



# Kiteworks Supports Compliance With the American Privacy Rights Act

## Comprehensive Features for Data Protection, Individual Rights, and Third-party Oversight

The American Privacy Rights Act is a comprehensive federal privacy legislation that aims to protect individuals' personal data and give them more control over how their information is collected, used, and shared. The Act applies to covered entities, which include companies subject to the FTC Act, common carriers, and certain nonprofit organizations. It also governs service providers that process data on behalf of covered entities. The Act sets forth requirements for data minimization, transparency, individual rights (such as access, correction, and deletion), data security, and the use of algorithms. It establishes additional obligations for large data holders, covered high-impact social media companies, and data brokers. The Act provides for enforcement by the FTC, state Attorneys General, and individuals through a private right of action. Companies that fall within the scope of the Act will need to review their data practices and make necessary changes to comply with its requirements.

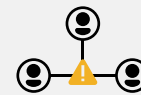
### Access Controls and Least-privilege Defaults Support Data Minimization

Section 3 establishes data minimization requirements for covered entities and service providers. They must limit data collection, processing, retention, and transfer to what is necessary and proportionate to provide requested products or services or for other permitted purposes. Special protections apply to sensitive data, biometric information, and genetic information, generally requiring affirmative express consent for collection, processing, retention, and transfer. Kiteworks' robust access controls and least-privilege defaults guarantee that data is only accessible on an as-needed basis. Comprehensive, timely, and detailed audit logs enable the tracking of all data-related activities for compliance monitoring purposes. Kiteworks' secure web forms streamline the consent collection process, and users have the ability to request the deletion of their personal information at any time. These features, in addition to stringent data security measures, empower organizations to minimize data collection and processing in accordance with the Act's provisions.

### Individual Control Over Covered Data Enables Individuals to Access, Correct, and Delete Personal Data

Individuals are granted the right to access, correct, delete, and export their covered data upon a verified request to a covered entity within Section 5. The Act specifies requirements for the format, frequency, cost, timing, and verification of such requests, as well as permissible exceptions.

## Solution Highlights



**Granular access controls**



**Least-privilege defaults**



**Secure web forms**



**Immutable audit logs**



**Seamless integration with SIEM systems**

Kiteworks provides features that help covered entities comply with these obligations. Its user-friendly interface allows individuals to securely access and correct their personal data. Users can also request deletion of their data, which is permanently removed in accordance with applicable laws. Kiteworks facilitates data portability by enabling users to securely export their personal information. The platform maintains detailed audit logs and reports, including file deletion activities, which can demonstrate compliance with data handling requirements. Kiteworks' customizable web forms and notification features further support the collection of user consent. These capabilities empower covered entities to respect individuals' rights over their data, as mandated by the Act.

### Verify Service Providers and Third-party Compliance With Immutable Audit Logs and SIEM Integrations

Within Section 11 of the American Privacy Rights Act, requirements are set for service providers and third parties that handle covered data on behalf of covered entities. Service providers must adhere to the covered entity's instructions, assist with consumer rights requests, and maintain reasonable safeguards. They must also enter into contracts with covered entities that govern data processing procedures and prohibit unauthorized activities. Third parties must also rely on covered entities' representations about data treatment. Kiteworks supports compliance with these provisions through its robust access controls, least-privilege defaults, and comprehensive audit logging capabilities. Its Enterprise Connect feature ensures that external content is subject to the same access controls as data stored directly in Kiteworks. The platform's detailed audit logs, which capture all relevant activities without throttling, can be seamlessly integrated with SIEM systems to detect and respond to security threats. These features help covered entities exercise due diligence and maintain control over data handled by service providers and third parties.

Kiteworks offers a robust suite of features that directly support compliance with the American Privacy Rights Act. By providing granular access controls, least-privilege defaults, and secure web forms, Kiteworks empowers organizations to minimize data collection, obtain user consent, and respect individual rights. Its comprehensive, immutable audit logs and seamless integration with SIEM systems enable covered entities to monitor data-related activities, detect security threats, and demonstrate compliance. The Enterprise Connect feature ensures consistent access control across repositories, while customizable web forms and notification features facilitate user consent collection. With these powerful tools, Kiteworks positions itself as a valuable partner for organizations seeking to navigate the complex landscape of privacy regulations, protect personal data, and maintain the trust of their customers. By leveraging Kiteworks' capabilities, covered entities can confidently adapt to the requirements of the American Privacy Rights Act and strengthen their commitment to data privacy and security.