Complyla

GUIDE COMPLET Conformité EU AI Act pour les PME françaises

Tout ce que vous devez savoir pour préparer votre entreprise avant la deadline du **2 août 2026**.

35M€	86%	49%	2 août 2026
Amende maximale	Employés utilisent l'IA	IA non approuvée	Deadline critique

CE QUE VOUS TROUVEREZ DANS CE GUIDE :

Préparé par Complyla — complyla.com — contact@complyla.com
v1.0 — Mars 2026 — Prochaine mise à jour : septembre 2026

1. Comprendre l'EU AI Act en 5 minutes

L'EU AI Act (Règlement (UE) 2024/1689) est **le premier cadre réglementaire mondial sur l'intelligence artificielle**. Adopté en 2024, il s'applique à toute entreprise qui développe, déploie ou utilise des systèmes d'IA dans l'Union européenne — quelle que soit sa taille.

Si votre entreprise utilise ChatGPT, Microsoft Copilot, un chatbot, un outil de recrutement IA, ou n'importe quel logiciel intégrant de l'intelligence artificielle, **vous êtes concerné**.

Pourquoi les PME sont particulièrement exposées :

- La plupart n'ont aucun inventaire de leurs systèmes IA
- Les employés utilisent des outils IA sans approbation formelle (Shadow AI)
- Aucune politique d'utilisation de l'IA n'est en place
- Les solutions existantes coûtent 10 000 à 100 000€/an et ciblent les grands groupes

> **Les sanctions vont jusqu'à 35 millions d'euros ou 7% du chiffre d'affaires mondial annuel — pour les pratiques interdites.**

La bonne nouvelle : l'EU AI Act prévoit des mesures spécifiques pour les PME — frais réduits, accès aux sandboxes réglementaires, et templates simplifiés.

2. Les 4 niveaux de risque

L'EU AI Act classe les systèmes d'IA en **4 niveaux de risque**. C'est la classification qui détermine vos obligations.

Niveau	Exemples	Obligations	Amende
INTERDIT	Scoring social, manipulation comportementale, surveillance biométrique de masse	INTERDIT — ces systèmes ne peuvent pas être utilisés.	35M€ ou 7% CA
HAUT RISQUE	Recrutement IA, scoring crédit, évaluation éducative, IA médicale	Documentation technique, supervision humaine, évaluation des risques, registre EU	15M€ ou 3% CA
LIMITÉ	Chatbots, deepfakes, génération de contenu	Obligation de transparence : informer que c'est de l'IA	15M€ ou 3% CA
MINIMAL	Filtres anti-spam, IA jeux vidéo, autocorrection	Aucune obligation spécifique	—

> *La majorité des PME se situent en « risque limité » ou « minimal ». Mais l'utilisation d'outils de recrutement IA ou d'IA dans la santé peut vous faire basculer en « haut risque » sans le savoir.*

3. Les dates clés à connaître

Date	Ce qui entre en vigueur	Impact PME
2 février 2025 (EN VIGUEUR)	Pratiques interdites + obligation de littératie IA (Article 4)	IMMÉDIAT : sensibiliser vos équipes
2 août 2025 (EN VIGUEUR)	Règles GPAI (modèles IA à usage général)	Concerne les fournisseurs de modèles IA
2 août 2026 (CRITIQUE)	Obligations complètes pour systèmes haut risque (Annexe III)	MAJEUR : documentation, supervision, évaluation des risques, registre EU
2 août 2027	IA embarquée dans les produits réglementés	Concerne les fabricants de produits avec IA

> **La date critique pour les PME : 2 août 2026. Si vous n'avez pas commencé, il est urgent d'agir maintenant.**

4. Shadow AI : le risque invisible

Le Shadow AI est l'utilisation d'outils d'IA par les employés **sans l'approbation formelle de l'entreprise**. C'est le premier risque de conformité pour les PME.

