Conformité IA en Europe

Par où commencer et pourquoi le RGPD seul ne suffit pas

Selon votre métier, vos systèmes et vos usages, plusieurs textes peuvent s'appliquer simultanément. Mais pas tous. Et pas à tout le monde. Ce guide pratique vous aide à identifier précisément ce qui vous concerne et à savoir par où commencer.

DPO · RSSI · DÉCIDEURS MÉTIERS

RGPD · AI ACT · NIS2 · DORA · CRA

Le problème de visibilité

80 % des organisations sans vision claire de leurs usages IA

Baromètre Privacy 2026 — EQS Group (206 professionnels DPO, 35 % PME / 41 % ETI, fév. 2026)

80%

Sans vision claire

Des organisations n'ont pas de vision consolidée de leurs usages IA internes

48%

Sans inventaire AI Act

N'ont pas identifié leurs systèmes IA au sens de l'AI Act

32%

Cartographie partielle

Ont une cartographie incomplète, sans analyse de risque associée

Dans beaucoup d'organisations : l'IT a déployé Copilot, le marketing utilise ChatGPT, les RH ont un outil de recrutement IA, les commerciaux un CRM avec scoring intégré. **Personne n'a la liste complète. Personne ne sait qui répondrait en cas de contrôle.**

Sans doute que la question à se poser avant les textes est : qui utilise quoi, pour quelles décisions ?

Faites la liste. Tout le reste en découle. Votre organisation a-t-elle un inventaire de ses systèmes IA ?

Ce que le RGPD couvre, et ce qu'il ne couvre pas

Le RGPD est une base solide. Pas un périmètre complet.

Le RGPD exige déjà une responsabilité continue : analyses d'impact (DPIA), gestion des violations, privacy by design, documentation des traitements. Mais il régule la **donnée personnelle**, pas le comportement du système IA.

📋 Présélection CV

- ✅ Données collectées avec consentement : **RGPD conforme**
- ❌ Aucun log permettant de reconstituer pourquoi un candidat a été écarté : **AI Act Art. 12 (systèmes haut risques) non couvert**

💳 Scoring crédit

- ✅ Droit à l'explication documenté : **RGPD Art. 22 conforme**
- ❌ Supervision humaine effective non documentée : **AI Act Art. 14 non couvert (pour système haut risque)**

Ce ne sont pas des redondances. Ce sont des **objets réglementaires différents** qui coexistent et se complètent. Avez-vous identifié ce que votre RGPD existant ne couvre pas sur vos systèmes IA ?

Les textes : à qui s'appliquent-ils ?

Votre contexte détermine les textes. Pas la technologie.

Trois questions structurantes à poser avant d'ouvrir un règlement :

1

Traitez-vous des données personnelles ?

→ **RGPD** applicable à quasi toutes les organisations traitant des données de résidents UE

2

Votre IA prend-elle des décisions significatives sur des personnes ?

→ **AI Act** : regarder la classification de risque Annexe III (recrutement, crédit, santé, accès à des services)

3

Êtes-vous dans un secteur critique ou construisez-vous un produit ?

→ Secteur essentiel : **NIS2** · Secteur financier : **DORA** (janv. 2025) · Produits numériques mis sur le marché UE : **CRA**

ⓘ Ces textes ne s'accumulent pas par défaut. Utiliser une API IA en interne ne déclenche ni le CRA ni le Data Act.

Trois situations, trois périmètres

Ce que ça donne en pratique

PME de services — Copilot bureautique

- ✅ RGPD applicable
- ✅ AI Act Deployer — obligations légères : littératie (Art. 4, fév. 2025), transparence tiers (Art. 50, août 2026)
- ❌ Haut risque AI Act, NIS2, DORA, CRA : hors périmètre

Banque — scoring crédit automatisé

- ✅ RGPD Art. 22 (décision automatisée à effet significatif)
- ✅ AI Act Annexe III point 5(b) — haut risque, deadline déc. 2027
- ✅ DORA : fournisseur du modèle dans cartographie ICT (janv. 2025)

Fabricant — équipement de surveillance connecté

- ✅ RGPD — données biométriques (catégorie sensible Art. 9)
- ✅ AI Act Art. 5 et Annexe III — potentiellement interdit ou haut risque
- ✅ CRA — sécurité by design et gestion des vulnérabilités

