AYI NEDJIMI Consultants

AI Act 2026 : Guide Conformité Systèmes IA à Haut Risque

Catégorie : Conformité Lecture : 12 min Publié le : 19/01/2026 Auteur : Ayi NEDJIMI

Guide complet AI Act 2026 : classification des risques IA, obligations systèmes haut risque, documentation technique, marquage CE, sanctions et.

AI Act 2026 : Guide Conformité Systèmes IA à Haut Risque constitue un enjeu majeur pour les professionnels de la sécurité informatique et les équipes techniques. Ce guide détaillé sur ai act 2026 conformite ia propose une méthodologie structurée, des outils éprouvés et des recommandations opérationnelles directement applicables. L'objectif est de fournir aux praticiens — consultants, ingénieurs sécurité, administrateurs systèmes — les connaissances et les techniques nécessaires pour aborder ce sujet avec rigueur. Chaque section s'appuie sur des retours d'expérience terrain et intègre les évolutions les plus récentes du domaine. Les recommandations présentées sont adaptées aux environnements d'entreprise et tiennent compte des contraintes opérationnelles réelles.

1 Introduction à l'AI Act

Premier cadre juridique mondial sur l'IA

Le Règlement (UE) 2024/1689 sur l'intelligence artificielle, communément appelé AI Act, représente une avancée réglementaire majeure à l'échelle mondiale. Adopté en mars 2024 et publié au Journal Officiel de l'Union européenne en juillet 2024, ce règlement établit le **premier cadre** juridique complet régissant le développement, la mise sur le marché et l'utilisation des systèmes d'intelligence artificielle. Guide complet AI Act 2026 : classification des risques IA,

obligations systèmes haut risque, documentation technique, marquage CE, sanctions et. Le cadre réglementaire européen impose des exigences croissantes aux organisations. Ce guide sur ai act 2026 conformite ia fournit les clés de compréhension et de mise en conformité. Nous abordons notamment : 1 introduction à l'ai act, 2 classification des risques ia et 3 systèmes ia interdits. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

> L'approche européenne repose sur une logique de proportionnalité : les obligations imposées aux acteurs varient selon le niveau de risque que présente le système IA concerné. Cette classification permet de concentrer les exigences les plus strictes sur les applications présentant les risques les plus élevés pour les droits fondamentaux et la sécurité des personnes.
>
> En janvier 2026, nous nous trouvons dans une phase critique de mise en conformité. Les interdictions des pratiques à risque inacceptable sont effectives depuis février 2025, les obligations sur les modèles d'IA à usage général (GPAI) depuis août 2025, et l'ensemble des règles relatives aux systèmes à haut risque s'appliqueront pleinement à partir d'août 2026.

Champ d'application territorial

L'AI Act s'applique selon une logique d'effet **territorial** étendu, similaire à celle du RGPD. Sont concernés tous les fournisseurs de systèmes IA mis sur le marché ou mis en service dans l'Union, qu'ils soient établis dans l'UE ou dans un pays tiers. Les déployeurs (utilisateurs professionnels) établis dans l'UE sont également soumis au règlement.

l'AI Act couvre les fournisseurs et déployeurs établis hors de l'UE lorsque les résultats produits par leur système IA sont utilisés dans l'Union. Cette disposition capture notamment les services IA fournis à distance depuis des pays tiers mais utilisés par des personnes situées sur le territoire européen.

Certaines exclusions s'appliquent : les systèmes IA développés et utilisés exclusivement à des fins militaires, de défense ou de sécurité nationale échappent au règlement. De même, les activités de recherche et développement scientifique non commerciales bénéficient d'exemptions, ainsi que les utilisations purement personnelles et non professionnelles.

08/2026
Application complète des règles systèmes haut risque

35 M€
Amende maximale pour pratiques interdites

4
Niveaux de risque définis par le règlement

Votre conformité ISO 27001 se traduit-elle par une amélioration réelle de votre sécurité ?

