Kiteworks

Data Sovereignty and GDPR

14 Sensitive Content Communication Use Cases Using Kiteworks

Introduction

In today's increasingly digital and global business environment, organizations must navigate complex regulations around data privacy, security, and sovereignty. With more sensitive content being created and shared across borders and jurisdictions, understanding data protection concepts like sovereignty is crucial.

This eBook examines data sovereignty and its relationship to the EU's General Data Protection Regulation (GDPR):

- What is data sovereignty and why is it important
- How data sovereignty relates to privacy, localization, and residency
- Landmark cases establishing data sovereignty
- GDPR's data residency requirements
- Approaching data sovereignty with cloud providers
- Ensuring GDPR compliance

Gaining insight into these issues helps organizations manage regulatory compliance, avoid data privacy violations, and build trust with customers. The eBook wraps up by identifying 14 sensitive content communication data sovereignty and GDPR use cases and how Kiteworks helps organizations address each one.

What Is Data Sovereignty?

Data sovereignty is the concept that information, and the protection and management of that information, belongs to the nation or individual in which it originates. It is the belief that data belonging to a French citizen, for example, should not be subject to U.S. laws just because it is stored or processed by an American company. The data instead should remain in France, subject to French and EU laws.

This concept regulates how data is governed and secured based on where it was collected, not where the collector is located. It aims to protect individuals' privacy rights and give them control over their personal data.

Why Is Data Sovereignty Important?

Data sovereignty provides several key benefits:

- Protects individuals' personal data from unauthorized access or use based on jurisdiction
- Assures companies that customer data will remain secured under relevant national laws
- Allows businesses to be confident using cloud storage and digital services that involve cross-border data transfers
- Ensures companies' proprietary data remains protected if they change service providers

Without data sovereignty, organizations risk legal liability, reputational damage, and loss of customer trust if unable to properly secure data. Individuals lose control over their personal information.

Data Sovereignty vs. Related Concepts

Data sovereignty is often conflated with related data protection concepts:

- Data residency refers to storing data within specific jurisdictions for regulatory compliance or business purposes
- Data localization requires that data stays within the country where it was collected, such as per GDPR rules
- Indigenous data sovereignty involves native groups controlling data privacy rights in their nations

While related, these concepts have distinct meanings around governing and securing data based on its origin.

Landmark Cases Establishing Data Sovereignty

Several landmark legal cases have shaped modern understanding of data sovereignty:

PRISM and the PATRIOT Act: The NSA PRISM program collected data internationally, including on foreign nationals, per the PATRIOT Act. This prompted concerns about U.S. overreach into other jurisdictions.

Microsoft vs. United States: Microsoft refused to provide customer data stored in Ireland to U.S. authorities. The case debated whether the U.S. can compel data disclosure across jurisdictions. It led to the CLOUD Act, which imposed limits on cross-border data requests.

These cases highlighted the need for clear rules governing cross-border data management and enhanced protections for data sovereignty.

GDPR Data Residency Requirements

The EU's GDPR imposed strict data sovereignty requirements in 2018. Under GDPR, EU residents' personal data must be stored and processed within the EU. Companies must obtain consent to collect data, implement security controls, and report breaches promptly.

GDPR also gives EU residents rights to access, modify, and delete their data. By keeping data within the EU, GDPR aims to uphold these rights and privacy standards. Noncompliance can trigger major fines upwards of 4% of global revenue.

Approaching Data Sovereignty With Cloud Providers

When selecting cloud services, organizations should assess providers' data sovereignty capabilities:

- **Server locations:** Use providers with in-country servers meeting localization needs
- **Privacy laws:** Understand applicable laws and provider practices for each jurisdiction
- **Consumer rights:** Clarify practices for providing access, deletion, and other consumer rights
- **Governance tools:** Ensure providers offer robust access controls, auditing, reporting, retention, and security

Vetting providers on these factors helps maintain data sovereignty across cloud environments.

Achieving GDPR Compliance With Data Sovereignty

To comply with GDPR, organizations must:

- Store and process EU personal data only within the EU
- Limit data sharing strictly to necessary, authorized purposes
- Obtain explicit consent to collect and use EU user data
- Provide mechanisms for EU data subjects to access and delete their information
- Implement strong technical controls like encryption to secure data
- Report any breaches involving EU data within 72 hours
- Document compliance efforts through data protection assessments

Adhering to GDPR's data sovereignty mandates requires both organizational commitment and the right technology tools for securing sensitive data.

14 Sensitive Content Communication Data Sovereignty and GDPR Use Cases

With the above in mind, organizations governed by GDPR must ensure they comply with data sovereignty compliance with sensitive content communications. Healthcare organizations can use the following 14 use cases to evaluate their regulatory compliance risk. Each use case also includes a discussion how Kiteworks addresses each one.