86%	**49%**
des employés utilisent l'IA au travail chaque semaine	utilisent des outils IA non approuvés

Exemples concrets :

- Un commercial colle des données clients dans ChatGPT pour rédiger un email
- Le service RH utilise un outil de tri de CV avec de l'IA sans le déclarer
- Un développeur utilise GitHub Copilot sans que la DSI le sache
- Le marketing utilise MidJourney pour créer des visuels sans approbation
- Un manager utilise Notion AI pour résumer des comptes-rendus confidentiels

Le risque : chaque usage non documenté est un angle d'attaque en cas de contrôle.

La solution : un inventaire systématique de tous les outils IA — approuvés ou non.

5. AI Workplace : Copilot, Gemini, Notion AI

Microsoft Copilot, Google Gemini, Notion AI, Slack AI — ces outils sont déployés massivement dans les PME, souvent avec les licences existantes, **sans que personne ne définisse les limites d'accès**.

Le problème : ces IA accèdent à vos emails, fichiers, CRM, données RH, calendrier. Elles peuvent résumer des informations confidentielles sans restriction.

Action immédiate : pour chaque outil IA intégré, vérifiez (1) à quelles données il a accès, (2) qui peut l'utiliser, (3) quelles restrictions sont en place.

> *L'audit AI Workplace est un volet spécifique de nos accompagnements : analyse des permissions, accès aux données, et actions autorisées pour chaque outil IA intégré.*

6. Checklist conformité 90 jours

Un plan d'action concret pour préparer votre PME à l'EU AI Act en 90 jours.

Jours 1-30 : Découverte et inventaire

1. **Désigner un responsable conformité IA** — DPO, DSI, ou dirigeant.
2. **Inventorier TOUS les systèmes IA** — outils approuvés ET non approuvés.
3. **Classifier chaque système par niveau de risque** — inacceptable / haut / limité / minimal.
4. **Identifier les usages Shadow AI** — sondage interne anonyme.

Jours 31-60 : Documentation

5. **Rédiger le Registre des Systèmes IA** — document officiel.
6. **Rédiger la Politique d'Utilisation de l'IA** — règles internes.
7. **Rédiger le Guide de sensibilisation IA** — Article 4 + attestation de lecture.
8. **Évaluer les risques par système** — documentation, évaluation d'impact, mitigation.

Jours 61-90 : Formation et suivi

9. **Former les équipes** — distribuer le guide, faire signer l'attestation (Article 4).
10. **Mettre en place le monitoring** — vérification régulière des usages.
11. **Planifier la révision** — minimum une fois par an.

> *Pour un accompagnement personnalisé, Complyla propose un audit gratuit (10 min de questionnaire, rapport sous 5 jours). Voir chapitre 11.*

7. Les 7 règles d'or pour vos équipes

Le socle de votre politique de littératie IA (obligation Article 4, en vigueur depuis le 2 février 2025).

#	Règle	Pourquoi
1	Pas de données sensibles dans les outils IA externes	Données clients, RH, financières = interdit dans ChatGPT
2	Toujours vérifier les résultats de l'IA	L'IA « hallucine » : elle invente des faits avec confiance
3	Transparence sur l'usage IA dans les comm. externes	Chatbots identifiés. Contenu IA majoritaire = le mentionner
4	Utiliser uniquement les outils approuvés	Tout outil non référencé = interdit (Shadow AI)
5	Jamais de décision automatisée sans supervision humaine	Recrutement, scoring : l'humain décide, l'IA assiste
6	Signaler tout incident IA immédiatement	Résultat incorrect, biais, fuite = signaler au responsable
7	Vérifier les permissions de l'IA intégrée	Copilot, Gemini accèdent à tout. Vérifier et restreindre

> *Ces 7 règles sont détaillées dans le Guide de sensibilisation IA (Article 4) que Complyla fournit, avec attestation de lecture — preuve documentaire de conformité.*

