BadgeIA · par Brozapi

AI Act : le guide du dirigeant de PME

Ce qui change, qui est concerné et les actions prioritaires pour les dirigeants de PME.

Auteur : Brozapi

Version : 1.0

Date du guide : 2026-08-19

PDF généré le 21/08/2026

Ce guide est fourni à titre indicatif et ne constitue pas un conseil juridique.

AI Act : le guide du dirigeant de PME

Ce guide a été rédigé par Brozapi pour accompagner les dirigeants de petites et moyennes entreprises dans la compréhension pratique du Règlement européen sur l'intelligence artificielle (AI Act). Il ne constitue pas un avis juridique.

Introduction

Depuis août 2024, l'Union européenne dispose d'un cadre réglementaire dédié à l'intelligence artificielle : le Règlement 2024/1689, communément appelé « AI Act ». Ce texte s'applique à toute entreprise qui met sur le marché européen un produit ou un service utilisant l'IA, quelle que soit sa taille ou son pays d'implantation.

Pour un dirigeant de PME, ce règlement peut sembler intimidant. Entre les classifications de risque, les obligations de documentation et les nouvelles responsabilités, il est difficile de savoir par où commencer sans y consacrer des semaines entières.

Le calendrier d'application est progressif : les systèmes à risque inacceptable sont déjà interdits depuis février 2025, les obligations de transparence s'appliquent depuis août 2025, et les exigences les plus strictes pour les systèmes à haut risque entreront en vigueur progressivement jusqu'en 2027. Cela signifie que vous avez encore du temps pour vous organiser, mais que plus vous attendez, plus la pression sera forte.

Ce guide a un objectif simple : vous donner une vision claire et actionnable de ce qui vous concerne réellement, et vous proposer un plan concret pour avancer sereinement.

---

1. Ce qui change vraiment pour une PME

Un changement de culture, pas une révolution technique

Le AI Act ne vous oblige pas à recruter une équipe de juristes ou à refondre vos outils informatiques du jour au lendemain. Ce qu'il demande, avant tout, c'est de la transparence et de la rigueur dans la manière dont vous utilisez ou vendez des systèmes d'IA.

Voici ce qui change concrètement :

Vous devez savoir ce que vous utilisez. Si votre entreprise intègre un outil d'IA — qu'il s'agisse d'un chatbot client, d'un moteur de recommandation ou d'un logiciel d'analyse de

candidatures — vous devez pouvoir identifier ce système, comprendre ses limites et documenter son usage.

Vous devez informer vos utilisateurs. Lorsqu'une personne interagit avec un système d'IA (par exemple un chatbot conversationnel), elle doit en être informée de manière claire. Ce n'est pas une contrainte technique lourde : un simple message informatif suffit.

Vous devez vérifier vos fournisseurs. Si vous achetez un logiciel contenant de l'IA à un éditeur, ce dernier a des obligations selon le règlement. En tant qu'utilisateur professionnel, vous devez vous assurer que vos fournisseurs respectent ces règles, notamment en réclamant la documentation technique.

Vous devez protéger les données d'entraînement. Si vous développez vous-même un modèle d'IA, vous devez respecter le droit d'auteur et la réglementation sur les données personnelles (RGPD) dans la constitution de vos jeux de données.

Quelques exemples concrets

Imaginons une PME de 30 salariés dans le secteur du recrutement qui utilise un outil de scoring automatique des CV. Ce système est classé à haut risque. Le dirigeant doit donc s'assurer que le fournisseur fournit une documentation complète, que les candidats sont informés de l'utilisation de l'IA, et qu'un recruteur humain valide chaque décision finale.

Prenons une agence marketing de 10 personnes qui utilise un générateur de texte pour rédiger des descriptions de produits. Ce système relève du risque limité. L'agence doit simplement indiquer clairement sur son site ou dans ses conditions générales qu'elle utilise l'IA, sans avoir besoin de documentation technique lourde.

Enfin, une boulangerie qui utilise un logiciel de comptabilité avec fonction de prévision des ventes basée sur l'IA. Si cette prévision ne déclenche aucune décision automatique vis-à-vis des clients ou des employés, l'outil relève probablement du risque minimal et ne nécessite aucune action spécifique liée à l'AI Act.

La conformité n'est pas un gouffre financier

Une idée reçue veut que le AI Act coûte une fortune aux PME. En réalité, pour la majorité des entreprises, la conformité passe par de la documentation, de la transparence et un peu d'organisation interne — des démarches qui ne nécessitent pas d'investissement technologique lourd. Les coûts deviennent significatifs uniquement pour les éditeurs de solutions à haut risque, qui doivent réaliser des évaluations de conformité approfondies.