2 Classification des risques IA

L'architecture fondamentale de l'AI Act repose sur une pyramide des risques qui détermine le régime **juridique** applicable à chaque système d'intelligence artificielle. Cette approche graduée permet d'adapter les contraintes réglementaires à la dangerosité potentielle des applications.

Pyramide de Classification des Risques AI Act

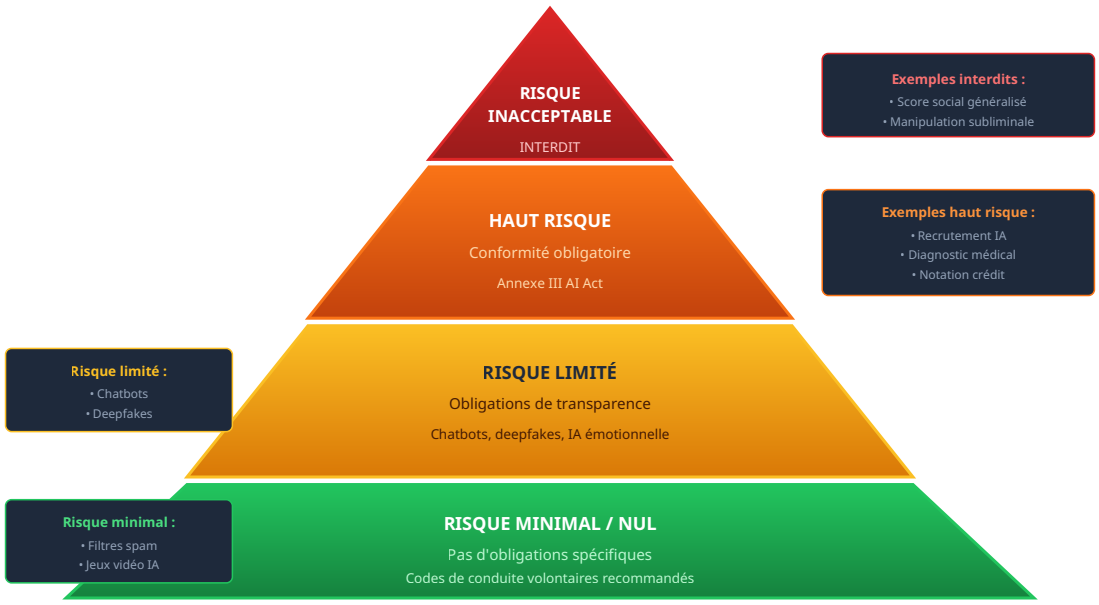

Figure 1 : Les quatre niveaux de risque définis par l'AI Act et leurs implications réglementaires

Risque inacceptable : l'interdiction

Au sommet de la pyramide se trouvent les systèmes IA dont le risque est jugé inacceptable et qui sont purement et simplement interdits. Cette catégorie inclut les techniques de manipulation subliminale ou trompeuse causant des préjudices, l'exploitation de vulnérabilités liées à l'âge, au handicap ou à la situation sociale, la notation sociale généralisée par les autorités publiques, et l'utilisation de la reconnaissance faciale en temps réel dans l'espace public par les forces de l'ordre (sauf exceptions strictes).

Haut risque : conformité obligatoire

Les systèmes IA à haut risque constituent le cœur du dispositif réglementaire. Ils sont soumis à un ensemble complet d'obligations préalables à leur mise sur le marché : système de gestion des risques, gouvernance des données, documentation technique, enregistrement des événements, transparence, supervision humaine, exactitude, robustesse et cybersécurité. Pour approfondir, consultez Top 10 des Attaques - Guide Pratique Cybersecurite.

Risque limité : transparence

Les systèmes présentant un risque limité sont principalement soumis à des obligations de transparence. Les utilisateurs doivent être informés qu'ils interagissent avec un système IA (chatbots), que le contenu a été généré ou manipulé artificiellement (deepfakes), ou que leurs émotions sont analysées.

Risque minimal : liberté encadrée

La grande majorité des systèmes IA relèvent de la catégorie risque minimal et ne sont soumis à aucune obligation spécifique. Néanmoins, le règlement encourage l'adoption volontaire de codes de conduite intégrant les principes de l'AI Act.

