



AI Act Européen

Le guide de référence sur le Règlement (UE) 2024/1689

Table des matières

01	Introduction	3
02	Chronologie et Cadre Juridique	4
03	Classification des Risques	6
04	Modèles d'IA à Usage Général (GPAI)	9
05	Obligations par Acteur	11
06	Gouvernance et Enforcement	13
07	Sanctions et Pénalités	14
08	Impact Sectoriel	15
09	Comparaison Internationale	17
10	Recommandations Pratiques	18
11	Conclusion	20
12	Annexes	21



1. Introduction

1.1 Contexte : Pourquoi l'Union Européenne Régule l'IA

L'intelligence artificielle transforme profondément nos sociétés, nos économies et nos modes de vie. Face à cette révolution technologique, l'Union européenne a choisi d'établir un cadre réglementaire harmonisé plutôt que de laisser chaque État membre légiférer individuellement.

Cette approche s'inscrit dans la continuité de la stratégie numérique européenne, qui comprend notamment le Règlement Général sur la Protection des Données (RGPD), le Digital Services Act (DSA) et le Digital Markets Act (DMA).

Les motivations principales de cette réglementation sont :

- **Protection des droits fondamentaux** : Prévenir les discriminations algorithmiques et protéger la dignité humaine
- **Sécurité des personnes** : Garantir que les systèmes d'IA intégrés dans des produits ne mettent pas en danger la santé et la sécurité
- **Harmonisation du marché intérieur** : Créer un cadre uniforme pour les 27 États membres, évitant la fragmentation réglementaire
- **Compétitivité européenne** : Établir un standard mondial que l'UE peut exporter (« effet Bruxelles »)

1.2 Objectifs du Règlement

L'AI Act poursuit plusieurs objectifs complémentaires, explicitement énoncés dans ses considérants :

1.3 Portée Géographique et Extraterritoriale

L'AI Act a une **portée extraterritoriale** significative. Il s'applique à :

1. **Les fournisseurs** établis dans l'UE ou dans un pays tiers, qui mettent sur le marché ou en service des systèmes d'IA dans l'Union
2. **Les déployeurs** de systèmes d'IA situés dans l'Union
3. **Les fournisseurs et déployeurs** situés dans un pays tiers, lorsque les résultats produits par le système d'IA sont utilisés dans l'Union
4. **Les importateurs et distributeurs** de systèmes d'IA
5. **Les fabricants de produits** qui mettent sur le marché ou en service un système d'IA avec leur produit sous leur propre nom ou marque

« *Toute entreprise, quelle que soit sa localisation, qui commercialise des systèmes d'IA destinés au marché européen ou dont les résultats sont utilisés dans l'UE doit se conformer à l'AI Act.* »

1.4 Ce que ce Livre Blanc Couvre

Ce document présente une analyse complète et neutre du Règlement (UE) 2024/1689. Il couvre :

- La genèse et le calendrier d'entrée en application
- Le système de classification des risques (quatre niveaux)
- Les dispositions spécifiques aux modèles d'IA à usage général (GPAI)
- Les obligations différencierées par type d'acteur
- Le régime de gouvernance et d'enforcement
- Les sanctions applicables
- L'impact sectoriel (RH, santé, finance, éducation)
- La comparaison avec les approches internationales

2. Chronologie et Cadre Juridique

2.1 Genèse du Règlement (2021-2024)

L'élaboration de l'AI Act a été un processus législatif de plusieurs années :

2.2 Calendrier d'Application Progressif

Le règlement adopte une **mise en application échelonnée** sur trois ans, permettant aux acteurs de s'adapter progressivement :

DATE	DÉLAI	DISPOSITIONS APPLICABLES
2 février 2025	6 mois	Pratiques interdites (Article 5) Littératie IA (Article 4)
2 août 2025	12 mois	Obligations GPAI (Chapitre V) Gouvernance : Désignation des autorités nationales Codes de pratique pour modèles GPAI
2 août 2026	24 mois	Systèmes à haut risque (Annexe III) Obligations des fournisseurs et déployeurs Régime de sanctions (Article 99) Majorité des dispositions
2 août 2027	36 mois	Systèmes à haut risque dans produits réglementés (Annexe I) Dispositifs médicaux, machines, véhicules, aéronefs Conformité complète GPAI (modèles antérieurs à août 2025)
31 déc. 2030	6+ ans	Systèmes IT à grande échelle (Annexe X) Systèmes existants mis sur le marché avant cette date

