Conformité IA en entreprise

Comprendre, encadrer et sécuriser les usages de l'intelligence artificielle

AI Act européen, cybersécurité, RGPD et gouvernance interne

L'intelligence artificielle devient un outil stratégique, mais son utilisation doit être maîtrisée pour éviter les risques juridiques, cyber et organisationnels.

Réglementation

AI Act européen et obligations progressives 2025–2027

Cybersécurité

Contrôles techniques, DLP, journalisation et filtrage

RGPD

Protection des données personnelles et rôle du DPO

Gouvernance

Politique interne, inventaire et validation des outils IA

Pourquoi parler de conformité IA ?

L'IA est déjà utilisée dans les entreprises à travers des outils comme :

Outils IA courants en entreprise

- Microsoft Copilot
- ChatGPT
- Mistral AI
- Notion AI
- Gemini
- Claude
- Outils RH, finance, marketing ou support client intégrant de l'IA

Le risque principal

Le risque principal n'est pas uniquement l'outil lui-même, mais **ce que les collaborateurs y déposent** :

- Données personnelles et données clients
- Documents internes et contrats
- Mots de passe et fiches de paie
- Informations confidentielles

Message clé : La conformité IA commence par l'identification des usages réels dans l'entreprise.

Le cadre réglementaire européen : AI Act

L'**AI Act**, ou règlement européen sur l'intelligence artificielle, est le premier cadre juridique complet au monde consacré à l'IA. Il vise à encadrer les systèmes d'IA selon leur niveau de risque et à favoriser une IA fiable, transparente et sécurisée.

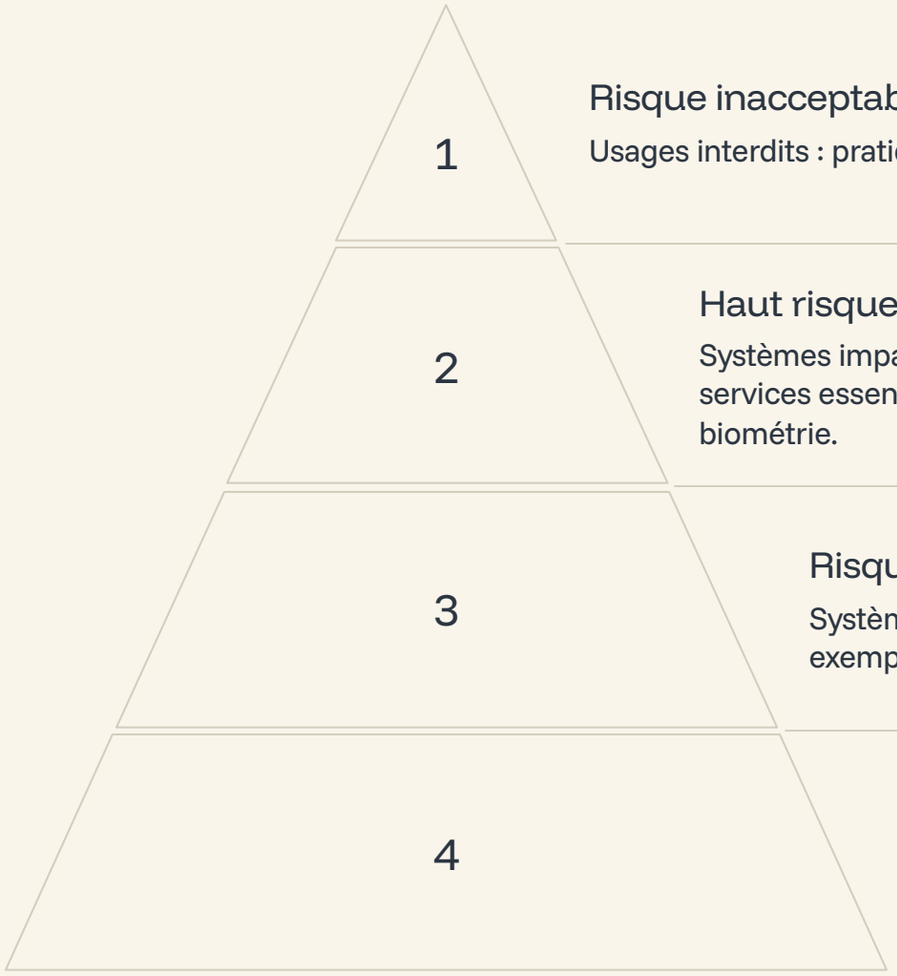
Les obligations s'appliquent progressivement :

1. **2 février 2025**
   Application des règles générales, de l'AI literacy et des interdictions sur certains usages IA.
2. **2 août 2025**
   Application des règles relatives aux modèles d'IA à usage général.
3. **2 août 2026**
   Application d'une grande partie du règlement, notamment plusieurs obligations liées aux systèmes IA à haut risque.
4. **2 août 2027**
   Déploiement complet prévu du règlement.

