L'IA Act

Le cadre réglementaire européen

Support pédagogique générique sur le cadre réglementaire de l'intelligence artificielle en Europe.

- Adoption en 2024 par l'Union européenne
- Encadrement des IA génératives et à haut risque
- Protection des droits fondamentaux et sécurité

Version 2025

L'IA Act : Le cadre réglementaire européen

Table des matières

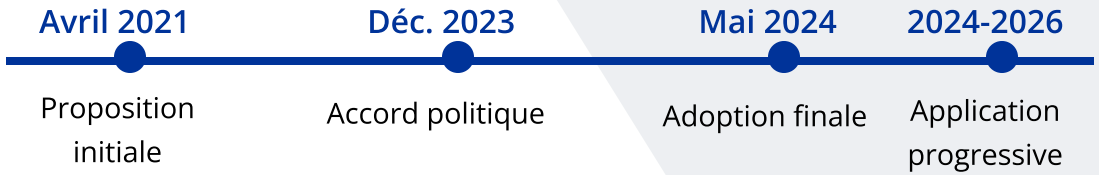
1. Introduction à l'IA Act

Le premier cadre européen dédié à l'intelligence artificielle

L'IA Act est la première législation complète au monde visant à réguler l'intelligence artificielle tout en favorisant son développement responsable.

- **Protection** : Garantit la sécurité et le respect des droits fondamentaux
- **Innovation** : Soutient le développement technologique responsable
- **Équilibre** : Approche proportionnée basée sur les risques
- **Leadership** : Établit un standard mondial de référence

Chronologie de l'IA Act



1er
Cadre réglementaire global au monde

4
Niveaux de risque définis

27
États membres concernés

7%
Sanction maximale (% du CA mondial)

Union Européenne

2. Objectifs et champ d'application

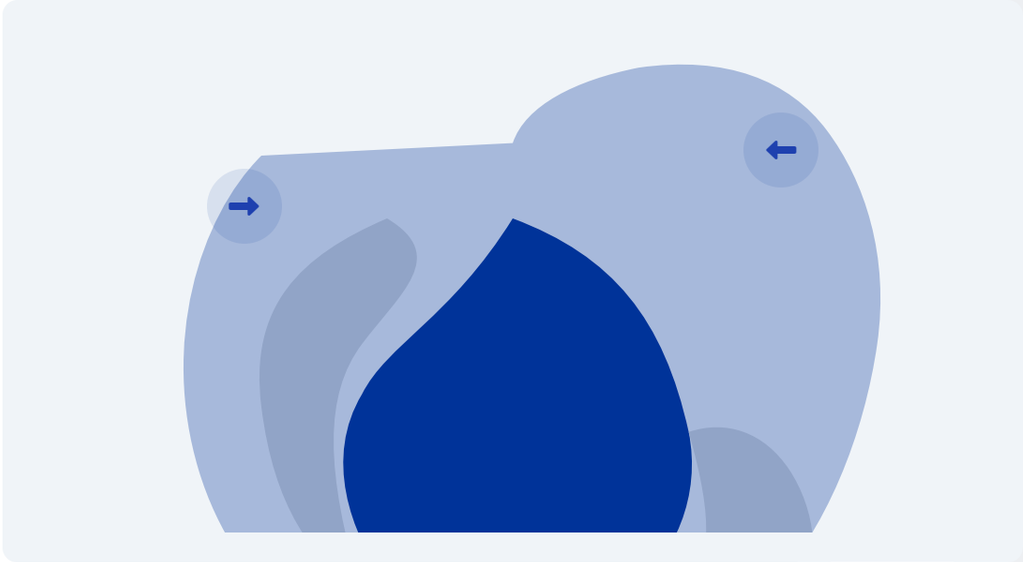
Objectifs principaux

- **Sécurité** : Garantir la sûreté et la fiabilité des systèmes d'IA
- **Droits fondamentaux** : Protéger la dignité et les libertés des citoyens européens
- **Innovation responsable** : Encourager le développement éthique de l'IA
- **Marché unique** : Harmoniser les règles à l'échelle européenne

Champ d'application

- **Fournisseurs** : Entreprises qui développent et commercialisent des systèmes d'IA dans l'UE
- **Utilisateurs** : Organisations déployant des systèmes d'IA sur le territoire européen
- **Acteurs hors UE** : Si leurs systèmes d'IA affectent des personnes dans l'Union