Le règlement prévoit des sanctions pour les manquements graves, mais l'approche des autorités européennes est avant tout incitative et progressive. L'objectif affiché est de faire

monter en compétence l'écosystème, pas de sanctionner à tout va. Ce qui compte, c'est de démontrer que vous faites des efforts sérieux et documentés.

---

2. Suis-je concerné ?

Le test en 4 questions

Pour savoir si le AI Act s'applique à votre activité, posez-vous ces quatre questions :

1. **Mon entreprise met-elle sur le marché européen un système d'IA ?** Cela inclut : vendre un logiciel utilisant l'IA, proposer un service en ligne fondé sur l'IA, ou intégrer de l'IA dans un produit physique.

2. **Mon entreprise utilise-t-elle un système d'IA dans un contexte professionnel ?** Même si vous ne vendez pas d'IA, si vous utilisez un outil d'IA dans votre activité (recrutement, marketing, relation client, comptabilité), certaines obligations peuvent s'appliquer.

3. **Le système d'IA est-il utilisé dans un des domaines à haut risque listés par le règlement ?** Les domaines à haut risque incluent : gestion des ressources humaines (recrutement, évaluation), éducation, finance (scoring de crédit), justice, emploi, accès à des services publics essentiels, et certains usages dans les transports ou la santé.

4. **Mon entreprise est-elle implantée dans l'Union européenne ou cible-t-elle des résidents européens ?** Le règlement s'applique dès lors que le système est mis à disposition ou utilisé sur le marché européen.

Si vous répondez « oui » à la question 1 ou 2, et « oui » à la question 4, alors le AI Act vous concerne.

Les 4 niveaux de risque du AI Act

Le règlement classe les systèmes d'IA en quatre catégories :

Risque inacceptable (interdit) Certaines pratiques sont purement interdites : la notation sociale à l'échelle d'une population par les autorités publiques, la reconnaissance émotionnelle dans les lieux de travail ou les écoles (sauf exceptions médicales), la manipulation comportementale subliminale, ou l'exploitation des vulnérabilités de groupes spécifiques.

En pratique pour une PME : vous ne risquez pas d'utiliser ces systèmes dans le cours normal de votre activité. Si vous travaillez dans l'édition de logiciels, vérifiez simplement que vos produits ne tombent pas dans ces catégories.

Haut risque (obligations strictes) Les systèmes utilisés dans les domaines sensibles listés ci-dessus (recrutement, crédit, éducation, etc.) sont soumis à des exigences élevées : conformité technique, documentation, évaluation des risques, supervision humaine, traçabilité.

En pratique pour une PME : si vous utilisez un logiciel de recrutement automatisé ou un outil de scoring client, vous entrez probablement dans cette catégorie.

Risque limité (obligations de transparence) Les chatbots, les deepfakes, les systèmes de génération de contenu (texte, image, audio) doivent respecter des règles de transparence : informer l'utilisateur qu'il interagit avec l'IA, indiquer lorsqu'un contenu est généré artificiellement.

En pratique pour une PME : si vous utilisez un chatbot sur votre site web ou si vous publiez des images générées par IA, vous devez appliquer ces règles de transparence.

Risque minimal (aucune obligation spécifique)

Les systèmes d'IA à faible risque, comme les filtres anti-spam ou les recommandations de contenu non sensibles, ne sont soumis à aucune obligation spécifique au-delà des lois existantes.

En pratique pour une PME : la plupart des outils d'IA généralistes que vous utilisez au quotidien (assistants de rédaction, outils de traduction, correcteurs orthographiques) relèvent de cette catégorie. Toutefois, même pour ces outils, il est recommandé de garder une trace de leur usage dans votre inventaire interne, car la frontière entre « généraliste » et « spécifique » peut évoluer avec les mises à jour des outils.

Comment croiser AI Act et RGPD ?

Un point crucial souvent négligé : le AI Act ne remplace pas le RGPD, il le complète. Si vous traitez des données personnelles dans un système d'IA — ce qui est presque toujours le cas — vous devez respecter les deux réglementations simultanément. Le RGPD règle la protection des données ; le AI Act règle la sûreté et les droits fondamentaux liés à l'IA. La CNIL insiste d'ailleurs sur ce croisement dans ses recommandations.

Pour une PME, cela se traduit concrètement par : informer les personnes que leurs données sont utilisées par un système d'IA (RGPD), et respecter les obligations de transparence spécifiques au AI Act. Ces deux exigences se recouvrent souvent : une bonne politique de confidentialité bien rédigée peut couvrir les deux aspects.