Message clé : L'entreprise ne doit pas attendre l'audit ou le contrôle pour structurer sa gouvernance IA.

Les niveaux de risque de l'AI Act

L'AI Act repose sur une logique de classification par risque.



Risque inacceptable

Usages interdits : pratiques manipulatoires, scoring social.

Haut risque

Systèmes impactant les droits fondamentaux, la sécurité ou l'accès à des services essentiels : RH, recrutement, éducation, infrastructures critiques, biométrie.

Risque limité

Systèmes nécessitant principalement de la transparence, par exemple informer l'utilisateur qu'il interagit avec une IA.

Risque minimal

Usages courants avec peu d'impact direct : assistance à la rédaction ou aide à la productivité.

Message clé : Tous les outils IA ne présentent pas le même niveau de risque, mais tous doivent être recensés.

Les principaux risques pour l'entreprise

L'usage non maîtrisé de l'IA peut entraîner :

Fuite de données

Fuite de données confidentielles et exposition de données personnelles.

Non-conformité RGPD

Non-respect du RGPD, risque d'audit ou de sanction réglementaire.

Réponses erronées

Réponses non vérifiées et absence de traçabilité des décisions.

Dépendance fournisseur

Dépendance à un fournisseur externe et utilisation d'outils non validés.

Perte de confiance

Perte de confiance des clients ou partenaires suite à un incident.

Message clé : L'IA doit être traitée comme un sujet de sécurité, de conformité et de gouvernance.

Les sanctions possibles

Le non-respect de certaines obligations de l'AI Act peut entraîner des sanctions administratives importantes.

35M€

ou 7 % du CA mondial

Violations liées aux pratiques interdites (montant le plus élevé retenu).

15M€

ou 3 % du CA mondial

Autres violations des obligations de l'AI Act (montant le plus élevé retenu).

Message clé : Le risque n'est pas seulement technique : il est aussi financier, juridique et réputationnel.

Ce que l'entreprise doit mettre en place

Pour encadrer l'IA, l'entreprise doit progressivement mettre en place :

01

Inventaire des outils IA

Recenser tous les outils IA utilisés dans l'entreprise, par service et par usage.

02

Politique d'usage

Définir une politique d'usage de l'IA et une classification des usages selon le niveau de risque.

03

Validation et analyse

Valider les outils autorisés et analyser les données manipulées par chaque outil.

04

Sensibilisation

Former les collaborateurs aux risques IA et mettre en place une procédure de déclaration des nouveaux outils.

05

Contrôle et traçabilité

Mettre en place des contrôles de sécurité, de conformité et une traçabilité des décisions et audits.

Message clé : La conformité IA doit devenir un processus continu, pas une action ponctuelle.

Gouvernance interne recommandée

Une gouvernance IA efficace repose sur plusieurs acteurs :

Rôle	Responsabilité
Direction	Valider la stratégie IA et accepter les risques
CISO / RSSI	Encadrer la sécurité, les risques cyber et les contrôles
DPO	Vérifier les impacts RGPD et données personnelles
IT	Contrôler les accès, outils, logs et intégrations
Métiers	Déclarer les usages réels et les besoins opérationnels
Achats / Juridique	Vérifier les contrats, fournisseurs et clauses de conformité

Message clé : La conformité IA ne peut pas reposer uniquement sur l'IT. Elle doit être collective.

Exemple de politique interne IA

Règles internes recommandées :

1	**Validation préalable obligatoire** Aucun nouvel outil IA ne doit être utilisé sans validation préalable.
2	**Outils audités sous surveillance** Les outils déjà audités peuvent être autorisés sous surveillance.
3	**Protection des données confidentielles** Les données confidentielles ne doivent pas être déposées dans des IA publiques non approuvées.
4	**Déclaration des outils utilisés** Les collaborateurs doivent déclarer les outils IA utilisés.
5	**Analyse de risque pour usages sensibles** Les usages sensibles doivent faire l'objet d'une analyse de risque.
6	**Validation humaine des sorties IA** Les sorties générées par IA doivent être relues et validées par un humain.
7	**Journalisation des accès IA** Les accès IA doivent être journalisés lorsque cela est possible.

