Complyla

GUIDE COMPLET Conformité EU AI Act pour les PME françaises

Préparer votre entreprise à la conformité EU AI Act 2026-2027

35M€	86%	49%	2026-27
Amende maximale	Employés utilisent l'IA	IA non approuvée	Calendrier dual

Calendrier dual depuis l'accord Digital Omnibus du 7 mai 2026. Le texte AI Act 2024 reste juridiquement applicable jusqu'à publication au JOUE de l'accord politique (fin juillet 2026 attendue). Anticiper sur le texte en vigueur reste la posture professionnelle prudente. Le calendrier dual est détaillé section 3.

CE QUE VOUS TROUVEREZ DANS CE GUIDE

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

L'accord politique du Digital Omnibus du 7 mai 2026 a modifié le calendrier d'application de plusieurs obligations. Cet accord reste politique provisoire jusqu'à publication officielle au JOUE (fin juillet 2026 attendue). Le tableau ci-dessous présente les deux calendriers en vigueur.

Obligation	Texte 2024 (en vigueur)	Accord Omnibus 7/05/2026
Pratiques interdites (Article 5)	**2 février 2025 EN VIGUEUR**	Inchangé
Littératie IA (Article 4)	**2 février 2025 EN VIGUEUR**	Inchangé
GPAI (Articles 51-56)	**2 août 2025 EN VIGUEUR**	Inchangé
Annexe III haut risque (Article 26 et suiv.)	**2 août 2026**	**2 décembre 2027** (postponé)
Article 50(1) transparence chatbots	**2 août 2026**	Inchangé
Article 50(2) marquage machine-readable	**2 août 2026**	**2 décembre 2026** (compressé)
Annexe I IA embarquée produits réglementés	2 août 2027	2 août 2028 (postponé)

> **La posture professionnelle prudente.** L'accord politique du 7 mai 2026 reste provisoire jusqu'à publication officielle au JOUE. Jusque-là, le texte AI Act 2024 reste juridiquement applicable. Construire un programme de conformité sur le texte en vigueur plutôt que parier sur une simplification non encore adoptée reste la posture prudente. Les obligations Article 4 (littératie IA) et Article 5 (pratiques interdites) sont déjà en vigueur depuis février 2025.

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%

des employés utilisent l'IA au travail chaque semaine

49%

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 un générateur d'images IA pour créer des visuels sans approbation
- Un manager utilise un assistant IA 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 assistants IA intégrés aux suites bureautiques sont déployés massivement dans les PME, souvent avec les licences existantes Microsoft 365 ou Google Workspace, sans que personne ne définisse formellement les limites d'accès aux données.

Le problème : ces IA accèdent par défaut à vos emails, fichiers SharePoint ou Drive, données CRM, dossiers RH et calendrier. Elles peuvent résumer, indexer ou exposer des informations confidentielles sans restriction explicite. Contrairement au Shadow AI, ces outils sont déployés *avec* les permissions natives de l'utilisateur, ce qui étend automatiquement la surface d'exposition de vos données.

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.

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 (interdit / 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 initial. Questionnaire en 10 minutes, rapport sous 5 jours ouvrés. Voir chapitre 11.

7. Les 7 règles d'or pour vos équipes

L'Article 4 de l'EU AI Act exige que toute personne utilisant un système d'IA dans le cadre de son travail dispose d'un niveau suffisant de littératie IA. Cette obligation est en vigueur depuis le 2 février 2025 et concerne toutes les tailles d'entreprise. Les 7 règles ci-dessous constituent le socle minimum d'une politique de littératie IA opérationnelle pour vos équipes.

#	Règle	Pourquoi
1	Pas de données sensibles dans les outils IA externes	Données clients, RH, financières = interdit dans les outils IA externes
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 communications 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	Les assistants intégrés accèdent à tout. Vérifier et restreindre

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

Priorisation des documents. Pour une PME en démarrage, commencez par trois documents essentiels : le Registre des Systèmes IA (inventaire centralisé), la Politique d'Utilisation IA (règles internes), et le Guide de Sensibilisation IA (formation Article 4). Ces trois documents couvrent les obligations de base et constituent la fondation sur laquelle s'appuieront les évaluations de risques (FRIA) et la documentation technique au fur et à mesure de l'identification de systèmes haut risque dans votre périmètre.

9. RGPD et EU AI Act

Le RGPD (en vigueur depuis 2018) et l'EU AI Act (déploiement progressif 2025-2027) sont deux régimes réglementaires **distincts**, avec des champs d'application et des obligations propres. Si vous êtes déjà en conformité RGPD, vous avez une longueur d'avance méthodologique, mais les deux cadres doivent être traités séparément.

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, tout en gardant les deux conformités structurées séparément.

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 ?

Compter 4 à 8 semaines pour une démarche complète selon la taille. État des lieux rapide en 5 jours.

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 ouvrés.
tally.so/r/1AKrp4

2 **Échangez avec un expert**
Décrivez votre contexte par email, réponse personnalisée 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 retenir pour 2026-2027. Les obligations Article 4 (littératie IA) et Article 5 (pratiques interdites) sont en vigueur depuis février 2025. Les obligations Annexe III haut risque sont reportées au 2 décembre 2027 selon l'accord politique du 7 mai 2026, mais le texte AI Act 2024 reste juridiquement applicable jusqu'à publication officielle au JOUE. Construire la conformité sur le texte en vigueur reste la posture professionnelle prudente.

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, méthodologie appliquée à la gouvernance IA.

Les accompagnements démarrent à 1 500€ pour un audit express.

complyla.com | contact@complyla.com

A. 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: ATS de tri CV	RH	CV candidats	Oui	HAUT

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