Les nouvelles obligations opérationnelles

Ce que le RGPD seul ne produit pas

Pour les Providers — systèmes haut risque

- **Art. 12** : logs d'exécution reconstituant le contexte de chaque décision significative
- **Art. 14** : supervision humaine testée et documentée — pas seulement déclarée
- **Art. 17** : système de management qualité (QMS)

Pour les Deployers — API ou SaaS IA (Art. 26)

- Documenter la supervision humaine effective
- Conserver les logs pendant **6 mois minimum**
- Informer les utilisateurs finaux si l'IA prend des décisions les affectant individuellement

Pour tous — dès maintenant

- **Art. 4** : littératie IA des équipes (depuis fév. 2025)
- **Art. 50** : transparence si interaction IA–personnes (août 2026)

⚠ La documentation RGPD existante est un point de départ. Elle ne se substitue pas à ces obligations opérationnelles spécifiques.

Ce que l'Omnibus change pour les PME

Des allègements ciblés — pas une dispense générale

Voté par le Parlement européen le **16 juin 2026** (423 voix). Adoption formelle du Conseil imminente. ⚠️ Jusqu'à publication au Journal officiel : calendrier 2024 en vigueur.

🗓️ Deadlines repoussées

- **Annexe III** (recrutement, crédit, éducation, biométrie…) : 2 décembre 2027 (au lieu de 2 août 2026)
- **Annexe I** (IA dans produits réglementés CE) : 2 août 2028

🏢 Allègements PME <750 sal. / <150M€ CA

- Documentation technique simplifiée
- QMS proportionné à la taille
- Sanctions : montant le plus bas entre seuil absolu et % CA

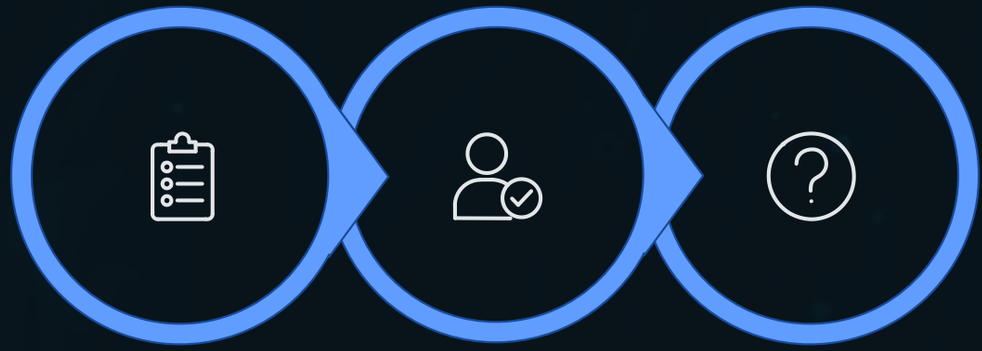
⚡ Ce qui reste en vigueur maintenant

- **Interdictions Art. 5** — depuis fév. 2025
- **Littératie Art. 4** — depuis fév. 2025
- **Obligations GPAI** — depuis août 2025
- **Transparence Art. 50** — août 2026 (nouveaux systèmes)

Savez-vous quelles obligations vous concernent aujourd'hui versus en 2027 ?

Par où commencer

Trois actes dans l'ordre — avant toute démarche de conformité



Inventaire Responsable Qualification

🗂️ 1. Inventaire

Listez chaque système IA actif : SaaS avec IA intégrée, API tierce, outil interne, modèle fine-tuné. Pour chacun : qui l'a déployé, qui l'utilise, pour quelles décisions. **Sans liste, rien d'autre n'est possible.**

👤 2. Responsable par système

Qui peut interrompre, corriger, documenter en cas d'incident ? Une personne nommée — pas une responsabilité collective diffuse.

❓ 3. Les trois questions

- Données personnelles ? → **RGPD**
- Décisions sur des personnes ? → **AI Act**
- Secteur réglementé ou produit ? → **NIS2 / DORA / CRA**

> Votre conformité RGPD couvre-t-elle vos nouvelles obligations IA ? Avez-vous identifié les obligations AI Act spécifiques à vos usages ? Savez-vous qui dans votre organisation répondrait en cas de contrôle ?