Kiteworks

COMPLIANCE-INFORMATION

Kiteworks ermöglicht die Einhaltung des EU-KI-Gesetzes

Robuste Sicherheitsmaßnahmen und umfassende Protokollierungsmöglichkeiten erleichtern die Einhaltung der Kapitel II und III des KI-Gesetzes der EU.

Mit der vorläufigen Einigung auf das Gesetz über Künstliche Intelligenz (KI-Gesetz) Anfang 2024 hat die Europäische Union große Fortschritte bei der Schaffung eines umfassenden Rechtsrahmens für Systeme der Künstlichen Intelligenz (KI) gemacht. Diese bahnbrechende Gesetzgebung zielt darauf ab, ein empfindliches Gleichgewicht zwischen der Förderung von Innovationen und dem Schutz von Grundrechten, Gesundheit, Sicherheit und Umwelt herzustellen. Das KI-Gesetz der EU führt einen risikobasierten Ansatz zur Regulierung von KI-Systemen ein, wobei der Schwerpunkt auf Anwendungen mit hohem Risiko liegt. Es legt eine Reihe von Verpflichtungen für Anbieter, Importeure, Distributoren und Anwender von KI-Systemen fest. Die Anwendung der Bestimmungen des EU-KI-Gesetzes erfolgt stufenweise, wobei die einzelnen Abschnitte zu unterschiedlichen Zeitpunkten nach Inkrafttreten der Verordnung zur Anwendung kommen. Die meisten Bestimmungen werden 24 Monate nach der Einführung in Kraft treten, so dass die Beteiligten genügend Zeit haben, ihre Verfahren anzupassen und die Einhaltung der Vorschriften sicherzustellen. Das EU-KI-Gesetz führt eine Reihe von Vorschriften und Kontrollen ein, um die Entwicklung, Installation und Nutzung von KI-Systemen in der EU zu regeln. Diese Bestimmungen sollen die mit KI verbundenen Risiken mindern und gleichzeitig das Vertrauen in die Technologie und die Verantwortlichkeit fördern. Kiteworks unterstützt die Einhaltung dieses Gesetzes folgendermaßen:

Strenge Zugriffskontrollen ermöglichen den Schutz von Daten

Das Kapitel II des KI-Gesetzes der EU, verbietet bestimmte risikoreiche KI-Verfahren, und Kiteworks unterstützt die Einhaltung durch robuste Maßnahmen. Um die Anforderungen von Artikel 9 zu erfüllen, werden Open-Source-Bibliotheken in einer Sandbox-Umgebung isoliert und der Zugriff auf sensible Daten und Funktionen eingeschränkt. Kiteworks unterstützt die Einhaltung von Artikel 10 durch die Implementierung strenger Data Governance-Verfahren. Die Plattform ermöglicht granulare Zugriffskontrollen und -richtlinien, die sicherstellen, dass Anwender nur die für die Ausübung ihrer Aufgaben erforderlichen Privilegien erhalten. Data Loss Prevention (DLP) Scanning und Verschlüsselung der Daten im ruhenden Zustand und während der Übertragung schützen sensible Informationen zusätzlich. Die Kunden behalten die volle Kontrolle über ihre Verschlüsselungscodes, so dass der Datenschutz gewährleistet ist. In Übereinstimmung mit Artikel 12 verfügt Kiteworks über umfassende Protokollierungs- und Auditing-Funktionen, die alle Systemaktivitäten detailliert aufzeichnen. Die in Artikel 15 geforderte Zero-Trust-

Highlights der Lösung

- **Unveränderliche Audit-Protokolle**
- **Granulare Zugriffskontrollen**
- **Strenge Authentifizierung und Autorisierung**
- **Starke doppelte Verschlüsselung**
- **SIEM-Integration**

Architektur behandelt die gesamte Servicekommunikation als nicht vertrauenswürdig und vermeidet Datenschutzverstöße durch mehrschichtige Sicherheitskontrollen, einschließlich Authentifizierungstoken und Verschlüsselung. Diese Maßnahmen bilden zusammen mit Hochverfügbarkeits- und Disaster-Recovery-Konfigurationen eine sichere und gesetzeskonforme Grundlage für Unternehmen, die KI-Systeme gemäß dem EU-KI-Gesetz implementieren.