3. Les 10 actions prioritaires

Voici un plan d'action progressif, classé par urgence. Vous n'avez pas besoin de tout faire en une semaine, mais chaque étape vous rapproche d'une posture conforme et rassurante.

Action 1 — Faire l'inventaire de vos systèmes d'IA

À faire immédiatement. Listez tous les outils, logiciels et services utilisant l'IA dans votre entreprise. Pour chacun, notez : le nom du fournisseur, la fonction métier (recrutement, marketing, etc.), et le type de technologie (chatbot, génération de texte, analyse prédictive, etc.).

Vérification : vous devez obtenir une liste documentée, même sous forme de tableau simple, reprenant chaque outil et son usage.

Action 2 — Identifier le niveau de risque de chaque système

À faire immédiatement. Pour chaque outil listé, déterminez s'il relève du risque minimal, limité, haut ou inacceptable. Référez-vous à la section 2 de ce guide. Quand vous avez un doute, classez-le une catégorie au-dessus par précaution.

Vérification : chaque outil de votre inventaire doit avoir une étiquette de risque associée.

Action 3 — Vérifier les informations de transparence sur vos outils publics

À faire dans les 30 jours. Si vous utilisez un chatbot sur votre site, une génération de contenu par IA, ou tout système interactif, assurez-vous que l'utilisateur est informé de manière visible qu'il interagit avec l'IA. Cela peut prendre la forme d'une mention en bas de page, d'un bandeau informatif, ou d'un message de bienvenue du chatbot.

Vérification : faites un test utilisateur anonyme — une personne étrangère à votre entreprise doit pouvoir identifier en moins de 10 secondes qu'elle interagit avec l'IA.

Action 4 — Réclamer la documentation technique à vos fournisseurs

À faire dans les 60 jours. Contactez chaque éditeur de logiciel d'IA utilisé dans votre entreprise pour obtenir : une déclaration de conformité, la documentation technique, et les conditions d'utilisation actualisées. Conservez ces documents dans un dossier dédié.

Vérification : vous devez posséder un document (PDF, email, ou lien) par fournisseur, attestant de ses obligations selon le AI Act.

Action 5 — Documenter votre propre usage interne de l'IA

À faire dans les 60 jours. Rédigez une note interne qui précise : quels outils d'IA sont utilisés, à quelles fins, quelles données sont traitées, qui en est responsable dans l'entreprise, et quelles sont les limites connues de ces outils.

Vérification : un nouvel employé arrivant dans votre entreprise doit pouvoir comprendre votre politique d'usage de l'IA en lisant ce document.

Action 6 — Mettre en place une supervision humaine sur les décisions sensibles

À faire dans les 90 jours. Si un outil d'IA participe à des décisions importantes (sélection de candidats, évaluation de dossiers, attribution de crédit), assurez-vous qu'une personne physique valide systématiquement la décision finale. L'IA peut recommander, mais elle ne doit pas décider seule dans ces cas.

Vérification : pour chaque processus à haut risque, identifiez le nom de la personne responsable de la validation humaine.

Action 7 — Vérifier la conformité RGPD de vos données d'IA

À faire dans les 90 jours. Si vous entraînez ou personnalisez un modèle d'IA avec vos propres données, vérifiez que vous disposez des bases légales nécessaires (consentement, intérêt légitime documenté, ou autre), que les droits des personnes sont respectés (accès, rectification, effacement), et que vous avez réalisé une analyse d'impact si vous traitez des données sensibles.

Vérification : votre registre des activités de traitement doit mentionner explicitement les traitements liés à l'IA.

Action 8 — Former votre équipe aux bases du AI Act

À faire dans les 90 jours. Organisez une session interne ou un partage de documentation pour sensibiliser vos collaborateurs. L'objectif n'est pas de former des experts, mais de faire comprendre à chacun : ce qu'est un système d'IA au sens du règlement, quelles sont les règles de transparence, et à qui s'adresser en cas de doute.

Vérification : rédigez un compte-rendu ou conservez une liste de présence attestant de la formation.

Action 9 — Prévoir un processus de veille réglementaire

À faire dans les 6 mois. Le AI Act évoluera au fil des années, avec des codes de conduite, des normes harmonisées et des jurisprudences. Désignez une personne (ou abonnez-vous à une newsletter spécialisée) pour suivre ces évolutions et alerter l'entreprise en cas de changement significatif.

Vérification : vous devez pouvoir nommer la personne ou la source responsable de cette veille.

