

Attestation de conformité à la loi européenne sur l'intelligence artificielle

Émis par : Akka Technologies, Inc.

Préparé par : Michael Nash, Directeur de la sécurité de l'information (CISO)

Date de l'attestation : 20 avril 2026

Classification du document : Public

Cycle de révision : Annuel

Introduction

La présente attestation est émise par Akka Technologies, Inc. (« Akka ») pour confirmer notre posture de conformité au règlement (UE) 2024/1689 du Parlement européen et du Conseil — la loi européenne sur l'intelligence artificielle (« la loi sur l'IA » ou « la loi »). Ce document est mis à disposition des clients, prospects, autorités réglementaires et autres parties intéressées à titre de preuve de l'engagement d'Akka en faveur d'une gouvernance responsable de l'IA dans le cadre du premier règlement mondial complet sur l'intelligence artificielle.

Akka est une société technologique dont le siège social est établi aux États-Unis, fournissant la plateforme Akka — une boîte à outils de microservices réactifs et de systèmes distribués permettant aux entreprises de concevoir et d'exploiter des applications d'IA agentique. Akka opère à l'échelle mondiale, avec une présence significative de clients dans l'Union européenne, et est donc directement soumise aux obligations de la loi sur l'IA en tant que fournisseur de systèmes d'IA et en tant qu'opérateur de systèmes d'IA dans ses propres activités internes.

La présente attestation couvre la période se terminant le 20 avril 2026 et sera révisée au moins annuellement, ou lors de modifications importantes des systèmes d'IA d'Akka, de sa structure organisationnelle ou des orientations réglementaires applicables.

Champ d'application et applicabilité

La loi sur l'IA (règlement (UE) 2024/1689) est entrée en vigueur le 1er août 2024, avec des dispositions s'appliquant selon un calendrier progressif jusqu'en 2027. La loi établit un système de classification fondé sur les risques pour les systèmes d'IA et les modèles d'IA à usage général (IAGP), imposant des obligations proportionnelles au niveau de risque que présente un système d'IA.

Le champ d'application principal d'Akka au titre de la loi est le suivant :

Rôle de fournisseur de systèmes d'IA : Akka développe et met à disposition la plateforme Akka, qui permet aux clients de concevoir, déployer et exploiter des applications d'IA agentique. Akka agit en tant que « fournisseur » au sens de l'article 3, paragraphe 3, de la loi pour les capacités d'IA intégrées ou activées par la plateforme.

Rôle d'habilitateur de l'IAGP : La plateforme Akka fournit l'infrastructure et les outils permettant aux clients d'intégrer et d'orchestrer des modèles d'IA à usage général dans leurs applications. Akka prend en charge les obligations de conformité qui découlent de la chaîne d'approvisionnement des modèles IAGP au titre du chapitre V de la loi.

Classification des risques : Les fonctionnalités d'IA propres à Akka et les capacités d'IA agentique de la plateforme sont plus précisément classées dans le niveau à risque limité ou de transparence au titre des articles 13 et 50 et de l'annexe III, selon le contexte de déploiement. Lorsque la plateforme est utilisée par des clients pour concevoir des applications d'IA à haut risque (par exemple dans les services financiers, la santé ou les infrastructures critiques), Akka fournit les contrôles techniques, la documentation et les mécanismes de transparence

dont les clients ont besoin pour satisfaire à leurs propres obligations liées aux systèmes à haut risque.

Déploiement interne de l'IA : Akka déploie l'IA dans ses propres opérations, notamment des outils de développement assistés par l'IA, la surveillance de la sécurité et l'automatisation du support client, tous soumis aux contrôles de gouvernance interne de l'IA.

La présente attestation couvre 82 contrôles mis en œuvre dans le cadre de conformité à la loi sur l'IA d'Akka. Parmi ceux-ci, 79 contrôles sont évalués à un risque résiduel Faible et 3 à un risque Moyen. Aucun contrôle n'est évalué à un risque résiduel Élevé. Les 82 contrôles sont à l'état Mis en œuvre.

