Kiteworks

COMPLIANCE BRIEF

Kiteworks Enables Compliance With the EU AI Act

Robust Security Measures and Comprehensive Logging Capabilities Facilitate Adherence to Chapters II and III of the EU AI Act

The European Union has made significant strides toward establishing a comprehensive regulatory framework for artificial intelligence (AI) systems with the provisional agreement on the Artificial Intelligence Act (AI Act) in early 2024. This landmark legislation aims to strike a delicate balance between fostering innovation and ensuring the protection of fundamental rights, health, safety, and the environment. The EU AI Act introduces a risk-based approach to regulating AI systems, with a particular focus on high-risk applications. It sets forth a range of obligations for providers, importers, distributors, and users of AI systems. The application of the EU AI Act's provisions will follow a phased approach, with different sections becoming applicable at various intervals after the regulation's entry into force. The majority of the provisions will come into effect 24 months after the entry into force, allowing stakeholders sufficient time to adapt their practices and ensure compliance. The EU AI Act introduces a range of rules and controls to govern the development, deployment, and use of AI systems in the EU. These provisions are designed to mitigate the risks associated with AI while promoting trust and accountability in the technology. Kiteworks supports compliance with this act. Here's how:

Strict Access Controls Enable Protection of Data

The EU AI Act Chapter II prohibits certain high-risk AI practices, and Kiteworks supports compliance through robust measures. To address Article 9 requirements, open-source libraries are isolated in a sandbox environment, restricting access to sensitive data and functions. Kiteworks supports compliance with Article 10 by implementing strong data governance practices. The platform enables granular access controls and policies, ensuring that users have the least privileges necessary to perform their roles. Data loss prevention (DLP) scanning and encryption for data at rest and in transit further protect sensitive information. Customers retain full control over their encryption keys, guaranteeing data privacy. In accordance with Article 12, Kiteworks maintains comprehensive logging and auditing capabilities, keeping detailed records of all system activities. The zero-trust architecture, as required by Article 15, treats all service communications as untrusted and contains breaches with multiple layers of security controls, including authentication tokens and encryption. These measures, along with high availability and disaster recovery configurations, provide a secure and compliant foundation for organizations implementing AI systems under the EU AI Act.

Solution Highlights

- **Immutable audit logs**
- **Granular access controls**
- **Strict authentication and authorization**
- **Strong double encryption**
- **SIEM integration**

Robust Audit Logs Monitor Data

The EU AI Act Chapter III focuses on high-risk AI systems and the obligations of providers and deployers. Kiteworks supports compliance through its comprehensive logging, reporting, and auditing capabilities. Kiteworks captures all log messages in full without throttling, ensuring complete data for compliance and audits as required by Article 20. In accordance with Articles 16, 23, and 29, the consolidated activity log can be searched, filtered, and sorted, with activities viewable at the system, user, file, folder, or form level. Log entries include key metadata and are appended immediately, enabling real-time monitoring and rapid response to incidents. Kiteworks offers a range of built-in and custom reports that can be generated on-demand or scheduled, providing comprehensive documentation of system activities to support compliance with Article 18. These reports cover various aspects of the system, including user activities, system usage metrics, uploads, downloads, file views, messages, and form activity. Reports can be exported in CSV format, facilitating easy sharing and long-term archiving. The platform's standardized logging format and integration with external SIEM tools like Splunk streamline log analysis and interpretation as required in Article 20. This centralized approach to logging and reporting simplifies cooperation with authorities during audits or investigations as required in Article 23. By providing detailed, tamper-proof logging and reporting features, Kiteworks helps high-risk AI system providers and deployers meet their obligations under the EU AI Act Chapter III.

The European Union's AI Act represents a significant step toward establishing a comprehensive regulatory framework for AI systems. By focusing on high-risk applications and introducing a range of obligations for providers, importers, distributors, and users, the EU AI Act seeks to mitigate risks while promoting trust and accountability in AI technology. Kiteworks, with its robust security measures and comprehensive logging capabilities, is well-positioned to support organizations in achieving compliance with the EU AI Act's requirements. The platform's zero-trust principles, granular access controls, data loss prevention scanning, immutable audit logs, and encryption features enable compliance with Chapter II. Simultaneously, Kiteworks' tamper-proof logging, detailed reporting, and integration with external SIEM tools facilitate adherence to Chapter III. As organizations navigate the complexities of the EU AI Act, Kiteworks provides a secure foundation for implementing high-risk AI systems, ensuring the protection of fundamental rights, health, safety, and the environment.