Robuste Audit-Protokolle überwachen die Daten

Das Kapitel III des EU-KI-Gesetzes konzentriert sich auf risikobehaftete KI-Systeme und die Verpflichtungen von Anbietern und Installationsbetreibern. Kiteworks unterstützt die Einhaltung der Vorschriften durch seine umfassenden Protokollierungs-, Berichts- und Auditing-Funktionen. Kiteworks erfasst alle Log-Meldungen vollständig und ohne Drosselung und gewährleistet so vollständige Daten für Compliance und Audits, wie in Artikel 20 gefordert. In Übereinstimmung mit den Artikeln 16, 23 und 29 kann das konsolidierte Aktivitätsprotokoll durchsucht, gefiltert und sortiert werden, wobei die Aktivitäten auf System-, Anwender-, Datei-, Ordner- oder Formularebene angezeigt werden können. Die Log-Einträge enthalten wichtige Metadaten und werden sofort angehängt, was eine Überwachung in Echtzeit und eine schnelle Reaktion auf Vorfälle ermöglicht. Kiteworks bietet eine Reihe integrierter und benutzerdefinierter Berichte, die bei Bedarf oder nach Zeitplan erstellt werden können und eine umfassende Dokumentation der Systemaktivitäten zur Unterstützung der Einhaltung von Artikel 18 liefern. Diese Berichte decken verschiedene Aspekte des Systems ab, einschließlich Anwenderaktivitäten, Systemnutzungsmetriken, Uploads, Downloads, Dateiansichten, Nachrichten und Formularaktivitäten. Die Berichte können im CSV-Format exportiert werden, was die Weitergabe und langfristige Archivierung erleichtert. Das standardisierte Logging-Format der Plattform und die Integration mit externen SIEM-Tools wie Splunk rationalisieren die Analyse und Interpretation von Protokollen, wie in Artikel 20 gefordert. Dieser zentralisierte Logging- und Reporting-Ansatz vereinfacht die Zusammenarbeit mit den Behörden bei Audits oder Ermittlungen, wie in Artikel 23 gefordert. Durch die Bereitstellung detaillierter, manipulationssicherer Logging- und Berichtsfunktionen hilft Kiteworks Anbietern und Installationsbetreibern von risikobehafteten KI-Systemen, ihre Verpflichtungen gemäß Kapitel III des EU-KI-Gesetzes zu erfüllen.

Das KI-Gesetz der Europäischen Union ist ein bedeutender Schritt zur Schaffung eines umfassenden Regulierungsrahmens für KI-Systeme. Durch die Konzentration auf risikoreiche Anwendungen und die Einführung einer Reihe von Verpflichtungen für Anbieter, Importeure, Distributoren und Anwender versucht das EU-KI-Gesetz, die Risiken zu mindern und gleichzeitig das Vertrauen in die KI-Technologie und die Verantwortlichkeit zu fördern. Kiteworks ist mit seinen robusten Sicherheitsmaßnahmen und umfassenden Logging-Funktionen gut positioniert, um Unternehmen bei der Einhaltung der Anforderungen des EU-KI-Gesetzes zu unterstützen. Die Zero-Trust-Prinzipien der Plattform, granulare Zugriffskontrollen, Scans zur Vermeidung von Datenverlusten, unveränderliche Audit-Protokolle und Verschlüsselungsfunktionen ermöglichen die Einhaltung von Kapitel II. Gleichzeitig erleichtern die manipulationssichere Protokollierung, die detaillierte Berichterstattung und die Integration mit externen SIEM-Tools die Einhaltung von Kapitel III von Kiteworks. Unternehmen, die sich mit der Komplexität des EU-KI-Gesetzes auseinandersetzen, erhalten mit Kiteworks eine sichere Grundlage für die Implementierung von risikobehafteten KI-Systemen, die den Schutz von Grundrechten, Gesundheit, Sicherheit und Umwelt gewährleisten.