Posture de conformité

Akka est conforme aux exigences de la loi sur l'IA applicables à son rôle de fournisseur de plateforme et d'habilitateur IAGP à la date de la présente attestation. Cette détermination est fondée sur :

- La mise en œuvre complète des 82 contrôles de la loi sur l'IA dans le SMSI d'Akka
- L'alignement sur la norme ISO/IEC 42001:2023 (Système de management de l'intelligence artificielle), au titre de laquelle Akka a mis en œuvre l'ensemble des 98 contrôles à risque résiduel Faible
- L'alignement sur le NIST AI RMF 1.0, avec les 14 contrôles mis en œuvre à risque Faible
- Le fonctionnement d'un Comité de révision de l'IA assurant une gouvernance de l'IA au niveau exécutif
- La tenue d'un Registre des agents documentant tous les agents d'IA déployés par ou pour le compte d'Akka

- La publication et l'application d'une Politique d'IA documentée régissant toutes les activités d'IA

Le programme de conformité d'Akka est intégré dans son Système de management de la sécurité de l'information (SMSI) aligné sur la norme ISO 27001, garantissant que les contrôles de gouvernance de l'IA sont intégrés aux pratiques plus larges de sécurité de l'information, de protection de la vie privée et de gestion des risques.

Classification des risques liés à l'IA et documentation technique

Akka maintient un processus formel de classification des risques liés à l'IA aligné sur les niveaux de risque de la loi. Pour chaque fonctionnalité ou système d'IA développé ou déployé :

Évaluation de la classification des risques : Chaque système d'IA est évalué par rapport aux catégories d'utilisations interdites (article 5), aux classifications à haut risque (annexe III) et aux seuils d'obligations de transparence (article 50) avant le déploiement.

Documentation technique : Akka maintient la documentation technique requise par l'article 11 et l'annexe IV pour les systèmes d'IA applicables, comprenant les descriptions des systèmes, les déclarations d'usage prévu, les mesures de performance, les résumés de gouvernance des données et les dispositions de surveillance humaine.

Supervision du Comité de révision de l'IA : Le Comité de révision de l'IA d'Akka examine les nouvelles fonctionnalités d'IA et les modifications importantes des systèmes d'IA existants avant le déploiement, en veillant à ce que les classifications des risques soient documentées, approuvées et maintenues à jour.

Registre des agents : Akka maintient un Registre des agents centralisé qui enregistre tous les agents d'IA en opération, leur périmètre d'action, les attributions de supervision et les classifications des niveaux de risque.

Obligations de transparence

Akka satisfait aux obligations de transparence des articles 13 et 50 de la loi dans le champ d'application applicable de ses systèmes d'IA :

Transparence vis-à-vis des utilisateurs : Lorsque la plateforme Akka interagit directement avec des personnes physiques, des informations appropriées sont fournies pour s'assurer que les personnes sont conscientes qu'elles interagissent avec des sorties générées par l'IA ou qu'elles y sont soumises.

Transparence vis-à-vis des clients : Akka fournit aux clients une documentation suffisante pour comprendre les capacités d'IA intégrées dans la plateforme, leur usage prévu, leurs caractéristiques de performance et leurs limites, permettant aux clients de prendre des décisions éclairées concernant les contextes de déploiement.

Publication de la Politique d'IA : La Politique d'IA d'Akka est un document accessible au public définissant les principes d'Akka pour le développement, le déploiement et la gouvernance de l'IA, incluant des engagements en matière de transparence, de supervision humaine et de pratiques d'IA responsables.

Transparence de la chaîne d'approvisionnement IAGP : Akka maintient des enregistrements des fournisseurs de modèles IAGP intégrés à la plateforme et veille à ce que les informations appropriées relatives aux capacités des modèles, à la provenance des données d'entraînement et aux propriétés de sécurité soient disponibles pour les clients, comme l'exige le chapitre V de la loi.

Supervision et contrôle humains

La plateforme Akka est conçue pour garantir une supervision humaine significative des sorties des systèmes d'IA, conformément aux articles 14 et 50 de la loi :

Contrôles humains dans la boucle : La plateforme fournit des contrôles configurables de supervision humaine dans la boucle aux niveaux du flux de travail, de la tâche et de l'action. Les clients peuvent exiger une approbation humaine avant qu'un agent prenne des actions au-dessus de seuils de signification définis, garantissant que les décisions autonomes à enjeux importants sont soumises à un examen humain.