Notre avis d'expert

3 Systèmes IA interdits

Application depuis février 2025
Les interdictions prévues par l'article 5 de l'AI Act sont effectives depuis le 2 février 2025. Tout déploiement de ces systèmes expose à des sanctions pouvant atteindre 35 millions d'euros ou 7% du chiffre d'affaires **mondial**.

Manipulation et exploitation des vulnérabilités

L'AI Act interdit les systèmes IA utilisant des techniques subliminales, manipulatrices ou trompeuses pour altérer significativement le comportement des personnes d'une manière qui cause ou est susceptible de causer un préjudice physique ou psychologique. Cette interdiction couvre les interfaces conçues pour exploiter les biais cognitifs ou les dark patterns.

Sont également interdits les systèmes exploitant les vulnérabilités des personnes dues à leur âge, leur handicap ou leur situation sociale ou économique. Un système de publicité ciblée exploitant la précarité financière pour pousser à l'endettement serait typiquement concerné. Les recommandations de CNIL constituent une reference essentielle.

Notation sociale

Les systèmes de notation sociale par les autorités publiques évaluant ou classifiant les personnes physiques sur la base de leur comportement social ou de caractéristiques personnelles sont interdits lorsqu'ils conduisent à un traitement préjudiciable disproportionné ou déconnecté du contexte dans lequel les données ont été collectées. Les recommandations de ENISA constituent une reference essentielle.

Reconnaissance faciale et biométrique

L'AI Act interdit plusieurs usages de l'identification biométrique : la constitution de bases de données de reconnaissance faciale par collecte non ciblée (scraping), l'inférence des émotions sur le lieu de travail et dans les établissements d'enseignement (sauf raisons médicales ou de sécurité), et la catégorisation biométrique déduisant des caractéristiques sensibles (race, opinions politiques, orientation sexuelle).

L'identification biométrique à distance en temps réel dans les espaces publics par les forces de l'ordre est interdite sauf dans trois cas exceptionnels : recherche de victimes d'enlèvement ou de traite, prévention d'une menace terroriste imminente, et localisation de suspects de crimes graves. Ces exceptions sont strictement encadrées par des autorisations judiciaires préalables.

4 Systèmes IA à haut risque

Définition et périmètre

Les systèmes IA à haut risque sont définis selon deux critères alternatifs. Premièrement, les systèmes qui sont eux-mêmes des produits ou des composants de sécurité de produits couverts par la législation d'harmonisation de l'Union listée à l'Annexe I (machines, jouets, équipements médicaux, véhicules, etc.) et qui requièrent une évaluation de conformité par un tiers.

Deuxièmement, les systèmes listés à l'Annexe III du règlement, organisée en huit domaines : identification biométrique, gestion d'infrastructures critiques, éducation et formation professionnelle, emploi et gestion des travailleurs, accès aux services essentiels, forces de l'ordre, migration et asile, administration de la justice.

Les 8 Domaines de Systèmes IA à Haut Risque (Annexe III)

Figure 2 : Les huit domaines **d'application** des systèmes IA à haut risque selon l'Annexe III

Obligations des fournisseurs

Les fournisseurs de systèmes IA à haut risque doivent mettre en place un système de gestion des risques documenté et itératif, couvrant l'ensemble du cycle de vie du système. Ce système doit identifier et analyser les risques connus et prévisibles, estimer et évaluer les risques qui peuvent survenir lors d'une utilisation conforme ou d'un mésusage raisonnablement prévisible, et mettre en œuvre des mesures de gestion appropriées.

La gouvernance des données est une exigence centrale. Les jeux de données d'entraînement, de validation et de test doivent être pertinents, représentatifs, exempts d'erreurs et complets. Des mesures spécifiques doivent être prises pour détecter, prévenir et atténuer les biais potentiels, notamment ceux liés aux caractéristiques protégées (origine, genre, âge, handicap, etc.). Pour approfondir, consultez NIS 2 : Guide Complet de la Directive Européenne sur la.