3. Classification des Risques

L'AI Act introduit une **approche pyramidale fondée sur le risque**. Quatre niveaux sont définis, chacun avec des obligations proportionnées :

⎩ Risque Inacceptable
INTERDIT

Risque Élevé
RÉGLEMENTÉ
 Risque Limité
TRANSPARENCE

⎩ Risque Minimal
NON RÉGLEMENTÉ

3.1 Risque Inacceptable – Pratiques Interdites (Article 5)

Le règlement **interdit** huit catégories de systèmes d'IA considérées comme portant atteinte aux droits fondamentaux ou à la dignité humaine. Ces interdictions sont **effectives depuis le 2 février 2025**.

3.2 Risque Élevé – Systèmes Réglementés (Articles 6-49)

Les systèmes d'IA à haut risque représentent le cœur du règlement. Ils sont soumis à des **obligations strictes** avant mise sur le marché et tout au long de leur cycle de vie.

CATÉGORIE 1 : COMPOSANTS DE SÉCURITÉ DE PRODUITS RÉGLEMENTÉS (ANNEXE I)

Systèmes d'IA constituant un **composant de sécurité** d'un produit couvert par la législation d'harmonisation de l'Union, notamment :

- Machines et équipements industriels
- Jouets
- Ascenseurs
- Équipements sous pression

- Dispositifs médicaux et dispositifs médicaux de diagnostic in vitro
- Véhicules (homologation)
- Aéronefs et systèmes de gestion du trafic aérien
- Équipements marins
- Équipements ferroviaires

CATÉGORIE 2 : DOMAINES SENSIBLES (ANNEXE III)

Systèmes d'IA déployés dans des **domaines à fort impact** sur les droits fondamentaux :

3.3 Risque Limité – Obligations de Transparence (Article 50)

Certains systèmes d'IA présentent un **risque de tromperie** mais ne sont pas considérés comme à haut risque. Ils sont soumis à des **obligations de transparence** :

- **Chatbots et agents conversationnels** : Les utilisateurs doivent être informés qu'ils interagissent avec une IA (sauf si c'est évident au vu des circonstances)
- **Systèmes de reconnaissance des émotions** : Information des personnes concernées (hors cas interdits)
- **Systèmes de catégorisation biométrique** : Information des personnes (hors cas interdits)
- **Deepfakes et contenus générés** : Marquage clair que le contenu (image, audio, vidéo, texte) a été généré ou manipulé par IA

3.4 Risque Minimal – Non Réglementé

La grande majorité des systèmes d'IA relèvent de cette catégorie et ne sont **pas spécifiquement réglementés** par l'AI Act. Exemples :

- Jeux vidéo utilisant l'IA
- Filtres anti-spam
- Systèmes de recommandation de contenu
- Assistants de traduction
- Outils d'optimisation industrielle

Ces systèmes restent toutefois soumis aux autres législations applicables (RGPD, droit de la consommation, droit de la concurrence, etc.).

4. Modèles d'IA à Usage Général (GPAI)

Les **modèles d'IA à usage général** (General-Purpose AI ou GPAI) font l'objet d'un chapitre dédié (Chapitre V), ajouté lors des négociations finales pour répondre à l'émergence de systèmes comme ChatGPT, Claude, Gemini ou DALL-E.

4.1 Définition

Un modèle GPAI est défini comme :

« Un modèle d'IA, y compris lorsqu'il est entraîné à l'aide d'un grand volume de données en utilisant l'auto-supervision à grande échelle, qui présente une généralité significative et est capable d'exécuter de manière compétente un large éventail de tâches distinctes, indépendamment de la manière dont le modèle est mis sur le marché, et qui peut être intégré dans une variété de systèmes ou d'applications en aval. »

Exemples : GPT-4, Claude, Gemini, LLaMA, Mistral, DALL-E, Midjourney, Stable Diffusion.