Application territoriale



- Union Européenne
- Zone d'influence
- Pays européens non-UE
- Effet extraterritorial

Effet Bruxelles : influence normative mondiale

Entreprises tech américaines | IA chinoise | Startups IA internationales | Plateformes britanniques

Union Européenne

3. Principes fondamentaux de l'IA Act

Les piliers de la réglementation européenne

L'IA Act s'articule autour de principes structurants qui équilibrent innovation et protection des droits :

Proportionnalité

Obligations réglementaires adaptées au niveau de risque identifié pour chaque système

Approche basée sur les risques

Classification des systèmes selon leur potentiel d'impact négatif sur les droits et la sécurité

Supervision humaine

Maintien d'un contrôle humain significatif sur les systèmes d'IA à haut risque

Innovation responsable

Encouragement du développement technologique dans un cadre éthique défini

Transparence

Obligation d'informer les utilisateurs et d'expliquer le fonctionnement des systèmes

Équilibre réglementaire

Proportionnalité
Obligations adaptées aux risques

Approche risques
Classification par niveau d'impact

Supervision
Contrôle humain effectif

Innovation
Développement encadré

Transparence
Information et explicabilité

Risques
Discrimination, surveillance, manipulation

=

Protection
Droits fondamentaux, sécurité, éthique

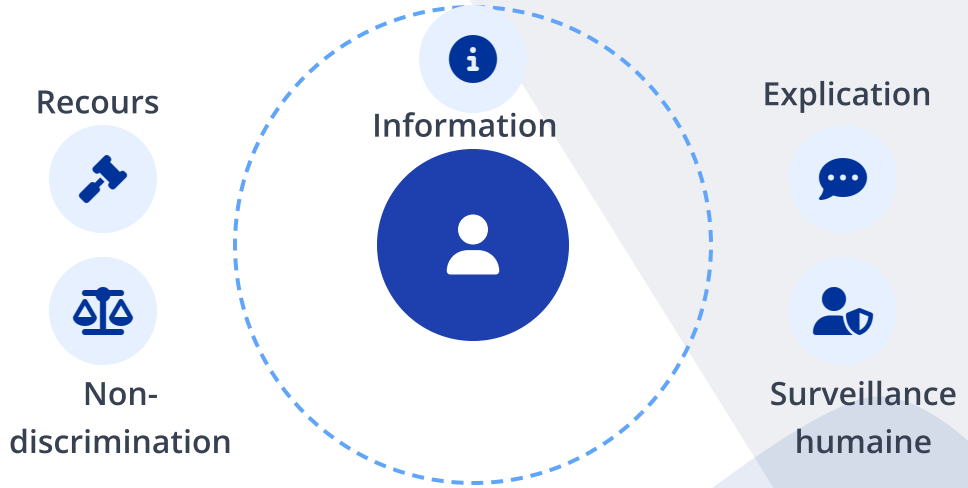
Union Européenne

4. Droits des personnes concernées

Protection des droits fondamentaux

L'IA Act établit des garanties concrètes pour les personnes interagissant avec des systèmes d'intelligence artificielle :

- **Droit à l'information** : Être informé qu'un système d'IA est utilisé et comprendre ses capacités
- **Droit à l'explication** : Recevoir une explication compréhensible des décisions automatisées
- **Droit à la surveillance humaine** : Garantie qu'un humain supervise les systèmes à haut risque
- **Droit à la non-discrimination** : Protection contre les biais et discriminations algorithmiques
- **Droit de recours** : Possibilité de contester une décision prise par un système d'IA



Principe clé : Les droits fondamentaux créent un bouclier protecteur entre les citoyens et l'IA, garantissant que la technologie respecte la dignité humaine.

Union Européenne

5. Typologie des risques IA

L'approche basée sur les risques

L'IA Act classe les systèmes d'intelligence artificielle en quatre niveaux de risque, avec des obligations réglementaires proportionnelles.