Les systèmes doivent être conçus pour permettre une supervision humaine effective. Selon le niveau de risque, cette supervision peut aller de la simple validation des résultats (human-on-the-loop) jusqu'à la possibilité d'intervention en temps réel (human-in-the-loop) ou de désactivation (human-in-command). Pour approfondir, consultez SecNumCloud 2026 : Migration et Certification EUCS.

Cas concret
L'amende record de 150 millions d'euros infligée par la CNIL à Google en 2022 pour non-conformité aux règles de gestion des cookies a envoyé un signal fort à l'industrie. Cette décision a accéléré l'adoption des Consent Management Platforms et la révision des pratiques de tracking publicitaire en Europe.

Êtes-vous certain que votre traitement des données personnelles est conforme au RGPD ?

5 Obligations de transparence

Systèmes interagissant avec des personnes

Tout système IA conçu pour interagir directement avec des personnes physiques doit informer celles-ci qu'elles interagissent avec un système IA, sauf si cela ressort clairement des circonstances et du contexte d'utilisation. Cette obligation s'applique notamment aux chatbots, assistants virtuels et systèmes de recommandation interactifs.

L'information doit être claire, compréhensible et fournie au moment opportun. Elle peut être délivrée par différents moyens : message textuel, icône standardisée, mention vocale, selon le canal d'interaction utilisé.

Contenus générés ou manipulés

Les utilisateurs de systèmes IA générant des contenus synthétiques (texte, image, audio, vidéo) doivent marquer ces contenus comme générés artificiellement ou manipulés. Cette obligation vise particulièrement les deepfakes et les contenus générés par IA qui pourraient être confondus avec des contenus authentiques.

Le marquage doit être lisible par machine et permettre une détection automatisée. Les normes techniques pour ce marquage sont en cours de développement. Une exception s'applique aux usages artistiques, satiriques ou parodiques qui ne portent pas atteinte aux droits des tiers.

Reconnaissance d'émotions et catégorisation

Les personnes exposées à un système de reconnaissance d'émotions ou de catégorisation biométrique doivent être informées de ce traitement. Cette information doit préciser les catégories utilisées (émotions, caractéristiques déduites) et l'usage qui en est fait.

6 Évaluation de conformité

Auto-évaluation vs évaluation par un tiers

L'AI Act prévoit deux voies d'évaluation de la conformité pour les systèmes à haut risque. La majorité des systèmes peuvent faire l'objet d'une auto-évaluation par le fournisseur (contrôle interne). Cette procédure implique de vérifier que le système de management de la qualité est conforme, que la documentation technique est complète et que le système satisfait aux exigences applicables.

Certains systèmes nécessitent une évaluation par un organisme notifié (tiers indépendant). C'est le cas des systèmes d'identification biométrique à distance et des systèmes IA intégrés dans des produits déjà soumis à évaluation par un tiers selon la législation sectorielle applicable.