4.2 Obligations des Fournisseurs de Modèles GPAI

Tous les fournisseurs de modèles GPAI doivent, à compter du 2 août 2025 :

1. **Rédiger et tenir à jour une documentation technique** du modèle et de son processus d'entraînement
2. **Établir et documenter une politique de conformité** au droit d'auteur de l'UE
3. **Publier un résumé détaillé** du contenu utilisé pour l'entraînement du modèle
4. **Fournir des informations et de la documentation** aux fournisseurs en aval intégrant le modèle
5. **Désigner un représentant** dans l'Union (pour les fournisseurs hors UE)

4.3 Modèles GPAI à Risque Systémique

Un modèle GPAI présente un **risque systémique** lorsque :

Les fournisseurs de modèles GPAI à risque systémique doivent, en plus des obligations générales :

- **Réaliser des évaluations de modèles** conformément à des protocoles et outils normalisés
- **Effectuer des tests adversariaux** pour identifier et atténuer les risques systémiques
- **Suivre, documenter et signaler** les incidents graves à l'AI Office et aux autorités nationales
- **Assurer un niveau adéquat de cybersécurité** pour le modèle et son infrastructure
- **Notifier la Commission** dans les 2 semaines si leur modèle atteint le seuil de risque systémique

4.4 Code de Pratique GPAI

Le 10 juillet 2025, la Commission européenne a publié le **Code de Pratique pour les modèles GPAI**, un instrument de droit souple (soft law) permettant aux fournisseurs de démontrer leur conformité.

L'adhésion volontaire au Code offre aux fournisseurs :

- Une présomption de conformité aux obligations de l'AI Act
- Une réduction de la charge administrative
- Une plus grande sécurité juridique

5. Obligations par Acteur

L'AI Act distingue plusieurs catégories d'acteurs dans la chaîne de valeur de l'IA, chacun avec des obligations spécifiques.

5.1 Fournisseurs (Providers/Developers)

Les **fournisseurs** sont les personnes physiques ou morales qui développent ou font développer un système d'IA en vue de le mettre sur le marché ou en service sous leur propre nom ou marque.

OBLIGATIONS POUR LES SYSTÈMES À HAUT RISQUE :

- 1 **Système de gestion des risques (Article 9)**
Établir, mettre en œuvre, documenter et maintenir un système de gestion des risques tout au long du cycle de vie du système d'IA.
- 2 **Gouvernance des données (Article 10)**
S'assurer que les jeux de données d'entraînement, de validation et de test sont pertinents, représentatifs, exempts d'erreurs et complets.

3 Documentation technique (Article 11)

Rédiger une documentation technique démontrant la conformité du système avant sa mise sur le marché.

4 Journalisation (Article 12)

Concevoir le système pour permettre l'enregistrement automatique des événements (logs) tout au long de son fonctionnement.

5 Transparence (Article 13)

Concevoir le système pour permettre aux déployeurs de comprendre son fonctionnement et d'interpréter ses résultats.

6 Contrôle humain (Article 14)

Concevoir le système pour permettre une supervision humaine efficace pendant son utilisation.

7 Précision, robustesse et cybersécurité (Article 15)

S'assurer que le système atteint un niveau approprié de précision, de robustesse et de cybersécurité.

8 Système de gestion de la qualité (Article 17)

Mettre en place un système de gestion de la qualité documenté sous forme de politiques et de procédures écrites.

9 Évaluation de conformité et marquage CE (Articles 43, 48)

Réaliser une évaluation de conformité (auto-évaluation ou via organisme notifié) et apposer le marquage CE.

10 Enregistrement dans la base de données UE (Article 49)

Enregistrer le système dans la base de données publique de l'UE avant sa mise sur le marché.

5.2 Déployeurs (Deployers/Users)

Les **déployeurs** sont les personnes physiques ou morales qui utilisent un système d'IA sous leur propre autorité (hors activité personnelle non professionnelle).

OBLIGATIONS PRINCIPALES :

- **Utilisation conforme** : Utiliser le système conformément aux instructions d'utilisation fournies par le fournisseur
- **Contrôle humain** : Veiller à ce que la surveillance humaine soit exercée par des personnes compétentes et habilitées
- **Données d'entrée** : S'assurer que les données d'entrée sont pertinentes au regard de la finalité du système
- **Surveillance du fonctionnement** : Surveiller le fonctionnement du système et suspendre son utilisation en cas de dysfonctionnement
- **Conservation des journaux** : Conserver les journaux générés automatiquement (minimum 6 mois)
- **Information des personnes** : Informer les personnes concernées qu'elles sont soumises à une décision prise par un système à haut risque
- **Analyse d'impact sur les droits fondamentaux** : Réaliser une analyse d'impact avant la mise en service (pour certains déployeurs)

5.3 Importateurs et Distributeurs

Importateurs : Personnes établies dans l'Union qui mettent sur le marché un système d'IA provenant d'un pays tiers.