Message clé : L'objectif n'est pas de bloquer l'innovation, mais de la sécuriser.

Inventaire des outils IA

L'entreprise doit identifier : nom de l'outil, service utilisateur, finalité d'usage, type de données traitées, fournisseur, localisation des données, présence ou non de données personnelles, niveau de risque, validation IT / sécurité / DPO, et statut.

Exemple de statut :

Outil	Usage	Statut
Microsoft Copilot	Productivité interne	**Autorisé sous contrôle**
ChatGPT Enterprise / Team	Assistance rédactionnelle	À auditer / surveiller
Notion AI	Documentation	À analyser
Outil IA inconnu	Usage non déclaré	**Interdit temporairement**

⚠ **Message clé :** On ne peut pas sécuriser ce que l'on ne connaît pas.

Contrôles techniques recommandés

Mesures possibles côté IT / cybersécurité :

Filtrage web

Filtrage web des IA non autorisées et blocage des extensions IA non validées.

Accès contrôlé

Accès IA uniquement depuis un navigateur contrôlé et journalisation des accès.

Supervision DLP

Supervision via DLP et alertes en cas de partage de données sensibles.

Revue périodique

Revue régulière des outils autorisés et mise à jour de la liste blanche.

Sensibilisation

Sensibilisation contre le copier-coller de données sensibles dans les IA publiques.

Gestion des incidents

Procédure de suppression de données en cas d'incident ou de fuite avérée.

Message clé : La conformité IA doit s'appuyer sur des règles, mais aussi sur des contrôles techniques.

Bonnes pratiques pour les collaborateurs

✅ À faire

- Utiliser uniquement les outils IA autorisés
- Anonymiser les données avant usage
- Vérifier les réponses générées
- Déclarer tout nouvel outil IA
- Demander validation en cas de doute
- Signaler tout incident ou fuite potentielle

