kiteworks

kiteworks for Data Sovereignty
Global Data Privacy Compliance

Enforce US and EU global data residency policies by restraining data storage to physical geographical boundaries to meet regional data security and compliance requirements.

With the invalidation of the Safe Harbor Agreement, organizations with offices in the European Union that share personal data with offices in the United States are now required to adopt adequate safeguards to comply with the European Union and individual country national security controls and privacy laws regarding the transfer of personal data outside of the European Economic Area (EEA).

US and EU Data Protection and Compliance

The European Commission's Directive on Data Protection states that personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. United States organizations with storage facilities in Europe are bound to the Patriot Act. In order for United States organizations to provide an adequate level of protection for European personal data, the data and metadata must reside in Europe, but in a way that ensures that the data is subjected to the laws of the country where it is stored.

Enforcing Data Sovereignty Policies

kiteworks by Accellion offers a viable solution by providing data sovereignty and 100% on-premises, private cloud capabilities to help ensure compliance with European laws that require personal data to stay within its borders. For extended security and control, the solution offers a choice of private cloud deployment; either 100% on-premises, hosted, or in a hybrid configuration. For increased security, the solution offers encryption key rotation.

Geographic Segregation of Data

The kiteworks prescriptive architecture allows for geographic segregation of data by enforcing policies that keep data belonging to EU users on servers physically located in that region. Global organizations with offices in the United States and Europe, and European organizations with offices only in Europe can meet European data security regulations by placing the storage tier for EU user data restricted to Europe and the application tier within the country with the strictest privacy laws.

Private Cloud – Extended Security and Control

The kiteworks private cloud deployment architecture ensures availability, integrity, and confidentiality of information; and is preferred by many enterprises and government agencies for its enhanced information security and control capabilities.

✔ Key Benefits

- Compliance with U.S.-EU and global privacy regulations
- Achieve data sovereignty
- Highest levels of security and control
- Enterprise-grade scalability for global enterprise deployments
- Business agility with rapid ROI
- Network bandwidth optimization

✪ Key Features

- Enforce geographical data residency policies
- 100% on-premises or hosted private cloud deployment
- Multi-tier modular architecture
- Deploy in VMware and Hyper-V virtual environments
- Support for S3 and Atmos storage
- Ownership of encryption keys
- Configurable storage
- Authentication via LDAP and two-factor integration
- Single sign-on via SAML
- User self-provisioning

"With the looming invalidation of the Safe Harbor agreements, organizations need to find an alternative solution to storing data in Europe and they must do so quickly, efficiently and in compliance with EU standards."

---

kiteworks Deployment Options

Private On-Premise
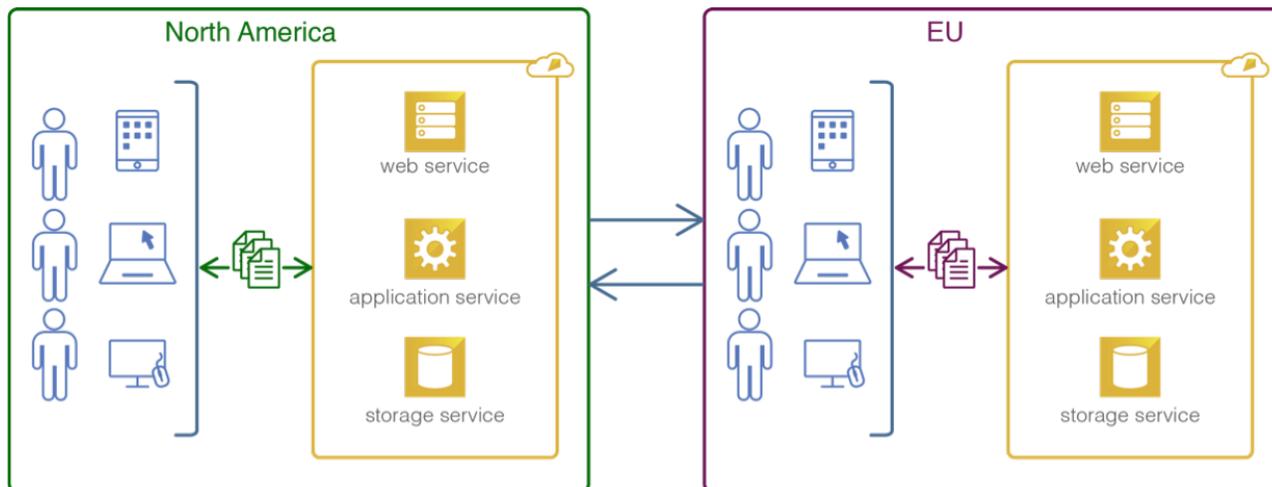Highest levels of security and control

Private Hosted
High security without capital investment

Hybrid
Ideal for remote offices and sites

Accellion

Data Sovereignty and Global Deployments

Enforce data sovereignty rules based on user location

Private Cloud On-Premises

Located inside the firewall, kiteworks 100% on-premises deployments are owned and controlled by the IT organization; allowing data to be solely owned and managed by enterprises, rather than delegated to third-party cloud providers. Furthermore, the organization itself controls the encryption keys and Accellion does not have any access to organization content.

Deploying kiteworks as a private cloud on-premises solution, is as simple as a software download; enabling rapid enterprise-wide deployment. Additional virtual instances and storage capacity can be quickly provisioned to provide for growing needs.

The kiteworks multi-tiered architecture allows the web, application, and storage tiers to separately placed in different geographical locations. This enables a deployment architecture such that the application and storage tiers for EU users are maintained in that geographical region, thus helping meet compliance with European privacy regulations.

Private Cloud Hosted

With the kiteworks private cloud hosted solution, Accellion handles the installation process, while the IT organization manages policies and users, configures server roles, and manages software updates. Files and reporting are only available to authorized users within the organization. The organization itself controls the encryption keys and Accellion does not have any access to your organization's data.

Global private cloud deployments can be architected such that the application and storage tiers for EU users are maintained in that geographical region, thus enabling compliance with European privacy regulations.

Private Cloud Hybrid

kiteworks deployment options can also be mixed and matched, by combining the control of on-premises file sharing with the ubiquitous accessibility of hosted deployments. Private cloud hosted deployments of kiteworks give organizations the opportunity to leverage cloud computing infrastructure and resources, while ensuring that data is not co-mingled. Organizations can immediately take advantage of cloud infrastructure to handle spikes in usage and bandwidth needs.

As with the on-premises and private cloud hosted deployments, hybrid environments can also be setup such that the application and storage tiers for EU users are maintained in that geographical region, thus enabling compliance with European privacy regulations.

Increased Security

Encryption Key Rotation

kiteworks administrators additionally have the flexibility to rotate encryption keys. First, each file is encrypted with its own encryption key. An administrator is able to protect all encryption keys with a passphrase for an additional level of security and this can be rotated as needed. Lastly, the encryption keys for server-to-server communication are automatically rotated each month.

For additional information: www.accellion.com/kiteworks

Accellion