electronic media and devices used in processing and the Personal Data they contain.	The hardened virtual appliance prevents direct access to the underlying OS, database, or file system, while double encryption at rest and TLS 1.3 in transit secure data across all processing states. Embedded firewalls, Fail2Ban, and AI-based intrusion detection protect the processing environment from external threats. Antivirus scanning, DLP, advanced threat protection, and CDR integration inspect and sanitize all content entering or leaving the system. Mobile apps include jailbreak detection, biometric authentication, secure offline containers, and remote wipe. The MCP Server stores credentials exclusively in OS-level secure keystores, never exposing tokens to AI clients. All processing activity across every channel is captured in a unified audit log, providing complete visibility into how personal data moves through electronic media and devices.

Article Requirements	Kiteworks Solution
Article (8)(7) — Maintain a special record of Personal Data which is processed on behalf of the Controller, provided that such record includes the data of the Controller, the Processor and the Data Protection Officer and a description of the categories of Personal Data they have, data of the persons authorized to access Personal Data, processing times, restrictions and scope, the mechanism of erasing, modifying or processing Personal Data, the purpose of processing, any data related to the cross-border movement and processing of such data and the technical and organizational measures related to information security and processing operations, provided that the Processor submits such record to the Bureau whenever it is requested to do so.	Kiteworks provides the controls and audit infrastructure processors need to maintain an accurate and complete personal data record. The unified audit log captures every processing activity — who accessed data, when, from where, and what action was taken — across all channels and on behalf of which controller. Role-based and attribute-based access controls document authorized users and their specific processing permissions. Data sovereignty and geofencing controls track and enforce cross-border movement restrictions. Configurable retention, expiration, and deletion policies document processing time frames, scope, and erasure mechanisms. Admin role separation ensures clear accountability between controllers, processors, and data protection functions. Compliance reports consolidate this information into structured, exportable outputs ready for submission to regulators upon request.
Article (18) paragraph 3 — The Controller shall adopt appropriate measures to protect the privacy and confidentiality of the Data Subject's Personal Data in the cases referred to in Paragraph 2 of this article and shall not cause any prejudice to the Data Subject's rights.	Kiteworks ensures that even when automated processing occurs, personal data remains protected and governed throughout. The Data Policy Engine applies dynamic RBAC and ABAC controls to all automated workflows — including MFT, API, and MCP-driven processes — ensuring only authorized operations are permitted on personal data. SafeVIEW and SafeEDIT prevent data from being extracted or exposed beyond its intended use, even during automated handling. Configurable retention, expiration, and deletion policies ensure personal data processed under contract or consent is not retained beyond its permitted scope. The unified audit log captures every automated processing event with full attribution, providing the evidentiary record needed to demonstrate that data subject rights were upheld. Role-based admin separation ensures accountability is maintained across all automated processing activities.
Article (20) paragraph 1 — The Controller and the Processor shall develop and take appropriate technical and regulatory measures to ensure the highest standard of information security that is suitable for the risks related to data processing in accordance with the best international practices and standards.	Kiteworks' comprehensive security architecture is aligned with leading international standards and best practices, including NIST CSF, ISO 27001 principles, and regional frameworks across EMEA and APAC. The hardened virtual appliance provides foundational protection with double encryption at rest, TLS 1.3 in transit, embedded firewalls, and AI-based intrusion detection. A rigorous secure development life cycle — encompassing threat modeling, code review, automated and manual penetration testing, and continuous bounty programs — ensures risks are identified and mitigated proactively. The Data Policy Engine enforces dynamic access controls calibrated to the sensitivity of each processing activity, while antivirus, DLP, advanced threat protection, and CDR integration address content-level risks. Admin role separation, risky settings detection, and configurable data policies enforce organizational measures proportionate to processing risk. A real-time unified audit log feeds SIEM systems for continuous monitoring, providing structured evidence of security controls aligned with internationally recognized information security management principles.

Article Requirements	Kiteworks Solution
Article (20) paragraph 1(a) — Encryption of Personal Data and the application of Pseudonymisation.	Strong, standards-based encryption is applied across all data states and processing channels. All data is double-encrypted at rest — once at the application level with a file-level key and again at the disk level — using AES-256 encryption. Data in transit is protected with TLS 1.3, with optional FIPS 140-3 validated cryptographic modules available for deployments requiring the highest encryption standards. Customer-owned encryption keys ensure that neither Kiteworks nor any third party can decrypt personal data without explicit authorization. The Email Protection Gateway adds S/MIME and OpenPGP encryption for email-borne personal data. On pseudonymisation, Kiteworks supports anonymized audit logs by default, replacing user identifiers with UUIDs to protect personal data in compliance reporting contexts, with administrator-controlled de-anonymization available only when operationally justified.
Article (20) paragraph 1(b) — Applying measures which ensure the continuous confidentiality, safety, accuracy and flexibility of data processing systems and services.	Confidentiality is enforced through double encryption at rest, TLS 1.3 in transit, and dynamic access controls restricting personal data to authorized users at all times. Integrity is preserved through file integrity monitoring, tamper-evident audit logging, and antivirus, DLP, and CDR scanning. Availability and resilience are supported through high-availability clustering, automated system updates, and disaster recovery configurations. Embedded firewalls, AI-based intrusion detection, and assume-breach architecture ensure processing systems remain secure and operational even under active threat conditions.

The information provided in this guide does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available in this guide are for general informational purposes only. Information in this guide may not constitute the most up-to-date legal or other information. Add-on options are included in this guide and are required to support compliance.