Distributeurs : Personnes (autres que le fournisseur ou l'importateur) qui mettent un système d'IA à disposition sur le marché.

Leurs obligations portent principalement sur :

- La vérification de la conformité et du marquage CE
- La vérification de la documentation et des instructions
- La traçabilité et l'identification des acteurs dans la chaîne d'approvisionnement
- La coopération avec les autorités de surveillance

5.4 Obligation Transversale : Littératie IA (Article 4)

En vigueur depuis le 2 février 2025, l'obligation de littératie IA s'applique à tous les fournisseurs et déployeurs :

6. Gouvernance et Enforcement

L'AI Act établit une **architecture de gouvernance multi-niveaux** combinant supervision européenne et nationale.

6.1 Au Niveau Européen

L'AI OFFICE (BUREAU EUROPÉEN DE L'IA)

Créé au sein de la Commission européenne, l'AI Office est responsable de :

- La supervision des modèles GPAI et des modèles à risque systémique
- L'élaboration de lignes directrices et de codes de pratique
- La coordination avec les autorités nationales
- L'application des règles aux fournisseurs de modèles GPAI

LE COMITÉ EUROPÉEN DE L'INTELLIGENCE ARTIFICIELLE (AI BOARD)

Composé de représentants des États membres, il :

- Conseille et assiste la Commission
- Contribue à l'application cohérente du règlement
- Coordonne les autorités nationales
- Émet des recommandations et des avis

6.2 Au Niveau National

Chaque État membre devait désigner au moins une autorité compétente avant le 2 août 2025 :

- **Autorité notifiante** : Responsable de la désignation et du contrôle des organismes notifiés
- **Autorité de surveillance du marché** : Responsable du contrôle et de l'application du règlement

Ces autorités peuvent être regroupées au sein d'une même entité ou réparties entre plusieurs organismes.

6.3 Plans de Mise en Œuvre Nationaux

Plusieurs États membres ont publié leurs plans de mise en œuvre de l'AI Act :

- **France** : La CNIL et la DGE co-pilotent la mise en œuvre

- **Allemagne** : L'Office fédéral de la sécurité des technologies de l'information (BSI) joue un rôle central
- **Italie, Espagne, Pays-Bas** : Ont également publié leurs stratégies

7. Sanctions et Pénalités

L'AI Act prévoit un régime de sanctions administratives gradué (Article 99), applicable à compter du 2 août 2025.

7.1 Structure des Amendes

Pour les PME et startups, les montants maximums sont adaptés :

- Les plafonds en pourcentage du CA s'appliquent de la même manière
- Les plafonds en montant absolu s'appliquent s'ils sont plus favorables

7.2 Autres Conséquences

Au-delà des amendes, les autorités peuvent :

- **Ordonner le retrait du marché** ou le rappel d'un système non conforme
- **Interdire la mise en service** d'un système d'IA
- **Exiger des mesures correctives** dans un délai déterminé
- **Publier les décisions** de non-conformité (name and shame)

8. Impact Sectoriel

L'AI Act a des implications différencierées selon les secteurs d'activité. Cette section analyse les quatre secteurs les plus impactés.

8.1 Ressources Humaines et Recrutement

Le secteur RH est **particulièrement concerné** par l'AI Act, la plupart des applications IA dans ce domaine étant classées à **haut risque**.

SYSTÈMES CLASSÉS À HAUT RISQUE :

- Outils de tri et de scoring de CV
- Systèmes de matching candidat-poste
- Outils d'analyse d'entretien vidéo
- Systèmes d'évaluation des performances
- Outils d'affectation des tâches et des horaires
- Systèmes de décision de promotion ou de licenciement

PRATIQUES INTERDITES EN CONTEXTE RH :

- **Reconnaissance émotionnelle** au travail (sauf raisons médicales/sécurité)
- **Scoring social** des employés
- **Surveillance biométrique invasive**

OBLIGATIONS CLÉS POUR LES EMPLOYEURS :

1. **Inventaire des systèmes IA** utilisés en gestion RH
2. **Formation à la littératie IA** des équipes RH (obligatoire depuis février 2025)
3. **Information des candidats et employés** sur l'utilisation de l'IA dans les processus décisionnels
4. **Mise en place d'une supervision humaine** effective des décisions automatisées
5. **Analyse d'impact sur les droits fondamentaux** pour certains systèmes

8.2 Santé et Dispositifs Médicaux

Le secteur de la santé combine deux cadres réglementaires : l'AI Act et le **Règlement sur les dispositifs médicaux** (MDR 2017/745).