Mécanismes de substitution et d'annulation : Les opérateurs humains peuvent remplacer, suspendre ou arrêter l'exécution d'un agent d'IA à tout moment dans un flux de travail. Les actions de substitution sont enregistrées avec horodatage et identité de l'opérateur, fournissant un enregistrement auditable des interventions humaines.

Limitation du périmètre par conception : Les agents d'IA déployés sur la plateforme Akka opèrent dans des limites de périmètre explicitement définies. Les actions dépassant ces limites nécessitent une autorisation humaine explicite, empêchant tout comportement autonome excessif ou non intentionnel.

Gouvernance des données et qualité

Akka applique des pratiques rigoureuses de gouvernance des données aux systèmes d'IA conformément aux articles 10 et 17 de la loi :

Gouvernance des données d'entraînement et d'entrée : Lorsqu'Akka développe des modèles d'IA ou affine des modèles pour une utilisation sur la plateforme, des contrôles de gouvernance des données s'appliquent à la sélection des données d'entraînement, à l'évaluation de la qualité, à l'évaluation des biais et à la documentation.

Minimisation des données pour l'IA : Les fonctionnalités d'IA et les flux de travail agentiques sont conçus pour opérer sur le minimum de données nécessaire à l'usage prévu. La conservation des données traitées par l'IA est soumise à des calendriers définis et à une mise en application automatisée.

Évaluation des biais et de l'équité : Akka effectue des évaluations des biais et de l'équité dans le cadre du processus de classification des risques liés à l'IA, en accordant une attention particulière aux systèmes d'IA utilisés dans des contextes où les décisions peuvent avoir des effets significatifs sur des personnes.

Isolation des données clients : Les données clients traitées par les fonctionnalités d'IA sur la plateforme Akka sont isolées logiquement et ne sont pas utilisées pour entraîner ou améliorer les modèles d'IA d'Akka sans le consentement explicite du client.

Robustesse, précision et cybersécurité

Akka maintient des contrôles pour garantir la robustesse, la précision et la cybersécurité des systèmes d'IA conformément aux articles 15 et 16 de la loi :

Surveillance des performances : Les fonctionnalités d'IA déployées sur la plateforme Akka font l'objet d'une surveillance continue des performances, avec des seuils de précision définis et des alertes en cas de dégradation des performances.

Robustesse aux attaques adversariales : Les contrôles de sécurité de l'IA d'Akka traitent les vecteurs d'attaque spécifiques à l'IA connus, notamment l'injection de prompts, l'inversion de modèles, les entrées adversariales et l'empoisonnement des données, s'appuyant sur les recommandations de la norme ISO/IEC 27090 et des directives de sécurité OWASP AI.

Réponse aux incidents liés à l'IA : Le programme de réponse aux incidents d'Akka comprend des procédures de classification et de réponse aux incidents spécifiques à l'IA, garantissant que les défaillances des systèmes d'IA, les comportements inattendus et les incidents de sécurité sont rapidement identifiés, contenus et corrigés.

Cybersécurité dès la conception : Les fonctionnalités d'IA sont développées dans le cadre du cycle de développement sécurisé d'Akka, intégrant des exigences de sécurité spécifiques aux composants d'IA depuis la conception jusqu'au déploiement.

Évaluation de la conformité et surveillance post-commercialisation

Akka maintient des processus pour soutenir les obligations d'évaluation de la conformité et la surveillance continue post-commercialisation conformément aux articles 16 à 20 de la loi :

Évaluation interne de la conformité : Le Comité de révision de l'IA d'Akka effectue des évaluations périodiques internes de la conformité des systèmes d'IA aux exigences de la loi, documentées dans le SMSI.

Surveillance post-commercialisation : Les systèmes d'IA déployés font l'objet d'une surveillance continue pour les performances, la sécurité et la dérive comportementale. Les résultats de la surveillance post-commercialisation alimentent le registre des risques liés à l'IA et éclairent le cycle de révision annuel.