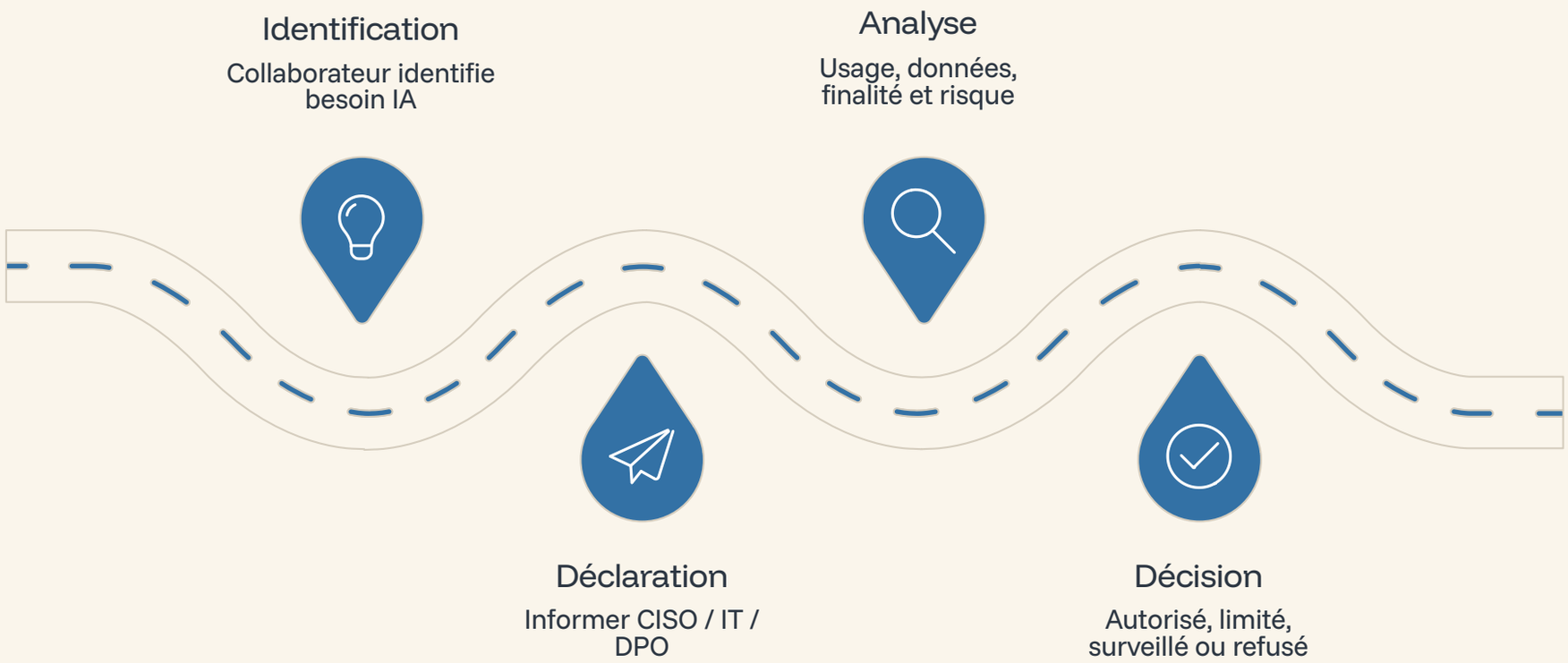
❌ À éviter

- Copier-coller des fiches de paie
- Envoyer des mots de passe
- Déposer des contrats confidentiels
- Partager des données clients
- Utiliser une IA personnelle pour des documents professionnels
- Prendre une décision RH, juridique ou financière uniquement sur la base d'une IA

Message clé : L'humain reste responsable de l'usage et de la validation des résultats IA.

Exemple de processus de validation IA

Chaque nouvel usage IA doit passer par un circuit de validation clair :



Ce processus garantit que chaque outil IA est évalué de manière structurée avant toute utilisation en production, et que les décisions sont documentées et révisables dans le temps.

Message clé : Chaque nouvel usage IA doit passer par un circuit de validation clair.

Plan d'action conformité IA

Étape 1 — Inventaire

Recenser tous les outils IA utilisés dans l'entreprise.

Étape 2 — Classification

Classer les usages selon le niveau de risque.

Étape 3 — Encadrement

Définir les outils autorisés et interdits.

Étape 4 — Sensibilisation

Former les collaborateurs aux risques IA.

Étape 5 — Contrôle

Mettre en place DLP, logs, filtrage et surveillance.

Étape 6 — Audit

Préparer les preuves de conformité et les revues périodiques.

Message clé : La conformité IA doit être documentée, prouvable et maintenue dans le temps.

Les quatre piliers de la conformité IA

Identifier

Recenser tous les usages IA réels dans l'entreprise, par service et par outil.

Évaluer

Analyser les risques associés à chaque outil : données, fournisseur, finalité, niveau de risque AI Act.

Encadrer

Définir et appliquer une politique interne claire sur les outils autorisés et les règles d'usage.

Contrôler

Mettre en place des contrôles techniques et organisationnels sur les données et les accès.

> *L'IA ne doit pas devenir une zone grise dans l'entreprise. Elle doit être gouvernée comme n'importe quel actif critique.*

Conclusion

L'intelligence artificielle représente une opportunité majeure pour l'entreprise, mais elle doit être utilisée dans un cadre maîtrisé.

Une opportunité à saisir

L'IA améliore la productivité, la qualité des décisions et la compétitivité. Ces bénéfices ne peuvent être pleinement réalisés que dans un cadre de confiance et de maîtrise.

Un cadre à construire dès maintenant

Les obligations réglementaires de l'AI Act s'appliquent progressivement jusqu'en 2027. Anticiper permet d'éviter les sanctions et de structurer une gouvernance solide.