Action 10 — Faire réaliser un audit externe si vous êtes à haut risque

À faire dans les 12 mois. Si votre activité repose largement sur des systèmes d'IA classés « haut risque » (par exemple, vous éditez un logiciel de recrutement automatisé), envisagez de faire auditer votre conformité par un cabinet spécialisé ou un organisme notifié. Cela n'est pas obligatoire pour tous les utilisateurs, mais c'est fortement recommandé pour les éditeurs de solutions.

Vérification : conservez le rapport d'audit, même s'il mentionne des points d'amélioration.

Questions fréquentes

Je n'ai que 5 salariés. Le AI Act s'applique-t-il vraiment à moi ? Oui, le règlement ne fait pas de distinction selon la taille de l'entreprise. Cela dit, si vous n'utilisez pas d'IA dans votre activité, ou si vous n'utilisez que des outils généralistes à faible risque (comme un correcteur orthographique), vos obligations seront quasi inexistantes. Le AI Act cible avant tout les usages sensibles, pas la taille de l'entreprise.

J'utilise ChatGPT pour rédiger des emails. Dois-je faire quelque chose ? Non, l'utilisation d'un assistant de rédaction généraliste dans un cadre interne relève du risque minimal. Par contre, si vous utilisez ce même outil pour générer du contenu publié sur votre site sans le mentionner, vous entrez dans le domaine du risque limité et devez appliquer les règles de transparence.

Mon fournisseur de logiciel est américain. Est-ce que le AI Act le concerne ? Oui, dès lors que le logiciel est mis à disposition sur le marché européen, le fournisseur est soumis au règlement. En tant qu'utilisateur, vous avez le droit — et l'intérêt — de lui réclamer la documentation de conformité. Si le fournisseur refuse ou ignore vos demandes, envisagez de changer de solution ou de documenter cette absence de réponse comme un risque identifié.

Puis-je me faire sanctionner si je ne fais rien ? Les sanctions prévues sont proportionnées au manquement. Une petite entreprise qui fait l'effort de documenter son inventaire,

d'informer ses utilisateurs et de solliciter ses fournisseurs sera considérée comme en démarche de conformité. À l'inverse, ignorer complètement le règlement alors que vous exploitez un système à haut risque expose l'entreprise à des mesures correctrices. L'approche est progressive, mais la mauvaise foi n'est pas tolérée.

Faut-il certifier chaque outil d'IA ? Non. Seuls les systèmes d'IA à haut risque doivent faire l'objet d'une évaluation de conformité approfondie, souvent via un organisme notifié. Pour les outils à risque limité ou minimal, la conformité repose sur l'auto-évaluation, la documentation interne et le respect des obligations de transparence.

---

4. Ressources et outils

Voici une sélection de ressources fiables pour approfondir chaque aspect du AI Act. Aucune de ces ressources ne coûte d'argent.

Textes officiels et portails européens

1. **Règlement européen sur l'intelligence artificielle (AI Act)** — EUR-Lex Le texte juridique complet, accessible gratuitement. La version consolidée permet de naviguer dans les articles. `https://eur-lex.europa.eu`

2. **Portail officiel de la Commission européenne sur l'IA** Présentation pédagogique du règlement, des calendriers d'application et des acteurs concernés. `https://digital-strategy.ec.europa.eu`

3. **European AI Office** Structure créée pour superviser la mise en œuvre du AI Act, publier des lignes directrices et accompagner les entreprises. `https://digital-strategy.ec.europa.eu/en/policies/ai-office`

4. **Shaping Europe's digital future** Hub de la Commission rassemblant les stratégies européennes sur l'IA, les données et la régulation numérique. `https://digital-strategy.ec.europa.eu/en`

Recommandations et guides nationaux

1. **CNIL — Intelligence artificielle** La Commission nationale de l'informatique et des libertés publie des recommandations sur l'IA et la protection des données, particulièrement utiles pour croiser AI Act et RGPD. `https://www.cnil.fr/fr/intelligence-artificielle`

2. **Guide de conformité RGPD pour les PME (CNIL)** Même si ce guide ne traite pas spécifiquement de l'IA, il est indispensable pour comprendre les bases légales des

données utilisées par les systèmes d'IA. `https://www.cnil.fr/fr/rgpd-passer-a-laction`

3. **France Num — Accompagnement numérique des TPE/PME** Programme d'État proposant des ressources et un accompagnement gratuit sur la transformation numérique, y compris l'adoption responsable de l'IA. `https://francenum.gouv.fr`

4. **Bpifrance — Hub Intelligence Artificielle** Ressources économiques et pratiques pour les entreprises françaises qui investissent dans l'IA. `https://www.bpifrance.fr`

Outils pratiques pour la mise en conformité

1. **BadgeIA (Brozapi)** Outil en ligne permettant de générer un badge de transparence pour votre site web ou votre application, indiquant clairement à vos visiteurs que vous utilisez l'IA. C'est une aide concrète pour respecter les obligations de transparence du AI Act. `https://badgeia.brozapi.com`

2. **EU AI Act Compliance Checker (Commission européenne)** Questionnaires et outils d'auto-évaluation mis à disposition par la Commission pour évaluer le niveau de conformité d'un système d'IA. Disponible via le portail digital-strategy.ec.europa.eu.