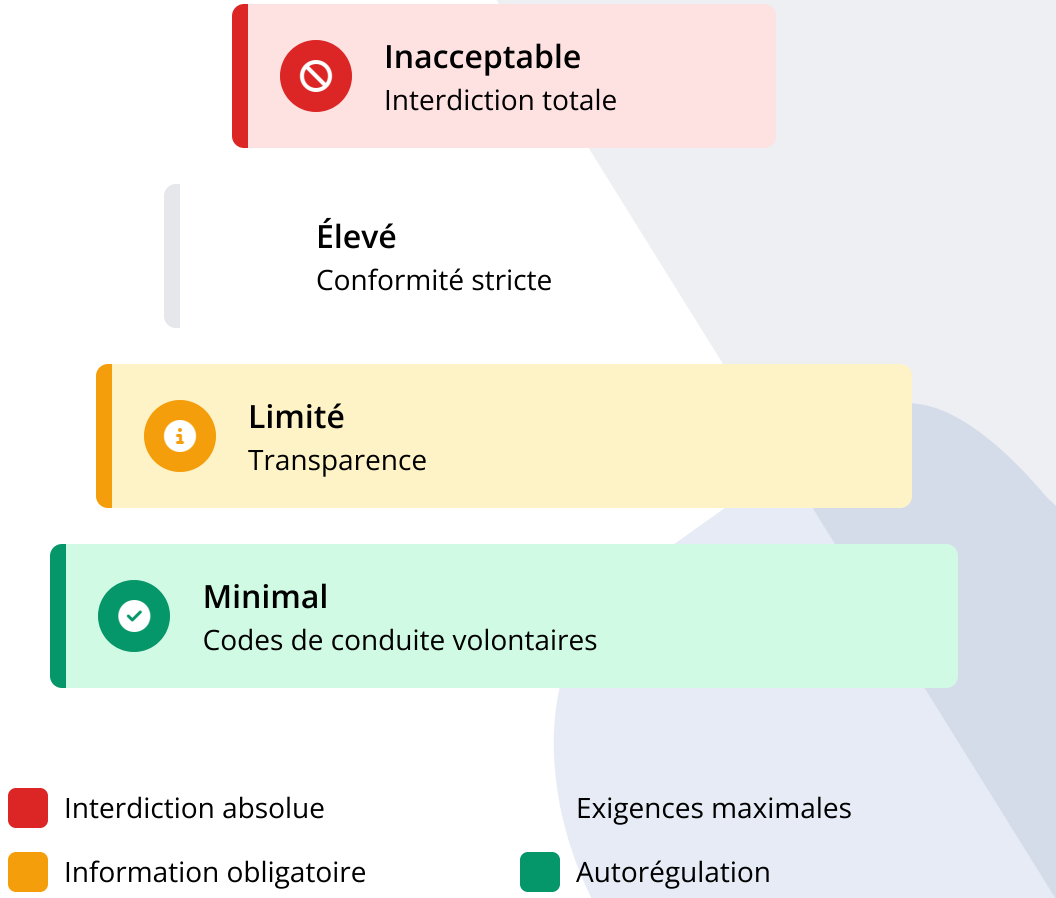
Risque inacceptable
Systèmes totalement interdits dans l'UE

Risque élevé
Systèmes soumis à des obligations strictes

Risque limité
Systèmes soumis à des obligations de transparence

Risque minimal
Systèmes sans obligations spécifiques

Pyramide des risques



Classification des systèmes d'IA

Les quatre niveaux de risque

L'IA Act établit une classification en 4 catégories selon le niveau de risque pour les droits et la sécurité des personnes :

Risque inacceptable (Systèmes interdits)
Pratiques incompatibles avec les valeurs européennes et explicitement interdites par l'IA Act.

Risque élevé
Systèmes pouvant impacter significativement les droits fondamentaux, la santé ou la sécurité. Soumis à des obligations strictes.

Risque limité
Systèmes présentant certains risques spécifiques. Soumis principalement à des obligations de transparence.

Risque minimal
Systèmes présentant peu ou pas de risques. Encouragement aux codes de conduite volontaires.

L'essentiel : Le niveau de risque détermine directement le niveau d'obligation réglementaire applicable au système d'IA.

Description détaillée par niveau

Risque inacceptable
Manipulation comportementale, notation sociale, identification biométrique en temps réel dans les espaces publics.

