Kiteworks

COMPLIANCE BRIEF

Navigating the EU-U.S. Data Privacy Framework

Leveraging Kiteworks' Features for Adherence to EU-U.S. Data Privacy Framework's Stringent Demands

The European Commission has officially approved its adequacy decision for the EU-U.S. Data Privacy Framework, ensuring that the United States offers an adequate level of protection for personal data transferred from the EU to U.S. companies. This decision allows the safe flow of personal data without the need for additional data protection measures. The new EU-U.S. Data Privacy Framework incorporates binding safeguards to address concerns raised by the European Court of Justice. These safeguards include limiting access to EU data by U.S. intelligence services to what is necessary and proportionate, as well as establishing a Data Protection Review Court (DPRC) accessible to EU individuals. Compared to its predecessor, the Privacy Shield, this Framework represents a significant improvement, enabling the DPRC to order data deletion if collected in violation of the new safeguards.

President Ursula von der Leyen expressed that the new framework fosters trust among citizens regarding data safety and strengthens economic ties between the EU and the U.S. U.S. companies can join the Framework by committing to comply with a detailed set of privacy obligations, ensuring continuity of protection when sharing data with third parties. EU individuals will have access to redress mechanisms if their data is mishandled by U.S. companies, including independent dispute resolution and an arbitration panel. Additionally, the U.S. legal framework provides safeguards for access to data by U.S. public authorities, particularly for criminal law enforcement and national security purposes, limited to what is necessary. The U.S.'s safeguards will facilitate transatlantic data flows in general, extending to other transfer tools like standard contractual clauses and binding corporate rules. This decision marks a significant step in promoting safe data flows between the EU and the U.S., providing legal certainty to companies on both sides and reaffirming shared values.

Securely Adopt Measures to Protect Personal Information

To be compliant with the EU-U.S. Data Privacy Framework, organizations must adhere to certain security standards, and organizations creating, maintaining, using, or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse, and unauthorized access, disclosure, alteration, and destruction, taking into due account the risks involved in the processing and the nature of the personal data. Kiteworks is a transformative solution for organizations seeking to align with the U.S.-EU Adequacy Decision.

Solution Highlights

- **Robust data security**
- **DLP seamless integration**
- **Authentication enhancements**
- **Granular permissions**
- **Explicit consent collection**
- **User access empowerment**

It ensures data security through AES encryption, both in motion and at rest, with 256-bit encryption. Files are shielded during transit between servers via SSL/TLS and AES encryption. Dual encryption layers, including FIPS 140-3-approved AES-256-bit disk encryption and individual file encryption, fortify data protection. Kiteworks seamlessly integrates with DLP products, enabling data-aware sharing restrictions. Authentication options like SAML SSO Integration and two-factor authentication bolster security. It's the only FedRAMP-authorized platform for file sharing, managed file transfer, and email data, meeting compliance standards such as CMMC 2.0 and HIPAA. Granular permissions, encryption, and audit logs prevent loss, misuse, unauthorized access, and disclosure. Kiteworks' comprehensive features ensure data integrity, availability, and confidentiality, making it easier to stay compliant.

Provide Clear Notice to Individuals When Gathering Personal Information and Create Transparency and Protection When Individuals Opt In

The Framework also lays out a few different tracking requirements around notice, choice, accountability for onward transfer, access, and recourse, enforcement, and liability. First, to be compliant with this adequacy decision, organizations must give individuals notice in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable. In adherence with the Framework, Kiteworks provides secure web forms and data collection mechanisms that can be used to obtain explicit consent from users. These forms can be customized to outline the purpose of data collection, usage, and third-party involvement.

According to the Framework, an organization must offer individuals the opportunity to choose whether their personal information is to be disclosed to a third party or to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. For sensitive information (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information specifying the sex life of the individual), organizations must obtain affirmative express consent from individuals if such information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. Kiteworks aligns seamlessly with the U.S.-EU Framework's data control emphasis. It facilitates compliance by offering secure web forms for explicit consent collection and data customization. Users can securely access and transfer personal information to other entities, reflecting the Framework's intent. Kiteworks' secure storage, audit logs, and compliance reporting cater to data security requirements. The reporting feature benefits both end-users and admins, showcasing user activities through the Admin Console and the Kiteworks web application. This holistic solution enables organizations to navigate the intricate data control demands outlined in the Framework while ensuring individuals retain authority over their personal data.