Notification des incidents : Akka maintient des procédures pour signaler les incidents graves impliquant des systèmes d'IA aux autorités compétentes et aux parties affectées, comme l'exige l'article 73 de la loi, intégrées au programme de réponse aux incidents et de notification de violations d'Akka.

Gestion des changements : Les modifications importantes des systèmes d'IA déclenchent une réévaluation de la classification des risques et de la documentation technique, garantissant que l'évaluation de la conformité reste à jour.

Alignement sur ISO/IEC 42001 et NIST AI RMF

Le programme de conformité à la loi sur l'IA d'Akka est fondé sur et renforcé par l'alignement avec des normes de gouvernance de l'IA reconnues internationalement :

Alignement sur ISO/IEC 42001:2023 : Akka a mis en œuvre l'ensemble des 98 contrôles de la norme ISO/IEC 42001 Système de management de l'intelligence artificielle à risque résiduel Faible. ISO/IEC 42001 fournit le cadre de gestion systématique dans lequel les contrôles de la loi sur l'IA sont opérationnalisés, couvrant la politique d'IA, la planification, l'évaluation des performances et l'amélioration continue.

Alignement sur NIST AI RMF 1.0 : Akka a mis en œuvre l'ensemble des 14 contrôles du Cadre de gestion des risques liés à l'IA du NIST, couvrant les fonctions fondamentales GOUVERNER, CARTOGRAPHIER, MESURER et GÉRER. L'alignement sur le NIST AI RMF renforce les processus d'identification, d'évaluation et de traitement des risques liés à l'IA d'Akka, fournissant une perspective complémentaire du cadre américain sur la gestion des risques liés à l'IA.

SMSI aligné sur ISO 27001 : Tous les contrôles de gouvernance de l'IA sont intégrés dans le SMSI d'Akka aligné sur ISO 27001, garantissant l'intégration avec la gestion des risques liés à

la sécurité de l'information, le contrôle des accès, la réponse aux incidents et les pratiques de continuité des activités.

Preuves à l'appui

Les éléments de preuve suivants étayent la présente attestation :

- SMSI d'Akka — Cadre de contrôle de la loi sur l'IA, 82 contrôles, tous mis en œuvre
- Politique d'IA d'Akka (disponible publiquement)
- Charte et procès-verbaux du Comité de révision de l'IA
- Registre des agents (document de gouvernance interne)
- Documentation technique pour les fonctionnalités d'IA déployées sur la plateforme Akka
- Enregistrements de mise en œuvre des contrôles ISO/IEC 42001
- Enregistrements de mise en œuvre des contrôles NIST AI RMF
- Évaluations des risques liés à l'IA et enregistrements de classification
- Rapport SOC 2 Type II (disponible sous NDA) démontrant les contrôles de sécurité et de disponibilité sous-tendant la fiabilité des systèmes d'IA
- Documentation de sécurité de l'infrastructure AWS (SOC 2, ISO 27001) soutenant la sécurité de la couche cloud pour les charges de travail d'IA
- Procédures de réponse aux incidents et de classification des incidents liés à l'IA

Conclusion

Akka s'engage en faveur d'un développement et d'un déploiement de l'IA responsables, transparents et sûrs. Notre conformité à la loi européenne sur l'intelligence artificielle reflète notre conviction que la gouvernance fiable de l'IA n'est pas seulement une obligation

réglementaire, mais un différenciateur concurrentiel et une marque de respect envers les clients et les personnes dont les intérêts sont affectés par nos systèmes d'IA.

Au 20 avril 2026, Akka a mis en œuvre les 82 contrôles de son cadre de conformité à la loi sur l'IA, avec une solide posture de risque global (79 Faible, 3 Moyen, 0 Élevé), et maintient un alignement complet sur ISO/IEC 42001 et NIST AI RMF en tant que cadres complémentaires.

La présente attestation est disponible sur demande auprès des clients et prospects et est soumise à une révision annuelle. Les questions relatives au programme de conformité à la loi sur l'IA d'Akka doivent être adressées à :

Michael Nash

Directeur de la sécurité de l'information (CISO)

Akka Technologies, Inc.

michael.nash@akka.io

Signé : Michael Nash, CISO, Akka Technologies, Inc.

Date : 20 avril 2026