Risque élevé
Infrastructures critiques, éducation, recrutement, crédit scoring, applications médicales, contrôle des frontières, justice.

Risque limité
Chatbots, assistants virtuels, générateurs de contenu (deep fake), reconnaissance d'émotions, catégorisation biométrique.

Risque minimal
Applications grand public à faible impact, jeux vidéo, filtres photos, outils de productivité, applications industrielles simples.

9. Exemples de classification

Cas d'usage par catégorie

L'IA Act classe les systèmes d'IA selon leur niveau de risque et leur cas d'usage. Voici quelques exemples concrets illustrant cette classification :

Risque inacceptable (interdit)
Systèmes de notation sociale par les autorités publiques, manipulation comportementale

Risque élevé
IA de recrutement, diagnostic médical, systèmes d'évaluation éducative

Risque limité
Chatbots, systèmes deepfake, reconnaissance d'émotions

Risque minimal
Filtres photos, jeux vidéo, systèmes de recommandation basiques

> La classification détermine les obligations légales et mesures de conformité nécessaires pour chaque système d'IA.

Exemples illustrés

Notation sociale
Évaluation générale des citoyens par les pouvoirs publics
INTERDIT

IA de recrutement
Analyse automatisée de CV et sélection de candidats
RISQUE ÉLEVÉ

Chatbots
Assistants virtuels conversationnels
RISQUE LIMITÉ

Deepfake
Génération de contenu visuel et audio artificiel
RISQUE LIMITÉ

10. Critères de classification des IA

Comment déterminer le niveau de risque d'un système d'IA

L'IA Act établit une méthode d'évaluation fondée sur quatre critères clés pour déterminer la classification d'un système d'IA :

Secteur d'application

Certains secteurs comme la santé, l'éducation, la justice et la sécurité sont automatiquement considérés à plus haut risque

Finalité et usage prévu

L'objectif poursuivi par le système et la nature des décisions qu'il est amené à prendre

Impact potentiel

Conséquences possibles sur les droits fondamentaux, la santé ou la sécurité des personnes

Niveau d'autonomie

Degré d'intervention humaine dans le processus de décision et possibilité de supervision

Processus d'évaluation

1

Identification du système d'IA

Est-ce un système utilisant l'IA selon la définition légale ?

2

Vérification des interdictions

Le système appartient-il à une catégorie interdite ?

3

Analyse du secteur et de la finalité

Domaine sensible ou usage à risque ?

4

Évaluation d'impact et autonomie

Quelles conséquences possibles et quel niveau de contrôle ?

La classification détermine directement les obligations légales applicables

11. Obligations pour systèmes à haut risque

Exigences réglementaires obligatoires

L'IA Act impose un cadre strict de conformité pour les systèmes d'intelligence artificielle classés à haut risque, avec quatre piliers principaux :

Système de gestion des risques
Identification, analyse et atténuation systématique des risques potentiels tout au long du cycle de vie

Gouvernance des données
Garanties de qualité, pertinence et représentativité des données d'entraînement et de test

Documentation technique
Description détaillée du système, algorithmes, processus de développement et validation

Registres automatiques
Enregistrement des événements et traçabilité des décisions pour audit et contrôle

Les 4 piliers de conformité

Gestion des risques
Analyse, évaluation et mesures d'atténuation adaptées au contexte d'utilisation

Qualité des données
Minimisation des biais, représentativité et validation des datasets

Documentation
Spécifications complètes, description des algorithmes et processus de test

Registres automatiques
Journalisation des événements et conservation des données pour audit

Ces obligations sont cumulatives et doivent être maintenues durant tout le cycle de vie du système.

10. Cycle de vie des systèmes IA à haut risque

Obligations à chaque phase du cycle

L'IA Act impose des exigences spécifiques tout au long du cycle de vie des systèmes à haut risque, de la conception à l'exploitation.