SYSTÈMES CLASSÉS À HAUT RISQUE :

- Systèmes d'aide au diagnostic (imagerie médicale, pathologie)
- Outils de triage des patients
- Systèmes de recommandation de traitement
- Dispositifs médicaux intégrant de l'IA
- Systèmes de priorisation des urgences

SPÉCIFICITÉS DU SECTEUR :

- Les systèmes IA dans les dispositifs médicaux bénéficient d'un **délai prolongé** (août 2027)
- Évaluation de conformité souvent réalisée par un **organisme notifié**
- Interaction avec les réglementations de pharmacovigilance et de matériovigilance

8.3 Finance et Assurance

Le secteur financier utilise largement l'IA pour l'évaluation des risques, ce qui le place dans le périmètre du haut risque.

SYSTÈMES CLASSÉS À HAUT RISQUE :

- **Scoring de crédit** et évaluation de solvabilité
- **Tarification d'assurance** basée sur l'IA (sauf assurance automobile)
- Systèmes de détection de fraude ayant un impact sur l'accès aux services
- Évaluation des risques pour les prêts immobiliers

POINTS D'ATTENTION :

- Interaction avec la réglementation financière existante (MiFID II, Solvabilité II)
- Exigences accrues en matière de transparence et d'explicabilité des décisions
- Obligation de permettre aux clients de contester les décisions automatisées

8.4 Éducation

L'IA dans l'éducation est classée à **haut risque** en raison de son impact potentiel sur les trajectoires de vie des apprenants.

SYSTÈMES CLASSÉS À HAUT RISQUE :

- Systèmes d'admission (algorithmes Parcoursup-like)
- Correction automatisée d'exams
- Évaluation des apprentissages et recommandations de parcours
- Systèmes de surveillance des exams (proctoring)
- Détection de plagiat avec implications décisionnelles

INTERDICTIONS SPÉCIFIQUES :

- **Reconnaissance émotionnelle** dans les établissements d'enseignement (interdite)
- **Surveillance biométrique** généralisée des étudiants

9. Comparaison Internationale

L'AI Act s'inscrit dans un contexte de **course mondiale à la réglementation de l'IA**. Les approches varient significativement selon les juridictions.

9.1 L'Effet Bruxelles

Comme pour le RGPD, l'AI Act pourrait générer un **effet Bruxelles** – la tendance des entreprises mondiales à aligner leurs pratiques sur les standards européens pour accéder au marché unique.

Facteurs favorisant cet effet :

- Taille du marché européen (450 millions de consommateurs)
- Complexité de maintenir des versions différentes de systèmes d'IA
- Pression des partenaires commerciaux européens
- Avantage compétitif d'être « AI Act compliant »

10. Recommandations Pratiques

Cette section présente une **checklist de conformité** pour les organisations souhaitant se préparer à l'AI Act.

10.1 Actions Immédiates (Déjà Applicables)

- Audit des pratiques interdites**
Vérifier qu'aucun système d'IA interdit (scoring social, reconnaissance émotionnelle au travail, etc.) n'est utilisé.
- Programme de littératie IA**
Former le personnel utilisant ou supervisant des systèmes d'IA.

10.2 Actions à Court Terme (Avant Août 2026)

- Inventaire des systèmes d'IA**
Recenser tous les systèmes d'IA utilisés ou développés par l'organisation.
- Classification des risques**
Classifier chaque système selon les catégories de l'AI Act (interdit, haut risque, limité, minimal).
- Analyse des écarts (Gap Analysis)**
Identifier les écarts entre les pratiques actuelles et les exigences de l'AI Act.
- Documentation technique**
Préparer la documentation requise pour les systèmes à haut risque.
- Processus de surveillance humaine**
Mettre en place des procédures de contrôle humain pour les systèmes à haut risque.
- Système de gestion de la qualité**
Établir un système de gestion de la qualité documenté.