Processus de Mise en Conformité AI Act

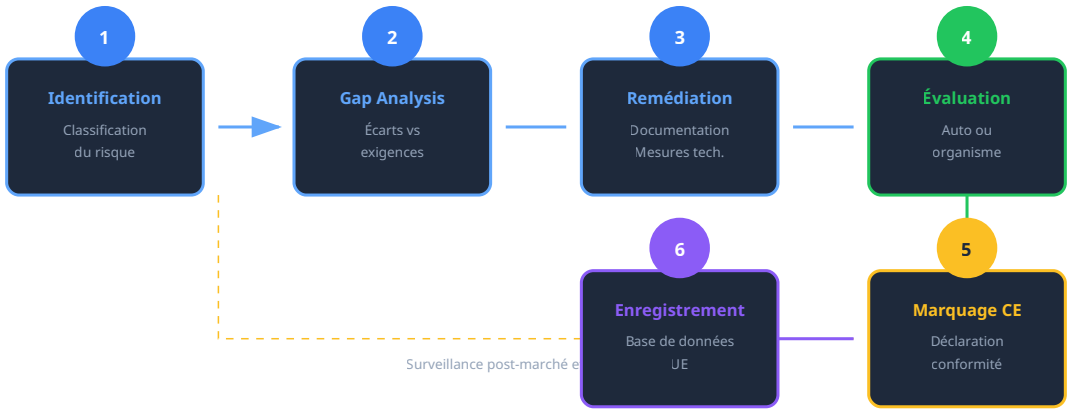

Figure 3 : Les étapes clés du processus de mise en conformité AI Act

Système de management de la qualité

Les fournisseurs de systèmes à haut risque doivent déployer un système de management de la qualité documenté couvrant : la stratégie de conformité réglementaire, les techniques et procédures de conception et développement, les procédures de test et validation, les spécifications techniques, les systèmes et procédures de gestion des données, et le système de gestion des risques.

Ce système doit être proportionné à la taille de l'organisation et faire l'objet d'audits internes réguliers. Il peut s'appuyer sur des normes existantes (ISO 9001, ISO/IEC 42001 sur le management de l'IA) adaptées aux exigences spécifiques de l'AI Act.

7 Documentation technique

Contenu obligatoire

La documentation technique constitue la preuve de la conformité du système IA aux exigences du règlement. Elle doit être établie avant la mise sur le marché et maintenue à jour tout au long du cycle de vie du système. L'Annexe IV de l'AI Act détaille le contenu minimal requis.

Cette documentation comprend notamment : une description générale du système (finalité prévue, développeur, versions), une description détaillée des éléments du système et de son processus de développement, les informations sur les données d'entraînement et de test, les méthodes et métriques utilisées pour évaluer les performances, les mesures de gestion des risques, et les instructions d'utilisation. Pour approfondir, consultez Cyber Resilience Act 2026 : Guide Anticipation Produits C....

Section	Contenu	Importance
Description générale	Finalité, fonctionnalités, versions, développeur	Critique
Architecture technique	Modèle, algorithmes, composants, interfaces	Critique
Données	Sources, caractéristiques, préparation, biais	Critique
Tests et validation	Métriques, résultats, limites identifiées	Élevée
Gestion des risques	Identification, évaluation, mesures d'atténuation	Critique
Instructions d'utilisation	Guide déployeur, supervision humaine, maintenance	Élevée

Conservation et mise à jour

La documentation technique doit être conservée pendant 10 ans après la mise sur le marché du système IA (ou la mise hors service pour les systèmes utilisés en continu). Toute modification substantielle du système nécessite une mise à jour de la documentation et potentiellement une nouvelle évaluation de conformité.

8 Marquage CE et mise sur le marché

Déclaration de conformité UE

Avant d'apposer le marquage CE, le fournisseur doit établir une déclaration de conformité UE écrite pour chaque système IA à haut risque. Cette déclaration contient l'identification du système et du fournisseur, une déclaration que le système est conforme au règlement, les références des normes harmonisées ou spécifications communes appliquées, et le cas échéant l'identification de l'organisme notifié ayant effectué l'évaluation.

La déclaration de conformité engage la responsabilité du fournisseur. Elle doit être tenue à disposition des autorités de surveillance du marché pendant au moins 10 ans et fournie aux déployeurs avec le système.

Cycle de Certification et Marquage CE

Figure 4 : Éléments requis pour l'obtention du marquage CE AI Act

Base de données européenne

Les systèmes IA à haut risque listés à l'Annexe III doivent être enregistrés dans la base de données européenne avant leur mise sur le marché. Cette base de données, gérée par la Commission européenne, est publiquement accessible et contient des informations essentielles sur les systèmes : identification, finalité, statut de conformité, coordonnées du fournisseur.

L'enregistrement a un double objectif : permettre aux autorités de surveillance du marché de suivre les systèmes en circulation et offrir aux utilisateurs potentiels une visibilité sur les systèmes conformes disponibles. Les déployeurs dans le secteur public doivent également s'enregistrer.

9 Régime de sanctions

Amendes administratives

L'AI Act prévoit un régime de sanctions administratives gradué selon la gravité des infractions. Les sanctions les plus sévères concernent les pratiques interdites (article 5) : jusqu'à 35 millions d'euros ou 7% du chiffre d'affaires annuel **mondial** total de l'exercice précédent, le montant le plus élevé étant retenu.