8. Les documents indispensables

Document	Contenu	Obligatoire ?
Registre des Systèmes IA	Tous les systèmes IA, classification, statut de conformité	OUI (pour tous)
Politique d'Utilisation IA	Règles internes, outils autorisés/interdits, approbation	OUI (pour tous)
Guide Sensibilisation IA	Formation employés (Art. 4), 7 règles, attestation	OUI (Art. 4)
Évaluation Risques (FRIA)	Risques par système, mitigation, plan d'action	OUI (haut risque)
Doc. Technique (Annexe IV)	Specs techniques, données entraînement, métriques	OUI (fournisseurs)
Plan d'Action Priorisé	Actions, responsables, délais, suivi	RECOMMANDÉ

9. RGPD et EU AI Act

Si vous êtes déjà en conformité RGPD, vous avez une longueur d'avance.

Thème	RGPD	EU AI Act
Inventaire	Registre des traitements	Registre des systèmes IA
Évaluation	DPIA (données personnelles)	FRIA (droits fondamentaux)
Transparence	Informer sur le traitement des données	Informer sur l'utilisation de l'IA
Supervision	DPO (optionnel pour PME)	Responsable conformité IA
Documentation	Politique de confidentialité	Politique IA + doc technique
Sanctions	Jusqu'à 20M€ ou 4% CA	Jusqu'à 35M€ ou 7% CA

Conseil : si vous avez un DPO, impliquez-le dans la démarche EU AI Act.

10. FAQ

Mon entreprise a moins de 50 employés, suis-je concerné ?

Oui. L'EU AI Act s'applique quelle que soit la taille. Des mesures spécifiques existent pour les PME, mais les obligations de base s'appliquent.

On utilise juste ChatGPT et Copilot, est-ce concerné ?

Oui. ChatGPT est à risque limité (transparence). Copilot accède à vos données — il doit être inventorié et encadré.

Quelles sont les sanctions pour une PME ?

Proportionnelles à la taille. Plafonds réduits pour les PME, mais même une amende réduite peut être dévastatrice.

Dois-je embaucher un avocat spécialisé ?

Pas nécessairement. C'est une question opérationnelle : inventaire, politique, sensibilisation nécessitent de la rigueur, pas de l'expertise juridique.

Combien de temps pour se mettre en conformité ?

PME typique : 4 à 8 semaines pour un accompagnement complet. État des lieux rapide en 5 jours.

Les sandboxes réglementaires, c'est quoi ?

Des environnements de test supervisés par les régulateurs. PME = accès prioritaire et gratuit.

11. Vos prochaines étapes

3 actions concrètes à mener cette semaine :

1 Évaluez votre situation en 10 minutes

Questionnaire d'évaluation gratuit. Rapport personnalisé sous 5 jours.
tally.so/r/1AKrp4

2 Échangez avec un expert

Décrivez votre contexte par email - réponse personalisée sous 48 heures ouvrées.
contact@complyla.com

3 Commencez l'inventaire

Utilisez le template en annexe pour lister tous les outils IA utilisés dans votre entreprise.

À propos de Complyla

Accompagnement des PME européennes pour la conformité EU AI Act.
20 ans d'expérience en conformité aéronautique (EASA/FAA) — documentation, traçabilité, gestion des risques — appliqués à la gouvernance IA.

Nos accompagnements démarrent à **1 500€** pour un audit express.

complyla.com | contact@complyla.com

ANNEXE — Template d'inventaire IA

Utilisez ce tableau pour commencer votre inventaire. Listez chaque outil IA utilisé dans votre entreprise — y compris ceux qui ne sont pas formellement approuvés.

Outil IA	Département	Données traitées	Approuvé ?	Risque
Ex: ChatGPT	*Marketing*	*Textes, briefs*	*Non*	*Limité*
Ex: Copilot	*Tous*	*Emails, fichiers*	*Oui*	*Limité*
Ex: HireVue	*RH*	*Vidéos candidats*	*Oui*	***HAUT***

> *Le Registre complet (fourni par Complyla) contient des colonnes supplémentaires : base légale, mitigation, supervision humaine, score de conformité.*