10.3 Gouvernance Recommandée

- Désigner un **responsable AI/IA** au sein de l'organisation
- Constituer un **comité IA** pluridisciplinaire (juridique, technique, métier, éthique)
- Intégrer l'**AI Act** dans les processus de conformité existants (RGPD, compliance)
- Établir une **politique IA** définissant les principes d'utilisation de l'IA
- Mettre en place un **registre IA** centralisé pour suivre tous les systèmes

11. Conclusion

Le Règlement (UE) 2024/1689 sur l'intelligence artificielle constitue une **avancée réglementaire majeure** à l'échelle mondiale. Premier cadre juridique global sur l'IA, il établit un équilibre entre protection des droits fondamentaux et préservation de l'innovation.

Points Clés à Retenir

1. **Approche fondée sur le risque** : Les obligations sont proportionnées au niveau de risque du système d'IA
2. **Application progressive** : De février 2025 (pratiques interdites) à décembre 2030 (systèmes IT à grande échelle)
3. **Portée extraterritoriale** : Toute organisation affectant des utilisateurs dans l'UE est concernée
4. **Sanctions significatives** : Jusqu'à 35 millions d'euros ou 7% du CA mondial
5. **Gouvernance multi-niveaux** : Coordination entre l'AI Office européen et les autorités nationales

Évolutions Attendues

Le cadre réglementaire continuera d'évoluer :

- Publication de **normes harmonisées** par les organismes de normalisation européens
- Émission de **lignes directrices** supplémentaires par la Commission
- Développement de **jurisprudence** par les autorités de contrôle et les tribunaux
- Potentielles **révisions du règlement** pour s'adapter aux évolutions technologiques

« L'AI Act n'est pas une fin en soi, mais le début d'un processus d'encadrement de l'intelligence artificielle qui évoluera avec la technologie. »

12. Annexes

Glossaire

Système d'IA

Système basé sur une machine conçu pour fonctionner avec différents niveaux d'autonomie, qui peut faire preuve d'adaptabilité après déploiement et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions.

Fournisseur (Provider)

Personne physique ou morale qui développe un système d'IA ou un modèle GPAI, ou fait développer un système d'IA ou un modèle GPAI, et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque.

Déployeur (Deployer)

Personne physique ou morale utilisant un système d'IA sous sa propre autorité, sauf lorsque le système d'IA est utilisé dans le cadre d'une activité personnelle à caractère non professionnel.

GPAI (General-Purpose AI)

Modèle d'IA à usage général capable d'exécuter de manière compétente un large éventail de tâches distinctes, indépendamment de la manière dont il est mis sur le marché.

Risque systémique

Risque spécifique aux capacités à fort impact des modèles GPAI, ayant un effet significatif sur le marché de l'Union en raison de leur portée, ou d'effets négatifs réels ou raisonnablement prévisibles sur la santé publique, la sécurité, les droits fondamentaux ou la société.

FLOPS

Floating Point Operations Per Second. Mesure de la puissance de calcul. Le seuil de risque systémique est fixé à 10^{25} FLOPS cumulés pour l'entraînement.

Marquage CE

Marquage attestant la conformité d'un produit aux exigences essentielles de la législation d'harmonisation de l'Union.

Bac à sable réglementaire (Regulatory Sandbox)

Cadre contrôlé établi par une autorité compétente permettant le développement, la formation et la validation de systèmes d'IA innovants pendant une durée limitée avant leur mise sur le marché.

Ressources Officielles

- [Texte officiel du Règlement \(EUR-Lex\)](#)
- [EU AI Act Portal \(analyses et résumés\)](#)
- [Commission Européenne - Cadre réglementaire IA](#)
- [Timeline d'implémentation officielle](#)
- [Guidelines pour les fournisseurs GPAI](#)
- [AI Act Service Desk de la Commission](#)

Calendrier Récapitulatif

Document : Livre Blanc – AI Act Européen : Le Guide de Référence

Version : 1.0

Date de publication : 20 janvier 2026

Auteur : JAIKIN

Ce document est fourni à titre informatif et ne constitue pas un avis juridique. Pour toute question spécifique relative à la conformité à l'AI Act, veuillez consulter un conseiller juridique qualifié.