Phase de conception

- **Analyse d'impact** : Évaluation préalable des risques potentiels
- **Qualité des données** : Sources pertinentes et représentatives
- **Documentation technique** : Spécifications et méthodes

Phase de déploiement

- **Formation des utilisateurs** : Instructions d'utilisation
- **Paramétrage** : Configuration pour usage prévu
- **Test pré-production** : Validation avant usage réel

Phase d'exploitation

- **Surveillance continue** : Monitoring des performances
- **Maintenance préventive** : Mises à jour régulières
- **Gestion des incidents** : Procédures d'alerte

Frise chronologique du cycle de vie

1. CONCEPTION

- Analyse des risques
- Tests préliminaires
- Documentation technique
- Plan de surveillance

↓

2. DÉPLOIEMENT

- Formation utilisateurs
- Supervision humaine
- Transparence
- Registres automatiques

↓

3. EXPLOITATION

- Monitoring continu
- Mises à jour
- Gestion des incidents
- Audits réguliers

13. Cybersécurité et robustesse

Exigences de sécurité pour les systèmes IA

L'IA Act impose des mesures strictes pour garantir la sécurité et la robustesse des systèmes d'IA, particulièrement pour les applications à haut risque.

Protection technique
Chiffrement des données, contrôle d'accès, authentification forte et mesures anti-intrusion

Résistance aux attaques
Tests réguliers de robustesse face aux tentatives de manipulation ou de détournement

Gestion des incidents
Procédures d'alerte, de réponse et d'atténuation en cas de faille ou de dysfonctionnement

Continuité de service
Plans de reprise d'activité et redondance des systèmes critiques

À noter : Les incidents de sécurité affectant un système IA à haut risque doivent être signalés aux autorités dans les 72 heures.

Mesures de cybersécurité

Chiffrement
Protection des données sensibles et des communications

Tests de pénétration
Évaluation régulière des vulnérabilités

Plans de reprise
Capacité à retrouver un état normal après incident

Surveillance
Détection d'anomalies et d'activités suspectes

Sécurité by design
La sécurité doit être intégrée dès la conception et non ajoutée après coup

12. Systèmes d'IA interdits

Pratiques prohibées par l'IA Act

L'IA Act interdit formellement certaines applications de l'intelligence artificielle jugées incompatibles avec les valeurs européennes et les droits fondamentaux.

- **Manipulation comportementale** : Systèmes utilisant des techniques subliminales pour altérer le comportement d'une personne ou exploitant les vulnérabilités liées à l'âge ou au handicap
- **Notation sociale** : Systèmes d'évaluation générale de la fiabilité des personnes par les autorités publiques aboutissant à des traitements préjudiciables
- **Identification biométrique à distance en temps réel** : Dans les espaces publics (avec exceptions très limitées pour certaines infractions graves)

Ces interdictions s'appliquent sans exception à tout déploiement dans l'UE, quelle que soit l'origine du fournisseur de l'IA.

Catégories de systèmes interdits

Manipulation comportementale

INTERDIT

Systèmes conçus pour manipuler le comportement humain par des techniques subliminales ou l'exploitation de vulnérabilités spécifiques

Notation sociale

INTERDIT

Évaluation ou classement des individus sur la base de leur comportement social ou de caractéristiques personnelles

Identification biométrique en temps réel

INTERDIT DÉROGATIONS LIMITÉES

Systèmes d'identification biométrique à distance en temps réel dans les espaces publics

13. Dérogations et exceptions

Identification biométrique : cas exceptionnels

Bien que l'identification biométrique en temps réel dans les espaces publics soit généralement interdite, l'IA Act prévoit des exceptions strictement limitées :

- **Recherche de victimes spécifiques** : Personnes disparues, victimes d'enlèvement ou d'exploitation
- **Menaces terroristes** : Prévention d'une menace terroriste spécifique et présente
- **Infractions graves** : Recherche d'auteurs de crimes spécifiquement listés

Conditions strictes requises :

- Autorisation préalable judiciaire ou administrative indépendante
- Limitations dans le temps et l'espace
- Supervision indépendante et reporting obligatoire
- Documentation des utilisations et justifications

Processus d'autorisation pour les dérogations

1. Demande d'autorisation

Soumission d'une demande documentée précisant le cas d'exception applicable, l'objectif précis et la durée envisagée

2. Évaluation indépendante

Examen par une autorité judiciaire ou administrative indépendante selon des critères de nécessité et proportionnalité

3. Autorisation limitée

Décision bornée dans le temps et l'espace, avec des conditions strictes d'utilisation et de périmètre

4. Contrôle continu

Surveillance permanente, rapports obligatoires et possibilité de révocation de l'autorisation à tout moment

Ces exceptions ne constituent pas un droit général à l'utilisation de l'identification biométrique dans l'espace public

16. Transparence et information

Obligations d'information des utilisateurs

L'IA Act impose des exigences de transparence pour permettre aux utilisateurs de comprendre qu'ils interagissent avec un système d'IA et d'en connaître les limites.