Organizations looking to adhere to the Frameworks must also grant individuals access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Notice and Choice Principles . Kiteworks offers robust support for individual access rights, granting users the ability to not only access their personal data but also gain insight into how their data is being processed. The platform enhances data portability, providing users with a secure avenue to access, transfer, and download their personal information. By upholding relevant data access permissions, as well as implementing secure locking and versioning of repositories, Kiteworks guarantees that users can engage with their data in a controlled and secure manner.

Lay Out Accountability for Onward Transfer

Organizations also must take ownership of accountability for onward transfer; to transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. Kiteworks plays a pivotal role in adhering to the U.S.-EU Framework's data control principles. This Framework mandates careful handling of personal information when transferring it to third parties, whether as controllers or agents. Kiteworks not only supports the Notice and Choice Principles but actively helps organizations comply with them. The platform provides secure web forms and customizable mechanisms for explicit consent collection, ensuring individuals understand data usage purposes and third-party involvement.

Kiteworks empowers organizations to establish opt-in mechanisms, enabling users to actively provide their information. Detailed consent forms elucidate data use, sharing, and retention, enabling informed choices. The platform also supports minor consent procedures, ensuring compliance with relevant laws.

Furthermore, Kiteworks strengthens data security through its least-privilege access control model. Admins finely manage access at individual and role levels, enhancing protection against unauthorized data access. Nested folder controls enable granular data and permission management. Features like real-time editing, view-only access, and controlled downloading are modulated based on roles and data sensitivity. Admins can establish domain blocking, geofencing, and feature permissions, refining access based on location and domain. In essence, Kiteworks encapsulates the Framework's principles and provides invaluable tools for seamless compliance, reinforcing data control and security for organizations.

Ensure Enforcement of Compliance and Limit Liability

Organizations looking to be compliant with the Framework must practice effective privacy protection, which includes robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by noncompliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and regarding cases of noncompliance. Kiteworks offers Advanced Governance that provides GDPR Compliance Reports. These reports help organizations meet the requirements of GDPR and automatically gather all the relevant information needed for audits. This includes data on how personal data is collected, stored, used, and shared within the organization. These reports also highlight discrepancies and potential compliance issues, allowing organizations to address them before an audit. This proactive approach helps organizations maintain compliance and avoid penalties associated with GDPR noncompliance. All events are logged and presented in a report that is available to application admins and system admins of Kiteworks. These admins have access to full audit logs of all actions taken on the system. In a broader scope, reports also allow organizations to monitor relevant operations and evaluate policy control settings. This helps to ensure that the organization's data protection policies are correctly implemented and effective. These GDPR Compliance Reports also provide evidence to prove to auditors that data checks and scans were applied. This includes checks for malware (AV and ATP), privacy (DLP), and other potential security threats.

Monitor Data Integrity and Purpose Limitation

To be compliant with this adequacy decision, organizations must adhere to data integrity and purpose limitation. These organizations must be consistent with the Principles, and personal information must be limited to the information that is relevant for the purposes of processing. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. Kiteworks implements a stringent approach to user access, ensuring that individuals are granted the least access necessary for their roles, mitigating the risk of both inadvertent and intentional data misuse. Admins wield fine-grained control over access, dictating data, structure, and permission management. The platform enables nuanced collaboration and view-only with watermarking, downloading, and blind uploading. This level of control guarantees that users have access only to essential data. Kiteworks further bolsters its security through robust auditing and reporting functionalities. Admins gain a comprehensive view of all user activities within the system, strengthening the enforcement of the principle of least privilege. This meticulous tracking of user actions not only safeguards data but also ensures the efficacy of the least-privilege approach.