Une responsabilité collective

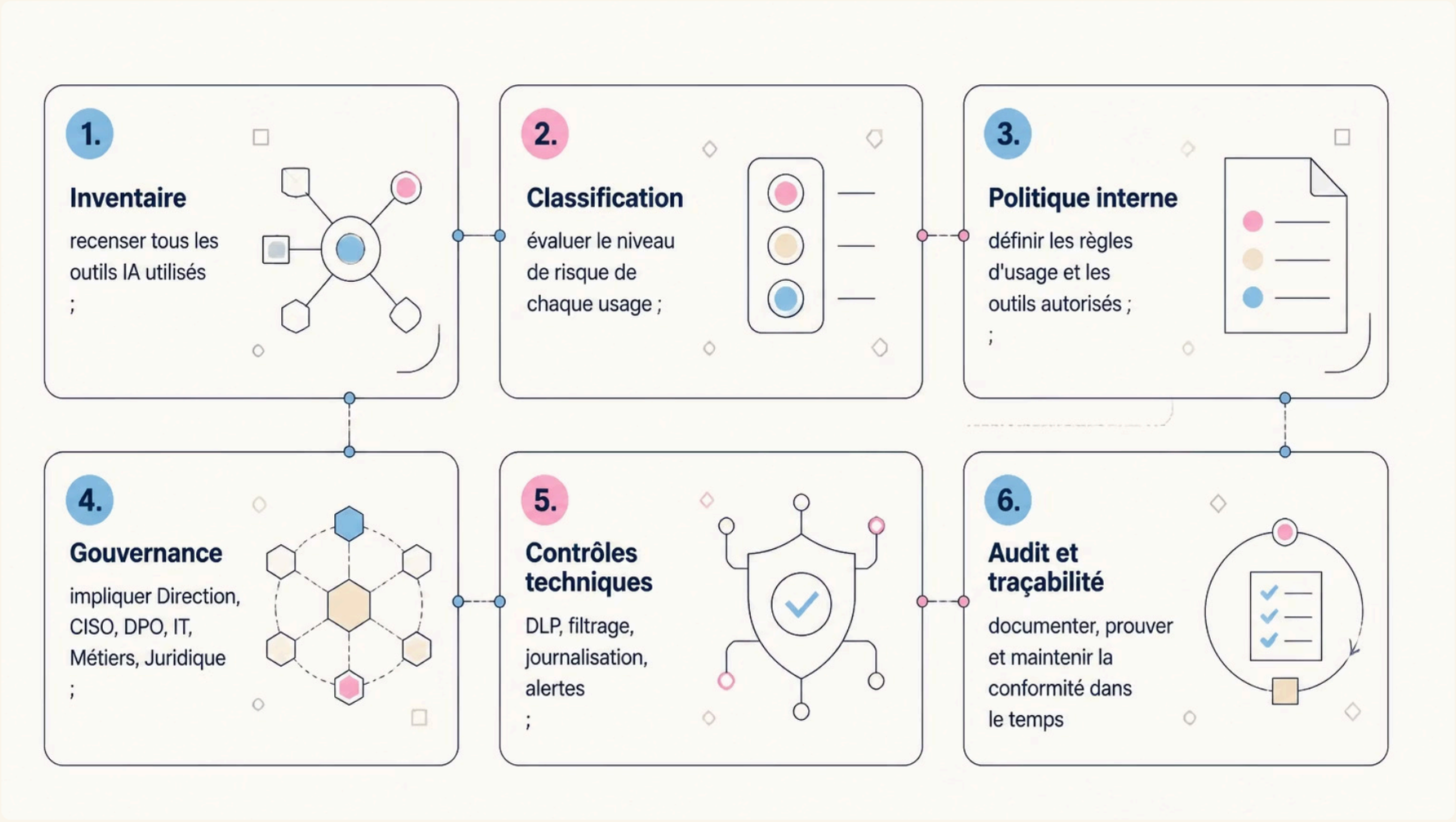
La conformité IA implique la Direction, le CISO, le DPO, l'IT, les métiers et le juridique. Elle ne peut pas reposer sur un seul acteur.

Un processus continu

La conformité IA n'est pas une action ponctuelle. Elle doit être documentée, prouvable et maintenue dans le temps à travers des audits et des revues périodiques.

SYNTHÈSE

Récapitulatif des actions prioritaires



Ces six priorités constituent le socle minimal d'une conformité IA robuste, alignée avec les exigences de l'AI Act européen et les bonnes pratiques de cybersécurité et de protection des données.

Conformité IA : agir maintenant pour éviter les risques demain

Questions / échanges

📋 Inventaire

Avez-vous déjà recensé les outils IA utilisés dans votre entreprise ?

🔒 Politique

Disposez-vous d'une politique interne encadrant l'usage de l'IA ?

⚖️ Conformité

Votre organisation est-elle prête pour les échéances de l'AI Act 2025–2027 ?

> *L'IA ne doit pas devenir une zone grise dans l'entreprise. Elle doit être gouvernée comme n'importe quel actif critique.*