Identification des systèmes d'IA

L'utilisateur doit être clairement informé lorsqu'il interagit avec un système d'IA comme un chatbot

Contenu généré par IA

Obligation de signaler le contenu créé ou manipulé par intelligence artificielle

Limites et capacités

Information sur le fonctionnement général, les performances et les limites du système

Recours humain

Indication des possibilités de contacter un opérateur humain quand nécessaire

Exemples de mentions obligatoires

Article sur un site d'information

GÉNÉRÉ PAR IA

Ce contenu a été partiellement ou entièrement généré à l'aide d'un système d'intelligence artificielle. Les informations présentées doivent être vérifiées auprès de sources officielles avant toute utilisation professionnelle.

Interface de chatbot

Assistant IA

Bonjour, comment puis-je vous aider aujourd'hui ?

AVERTISSEMENT DE TRANSPARENCE

Vous discutez avec un assistant virtuel basé sur l'intelligence artificielle. Il peut commettre des erreurs ou mal interpréter certaines demandes. Pour toute décision importante, veuillez consulter un expert humain.

Éléments à vérifier

- Information claire et visible
- Langage compréhensible
- Accessibilité pour tous les utilisateurs
- Indication des limitations du système

17. Exemples sectoriels (RH et éducation)

Obligations spécifiques par secteur

Recrutement assisté par IA

Les systèmes d'IA utilisés dans les processus de recrutement sont considérés à haut risque et doivent respecter des obligations spécifiques :

- ✓ **Information préalable** aux candidats
- ✓ **Transparence des critères** d'évaluation
- ✓ **Supervision humaine** obligatoire
- ✓ **Droit de contestation** des décisions

Éducation assistée par IA

Dans le domaine éducatif, les systèmes d'IA sont soumis à un cadre de protection renforcé :

- ✓ **Contrôle pédagogique humain** constant
- ✓ **Information** des élèves et parents
- ✓ **Protection renforcée** des données des mineurs
- ✓ **Équité et non-discrimination** dans l'évaluation

Cas du recrutement par IA

✗ Non conforme

Algorithme de présélection automatique sans information aux candidats ni explication des critères

✓ Conforme

Système d'aide à la décision avec notification, critères transparents et validation humaine finale

Cas de l'éducation assistée par IA

✗ Non conforme

Système automatisé d'évaluation et d'orientation des élèves sans supervision enseignante

✓ Conforme

IA comme outil d'assistance pédagogique avec validation par l'enseignant des recommandations

+ L'IA comme assistant, jamais comme décideur final

Gouvernance IA et contrôle

Structure de gouvernance européenne

Comité européen de l'IA
Coordonne les politiques nationales et établit des lignes directrices communes pour toute l'Union

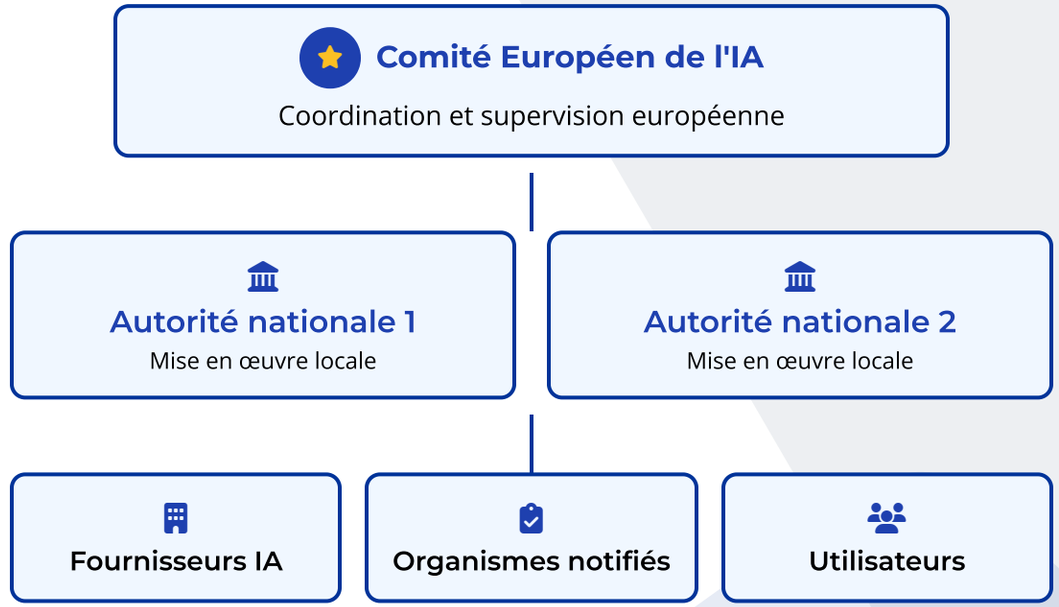
Autorités nationales
Chaque État membre désigne une autorité compétente pour la mise en œuvre et le contrôle