Use Case	Description	Kiteworks Solution
1. Data Residency	Organizations are often faced with the challenge of ensuring that their data resides in a specific geographical location due to data sovereignty laws. This becomes particularly difficult when using cloud services, which often distribute data across multiple locations. The challenge is to maintain control over where data is stored while still leveraging the benefits of cloud services.	Kiteworks offers a flexible deployment model that allows organizations to choose where their data resides. This could be on-premises, in the cloud, or a hybrid of both. This ensures compliance with data sovereignty laws and gives organizations control over their data.
2. Data Transfer	Transferring data across borders can be a complex process due to data sovereignty laws. This is especially true in regions like the EU where GDPR is enforced. Organizations need to ensure that data is transferred securely and only to locations that comply with data sovereignty laws.	Kiteworks provides secure, compliant data transfer capabilities. It ensures that data is encrypted during transit and at rest. This means that data is always secure, even when being transferred across borders.
3. Data Access	Unauthorized access to sensitive data can lead to noncompliance with GDPR. Organizations need to ensure that only authorized individuals can access sensitive data. They also need to provide detailed audit logs for accountability and compliance.	Kiteworks offers robust access controls, ensuring that only authorized individuals can access sensitive data. It also provides detailed audit logs. This means that organizations can demonstrate compliance and maintain accountability.
4. Data Deletion	Under GDPR, individuals have the right to request the deletion of their personal data. Organizations often struggle to locate and delete this data across their systems. The challenge is to ensure that all personal data can be located and deleted promptly upon request.	Kiteworks provides tools for locating and deleting personal data across the system. This ensures compliance with GDPR's right to erasure. It also means that organizations can respond promptly to deletion requests.

Use Case	Description	Kiteworks Solution
5. Data Breach Notification	GDPR requires organizations to notify affected individuals and authorities within 72 hours of discovering a data breach. Organizations need to be able to identify potential breaches quickly and notify the relevant parties promptly.	Kiteworks' advanced threat detection capabilities can identify potential breaches quickly. This enables organizations to meet GDPR's notification requirements. It also means that organizations can respond promptly to potential breaches.
6. Data Protection by Design	GDPR requires organizations to implement data protection measures from the onset of system design. Organizations need to ensure that their systems are designed with data protection in mind. This includes features like encryption, access controls, and audit logs.	Kiteworks' platform is designed with security in mind. It incorporates features like encryption, access controls, and audit logs from the ground up. This means that organizations can ensure data protection from the onset of system design.
7. Data Processing Records	GDPR requires organizations to keep detailed records of their data processing activities. Organizations need to be able to maintain accurate records of all data processing activities. This includes who accessed what data, when, and why.	Kiteworks provides comprehensive logging and reporting capabilities. This makes it easy for organizations to maintain accurate records of their data processing activities. It also means that organizations can demonstrate compliance with GDPR's record-keeping requirements.
8. Data Protection Impact Assessments	GDPR requires organizations to conduct Data Protection Impact Assessments (DPIAs) for high-risk data processing activities. Organizations need to have visibility and control over data processing activities to conduct effective DPIAs.	Kiteworks' platform provides the necessary visibility and control over data processing activities and detailed reporting through audit logs. This enables organizations to conduct effective DPIAs. It also means that organizations can identify and mitigate risks associated with data processing activities.
9. Data Protection Officer	GDPR requires organizations to appoint a Data Protection Officer (DPO) in certain circumstances. The DPO needs to have the necessary tools to monitor compliance, assess risks, and liaise with supervisory authorities.	Kiteworks' platform provides the DPO with the necessary tools to monitor compliance. This includes features for assessing risks and liaising with supervisory authorities. This means that the DPO can effectively fulfill their role and ensure compliance with GDPR.

Use Case	Description	Kiteworks Solution
10. Data Minimization	GDPR requires organizations to limit data collection to what is necessary for the intended purpose. Organizations need to have controls over what data is collected and how it is used to enforce data minimization principles.	Kiteworks' platform helps organizations enforce data minimization principles. Kiteworks' secure web forms provide controls over what data is collected and how it is used. This means that organizations can ensure they are only collecting the data that is necessary for the intended purpose.
11. Privacy by Default	GDPR requires that organizations implement privacy settings at the highest level by default. This means that without manual change from the user, the strictest privacy settings should apply. This can be a challenge for organizations to implement effectively.	Kiteworks' platform is designed with privacy in mind. It implements the highest level of privacy settings by default, ensuring that without any manual change from the user, the strictest privacy settings apply. This helps organizations comply with GDPR's privacy by default requirement.
12. Data Retention	GDPR requires organizations to not hold onto personal data for longer than necessary. Determining the appropriate retention period can be challenging, and organizations must have mechanisms in place to delete data after this period.	Kiteworks provides features that allow organizations to set data retention periods and automatically delete data after this period. This ensures that organizations do not hold onto personal data for longer than necessary, thereby complying with GDPR's data retention requirements. Kiteworks also enables organizations and users to establish expiration rights to content to the level of users.
13. Third-party Data Sharing	GDPR requires organizations to ensure that any third parties they share data with also comply with GDPR. This can be challenging, as organizations must vet third parties and have legal agreements in place.	Kiteworks provides features that allow organizations to securely share data with third parties. It also provides audit logs to ensure that third parties are also complying with GDPR. This helps organizations maintain control over their data, even when shared with third parties.
14. Data Encryption	GDPR requires that personal data be encrypted both in transit and at rest. This is to ensure that even if data is intercepted or accessed without authorization, it remains unintelligible and useless to the attacker.	Kiteworks ensures that all data is encrypted both in transit and at rest. This provides an additional layer of security and ensures that even if data is intercepted, it cannot be accessed or used, thereby complying with GDPR's encryption requirements.

EBOOK

Managing Data Sovereignty Risks Across Use Cases

Data sovereignty is a crucial issue that organizations must address to manage regulatory compliance, privacy risk, security threats, and customer trust. As cross-border data flows accelerate, understanding sovereignty rights and regulations for protecting data based on jurisdiction is imperative. By leveraging solutions that provide data governance, user control, localized storage, and compliance reporting, companies can better navigate requirements like GDPR. A proactive strategy for data sovereignty ultimately reduces risk and helps build durable trust with customers and partners.

Kiteworks

www.kiteworks.com

September 2023