Pour les violations des obligations relatives aux systèmes à haut risque et autres exigences substantielles, les amendes peuvent atteindre 15 millions d'euros ou 3% du chiffre d'affaires mondial. La fourniture d'informations incorrectes, incomplètes ou trompeuses aux autorités est passible d'amendes jusqu'à 7,5 millions d'euros ou 1,5% du chiffre d'affaires.

Barème des sanctions AI Act
Pratiques interdites (Art. 5) 35 M€ / 7% CA
Obligations systèmes haut risque 15 M€ / 3% CA
Informations incorrectes aux autorités 7,5 M€ / 1,5% CA

Adaptations pour PME et startups

L'AI Act prévoit des plafonds adaptés pour les PME et les startups. Pour ces structures, les amendes sont plafonnées au montant le plus bas entre le pourcentage du CA et le montant fixe. Cette disposition vise à éviter que des sanctions disproportionnées ne mettent en péril la viabilité d'entreprises innovantes.

Les autorités de surveillance doivent également prendre en compte les circonstances atténuantes : **premier** manquement, mesures correctives prises, coopération avec les autorités, absence de faute intentionnelle. À l'inverse, les récidives et l'obstruction aux contrôles constituent des circonstances aggravantes.

10 Checklist de conformité

Phase 1 : Identification et classification

- ☐ Inventorier tous les systèmes IA de l'organisation (développés ou utilisés)
- ☐ Classifier chaque système selon les catégories de risque AI Act
- ☐ Vérifier l'absence de pratiques interdites (article 5)
- ☐ Identifier les systèmes relevant de l'Annexe III (haut risque)

Phase 2 : Gap analysis et planification

- ☐ Évaluer les écarts entre l'existant et les exigences applicables
- ☐ Définir un plan de remédiation priorisé avec échéances
- ☐ Allouer les ressources nécessaires (budget, compétences)
- ☐ Identifier les besoins en formation des équipes

Phase 3 : Mise en conformité (systèmes haut risque)

- ☐ Configurer le système de gestion des risques
- ☐ Documenter la gouvernance des données (sources, qualité, biais)
- ☐ Établir la documentation technique complète (Annexe IV)
- ☐ Implémenter la traçabilité et les logs
- ☐ Concevoir les mécanismes de supervision humaine
- ☐ Rédiger les instructions d'utilisation pour les déployeurs

Phase 4 : Évaluation et mise sur le marché

- ☐ Réaliser l'évaluation de conformité (auto ou organisme notifié)
- ☐ Établir la déclaration de conformité UE
- ☐ Apposer le marquage CE
- ☐ Enregistrer dans la base de données européenne
- ☐ Installer la surveillance post-marché

Besoin d'accompagnement AI Act ?

Nos experts vous accompagnent dans l'évaluation de vos systèmes IA, la classification des risques et la mise en conformité avec le règlement européen sur l'intelligence artificielle.

Demander un audit AI Act

Pour approfondir ce sujet, consultez notre outil open-source rgpd-compliance-checker qui facilite la vérification automatisée de conformité RGPD.

Questions frequentes

Comment ce sujet impacte-t-il la securite des organisations ?

Ce sujet a un impact significatif sur la securite des organisations car il touche aux fondamentaux de la protection des systemes d'information. Les entreprises doivent evaluer leur exposition, appliquer des mesures preventives adaptees et former leurs equipes pour faire face aux risques associes a cette problematique.

Quelles sont les bonnes pratiques recommandees par les experts ?

Pourquoi est-il important de se former sur ce sujet en 2026 ?

En 2026, la maitrise de ce sujet est devenue incontournable face a l'evolution constante des menaces et des exigences reglementaires. Les professionnels de la cybersecurite doivent maintenir leurs competences a jour pour proteger efficacement les actifs numeriques de leur organisation et repondre aux obligations de conformite.

Sources et références : CNIL · ANSSI

Conclusion

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr