Kiteworks

COMPLIANCE BRIEF

Kiteworks garantit la conformité avec la loi européenne sur l'IA

Les mesures de sécurité et de traçabilité de Kiteworks répondent aux exigences des chapitres II et III de la loi sur l'IA de l'UE

L'Union européenne a marqué une avancée significative dans la réglementation en matière d'IA avec l'accord provisoire sur l'Artificial Intelligence Act (AI Act) début 2024. Ce texte historique vise à trouver le juste équilibre entre la promotion de l'innovation et la protection des droits fondamentaux, de la santé, de la sécurité et de l'environnement. La législation sur l'IA introduit une approche fondée sur les risques pour réglementer les systèmes d'IA, en mettant l'accent sur les applications à haut risque. Le texte prévoit une série d'obligations pour les fournisseurs, les importateurs, les distributeurs et les utilisateurs de systèmes d'IA. Son application se fera de manière progressive, avec des articles applicables à différentes échéances. La majorité des dispositions seront effectives 2 ans après leur entrée en vigueur, pour laisser le temps aux organisations concernées d'adapter leurs pratiques et de se conformer à la réglementation. La loi introduit une série de règles et de contrôles pour régir le développement, le déploiement et l'utilisation des systèmes d'IA dans l'UE. Elle vise à atténuer les risques associés à l'IA tout en encourageant la confiance et la responsabilité dans cette technologie. Kiteworks est conforme à cette loi :

Des contrôles d'accès stricts pour protéger les données

Le chapitre II de la loi européenne sur l'IA interdit certaines pratiques d'IA très risquées, et Kiteworks soutient cette exigence grâce à des mesures de sécurité très strictes. Pour répondre aux exigences de l'article 9, les bibliothèques open source sont isolées dans un environnement sandbox, ce qui limite l'accès aux données et fonctions sensibles. De plus, Kiteworks satisfait aux exigences de l'article 10 en instaurant des pratiques de gouvernance des données rigoureuses. La plateforme prévoit des contrôles et des politiques d'accès granulaires, conformément au principe du moindre privilège. La prévention des pertes de données (DLP) et le chiffrement des données au repos et en transit protègent également les informations sensibles. Par ailleurs, les clients conservent le contrôle total de leurs clés de chiffrement, pour assurer la confidentialité des données. Et comme l'impose l'article 12, Kiteworks assure une traçabilité totale, en conservant des enregistrements détaillés de toutes les activités du système. Enfin, l'article 15 exige une architecture zéro trust, et Kiteworks traite toutes les communications de service comme non fiables et prévient les violations grâce à de multiples couches de contrôles de sécurité (jetons d'authentification et chiffrement). Ces mesures, associées aux configurations de reprise après sinistre, constituent une base sûre et conforme pour les organisations utilisant des systèmes d'IA en vertu de la loi européenne.

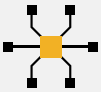
Avantages de la solution :

Journaux d'audit immuables

Contrôles d'accès granulaires

Authentification et autorisation strictes

Double chiffrement fort



Intégration SIEM

Des journaux d'audit robustes pour surveiller les données

Le chapitre III de la loi se concentre sur les systèmes d'IA à haut risque et sur les obligations des fournisseurs et des déployeurs. Kiteworks offre des fonctions complètes de journalisation, de reporting et d'audit et capture tous les messages sans restriction, utile pour la conformité et les audits et conformément à l'article 20. En application des articles 16, 23 et 29, le journal d'activité consolidé peut être recherché, filtré et trié, les activités pouvant être visualisées au niveau du système, de l'utilisateur, du fichier, du dossier ou du formulaire. Les entrées du journal comprennent des métadonnées clés et sont ajoutées immédiatement, ce qui permet une surveillance en temps réel et une réponse rapide aux incidents. Kiteworks permet de générer des reportings personnalisés à la demande ou programmés, pour obtenir une documentation complète des activités du système (article 18). Ces reportings contiennent notamment les activités des utilisateurs, les paramètres du système, les téléchargements, les visualisations de fichiers, les messages et les formulaires. Ils sont téléchargeables au format CSV pour faciliter leur partage et archivage à long terme. Le format de journalisation standardisé de la plateforme et l'intégration avec des outils SIEM externes tels que Splunk simplifient leur analyse et leur interprétation, comme préconisé par l'article 20. Cette approche centralisée simplifie la coopération avec les autorités lors d'audits ou d'enquêtes, comme l'exige l'article 23. En fournissant des fonctions de journalisation et de reporting détaillées et inviolables, Kiteworks aide les fournisseurs et les déployeurs de systèmes d'IA à haut risque à répondre aux exigences du chapitre III de la loi sur l'IA de l'UE.

La loi sur l'IA de l'Union européenne est une étape majeure dans l'élaboration d'un cadre réglementaire complet pour les systèmes d'IA. En se concentrant sur les applications à haut risque et en introduisant une série d'obligations pour les fournisseurs, les importateurs, les distributeurs et les utilisateurs, cette loi vise à atténuer les risques tout en promouvant la confiance et la responsabilité dans les technologies de l'IA. Kiteworks est la solution idéale pour les organisations cherchant à se conformer aux exigences de la loi européenne sur l'IA, grâce à des mesures de sécurité robustes et à des capacités de journalisation complètes. Les principes de zéro trust, les contrôles d'accès granulaires, la prévention des pertes de données, les journaux d'audit immuables et les fonctions de chiffrement de la plateforme garantissent la conformité avec le chapitre II. En outre, la traçabilité de Kiteworks, les reportings détaillés et l'intégration avec des outils SIEM externes répondent aux exigences du chapitre III. Alors que les entreprises découvrent les subtilités de la loi européenne sur l'IA, Kiteworks offre une plateforme sécurisée pour mettre en œuvre des systèmes d'IA à haut risque, tout en garantissant la protection des droits fondamentaux, de la santé, de la sécurité et de l'environnement.