3. **Modèles de déclaration de conformité UE** La Commission met à disposition des modèles standardisés pour la déclaration de conformité des systèmes d'IA à haut risque. Disponibles via le European AI Office.

Réseaux et communautés

1. **France IA — Écosystème national** Cartographie et actualité de l'écosystème français de l'intelligence artificielle, avec des événements et des rencontres destinés aux entreprises. `https://franceia.org`

2. **European DIGITAL SME Alliance** Alliance européenne des PME du numérique, qui publie des analyses réglementaires et défend les intérêts des petites structures face aux grands acteurs. `https://digitalsme.eu`

Normes techniques

1. **CEN-CENELEC — Normes harmonisées sur l'IA** Les organismes de normalisation européens développent des standards techniques pour accompagner la mise en œuvre du AI Act. Leur portail permet de consulter les normes en cours de publication. `https://www.cencenelec.eu`

2. **ISO/IEC 42001 — Systèmes de management de l'IA** Norme internationale dédiée à la gouvernance de l'IA dans les organisations. Utile pour structurer une démarche de

conformité sur le long terme. Informations disponibles via les organismes de normalisation nationaux (AFNOR en France).

---

5. Ce que ce guide ne couvre pas (mention honnête)

Il est important de poser les limites de ce document pour ne pas vous induire en erreur.

Ce guide ne remplace pas un conseil juridique. Le AI Act est un texte de plus de 400 articles, avec des déclinaisons sectorielles et des interprétations qui évolueront. Si votre activité repose de manière centrale sur des systèmes d'IA à haut risque, consultez un avocat ou un cabinet spécialisé en propriété intellectuelle et droit du numérique.

Ce guide ne garantit pas votre conformité. Suivre les dix actions proposées vous met dans une posture sérieuse et documentée, mais elle ne constitue pas une certification officielle. Seuls les organismes notifiés ou les autorités compétentes peuvent attester de la conformité d'un système d'IA à haut risque.

Ce guide ne traite pas des sanctions en détail. Le règlement prévoit des amendes importantes pour les manquements graves, mais leur application dépendra de la transposition et de la pratique des autorités nationales. L'objectif de ce document est de vous aider à avancer sereinement, pas de vous alarmer avec des chiffres hors contexte.

Ce guide évoluera. La réglementation sur l'IA est jeune. Nous mettrons ce guide à jour régulièrement pour refléter les évolutions législatives, les nouvelles lignes directrices et les retours d'expérience des entreprises.

Checklist d'actions vérifiables

Utilisez cette checklist pour suivre votre avancement. Cochez chaque case quand l'action est réalisée et documentée.

- [ ] **Inventaire** — J'ai listé tous les outils d'IA utilisés dans mon entreprise.
- [ ] **Risque** — J'ai identifié le niveau de risque (minimal, limité, haut, inacceptable) pour chaque outil.
- [ ] **Transparence publique** — Mes outils interactifs (chatbots, générateurs de contenu) informent l'utilisateur qu'ils utilisent l'IA.
- [ ] **Documentation fournisseurs** — J'ai récupéré et archivé la documentation technique/conformité de chaque éditeur.

- [ ] **Politique interne** — J’ai rédigé une note interne sur l’usage de l’IA dans mon entreprise.
- [ ] **Supervision humaine** — Les décisions sensibles prises avec l’aide d’un outil d’IA sont systématiquement validées par une personne.
- [ ] **RGPD** — J’ai vérifié que les données utilisées pour l’IA respectent le RGPD (base légale, droits des personnes, registre des traitements).
- [ ] **Formation** — J’ai sensibilisé mon équipe aux bases du AI Act et de la transparence.
- [ ] **Veille** — J’ai désigné une personne ou une source responsable du suivi des évolutions réglementaires.
- [ ] **Audit (si haut risque)** — J’ai envisagé ou réalisé un audit externe si mon activité repose sur des systèmes à haut risque.

Guide rédigé par Brozapi — Version 1.0 — Août 2026 Pour toute question ou suggestion d’amélioration : contact@brozapi.com

—

Brozapi, 2026. Ce document est fourni à titre indicatif. Il ne constitue pas un conseil juridique ni une garantie de conformité.