Audits réguliers
Contrôles périodiques des systèmes à haut risque et vérification de conformité

Accès aux données
Les autorités peuvent accéder aux données et algorithmes pour vérifier la conformité

Les organismes notifiés indépendants réalisent les évaluations de conformité pour les systèmes à haut risque avant leur mise sur le marché.

Organigramme de la gouvernance IA



Mécanismes de contrôle

- Signalements d'incidents
- Inspections régulières
- Évaluations de conformité
- Alertes et sanctions

Union Européenne

19. Contrôle, audit et sanctions

Un régime dissuasif et proportionné

Sanctions administratives : Amendes calculées selon la gravité de l'infraction et la taille de l'entreprise

Mesures correctives : Injonctions, suspension temporaire ou retrait définitif du marché

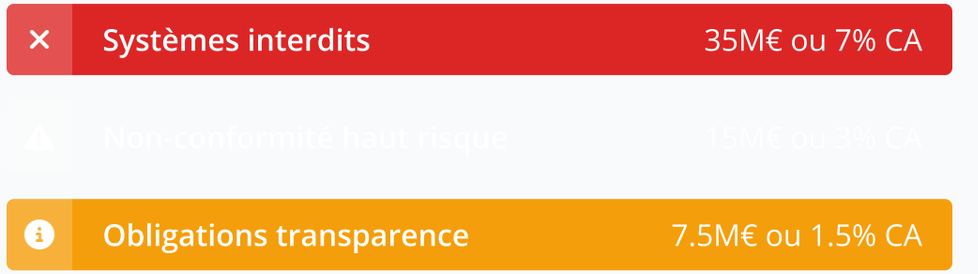
Procédures de contrôle

Auto-évaluation
Pour certains systèmes à haut risque, avec documentation à conserver

Audit externe
Évaluation par des organismes notifiés indépendants

Marquage CE
Obligatoire pour les systèmes conformes mis sur le marché

Baromètre des sanctions



Processus d'évaluation

1. **Classification du niveau de risque**
   Déterminer si le système est à haut risque
2. **Documentation et tests**
   Constitution du dossier technique
3. **Conformité et marquage**
   Obtention du marquage CE obligatoire

CE Marquage obligatoire
Attestation visible de conformité

Union Européenne

Conclusion & points clés à retenir

L'IA Act en synthèse

- **Approche basée sur les risques** : Obligations proportionnelles au niveau de risque identifié
- **Protection des droits** : Garanties pour les personnes impactées par l'IA
- **Transparence** : Exigence d'explicabilité des décisions automatisées
- **Supervision humaine** : Maintien du contrôle sur les systèmes à haut risque

L'IA Act n'est pas un frein à l'innovation mais un cadre pour une IA éthique et responsable au service des citoyens européens.

Préparer votre organisation

Check-list de conformité

- [x] Inventaire des systèmes d'IA utilisés
- [x] Classification selon les niveaux de risque
- [ ] Évaluation d'impact pour les systèmes à haut risque
- [ ] Documentation technique et registres obligatoires
- [ ] Formation des équipes aux exigences IA Act

IA
IA ACT
UNION EUROPÉENNE
2024-2026

Union Européenne