AI Act : le compte à rebours opérationnel de l'intelligence artificielle en entreprise

Objet. Comprendre ce que l'AI Act change concrètement pour les organisations qui conçoivent, achètent, intègrent ou utilisent des systèmes d'IA. Distinguer les obligations déjà applicables, les échéances à venir et les actions à engager pour préparer la transparence du 2 août 2026.

Par Stéphane Nachez*, Président d'IntelligenceArtificielle.com*

NOTE DE RÉFÉRENCE N°002 23 JUIN 2026 RÉF. IA·2026·002

VERSION & MISES À JOUR

Note de référence – version 1.0 – 23 juin 2026. Cette note est mise à jour au fil de l'application du règlement, de la publication des lignes directrices, des normes harmonisées, des actes d'exécution et des clarifications apportées par la Commission européenne, le Bureau européen de l'IA (*AI Office*), les autorités nationales et les juridictions compétentes.

État législatif au 23 juin 2026. Le calendrier des systèmes à haut risque est réaménagé par le règlement de simplification dit « Digital Omnibus ». Après l'accord en trilogue du 7 mai 2026, le Parlement européen a donné son approbation finale au texte le 16 juin 2026 (423 voix pour, 57 contre, 174 abstentions) ; celui-ci est en cours d'adoption formelle par le Conseil et n'a pas encore été publié au *Journal officiel de l'Union européenne*. Les nouvelles échéances — 2 décembre 2027 et 2 août 2028 — ne deviendront pleinement opposables qu'à cette publication, attendue avant le 2 août 2026 ; jusque-là, les échéances initiales du règlement demeurent la référence.

Résumé exécutif

L'AI Act n'est plus une perspective réglementaire : il est entré dans sa phase d'application. Le règlement (UE) 2024/1689 sur l'intelligence artificielle est entré en vigueur le 1er août 2024 et s'applique progressivement depuis. Il concerne les acteurs publics et privés, dans l'Union européenne ou hors UE, dès lors qu'ils mettent sur le marché, mettent en service ou utilisent des systèmes d'IA dans l'Union (art. 2).

La première erreur consiste à croire que « tout commence » en août 2026. C'est faux. Les interdictions visant certaines pratiques d'IA et l'obligation de culture IA sont applicables depuis le 2 février 2025. Les règles de gouvernance et les obligations relatives aux modèles d'IA à usage général le sont depuis le 2 août 2025. Le 2 août 2026 reste une échéance majeure, notamment pour les obligations de transparence (art. 50) : chatbots, interactions avec des systèmes d'IA, marquage des contenus générés ou manipulés, hypertrucages (*deepfakes*) et certains textes publiés sur des sujets d'intérêt public.

La seconde erreur consiste à réduire l'AI Act à un sujet juridique. Pour les entreprises, le règlement devient surtout un sujet de gouvernance opérationnelle : savoir quels systèmes d'IA sont utilisés, par qui, dans quel contexte, avec quelles données, pour quelles décisions, sous quelle supervision humaine, avec quelles informations données aux personnes concernées et quelles preuves conservées.

La troisième erreur consiste à se croire à l'abri parce que le « haut risque » a été repoussé. Le Digital Omnibus réaménage l'entrée en application des règles sur les systèmes à haut risque, désormais fixée à des dates *fermes* (2 décembre 2027 et 2 août 2028). Mais ce report ne touche ni aux interdictions de février 2025, ni aux obligations sur les modèles d'IA à usage général d'août 2025, ni aux obligations de transparence d'août 2026. Il ne suspend donc rien de ce qui s'applique déjà ou s'appliquera cet été. Les entreprises doivent dès

maintenant cartographier leurs usages, qualifier les risques, revoir leurs contrats fournisseurs, former les équipes concernées et préparer leur transparence.

Le risque immédiat n'est pas seulement l'amende. Les sanctions peuvent atteindre jusqu'à 35 millions d'euros ou 7 % du chiffre d'affaires annuel mondial pour les pratiques interdites (art. 99 §3) ; jusqu'à 15 millions d'euros ou 3 % pour la plupart des autres manquements (art. 99 §4) ; et jusqu'à 7,5 millions d'euros ou 1 % pour la fourniture d'informations incorrectes, incomplètes ou trompeuses aux autorités (art. 99 §5). Mais le risque le plus probable à court terme est plus diffus : appel d'offres perdu, fournisseur non documenté, chatbot mal signalé, outil RH sensible mal gouverné, impossibilité de prouver qu'une décision assistée par IA reste supervisée par un humain.

Recommandation cardinale. Ne pas attendre une conformité parfaite. Mettre en place un registre des usages IA, classer les usages par niveau de risque, traiter immédiatement les cas critiques, préparer la transparence du 2 août 2026, et constituer un dossier de preuve minimal pour les usages sensibles.

---

1. Pourquoi cette note

Depuis l'adoption de l'AI Act, une grande partie de la couverture du sujet reste dominée par les cabinets d'avocats, les départements conformité et les commentaires article par article. Cette approche est nécessaire, mais insuffisante pour les décideurs.

Un dirigeant, un DSI, un DRH, un responsable marketing, un directeur produit ou un responsable achats n'a pas seulement besoin de savoir ce que dit le règlement. Il doit savoir quoi faire lundi matin.

Cette note prolonge, sur le terrain réglementaire, la première note de la série, consacrée aux dépendances technologiques de l'IA : là où la souveraineté pose la question du *« qui peut nous débrancher ? »*, la conformité pose celle du *« savons-nous ce que nous faisons tourner, où, pour quoi faire, et pouvons-nous le prouver ? »*.

L'AI Act impose en effet un changement de perspective. Il ne s'agit plus seulement de demander : « Sommes-nous conformes ? » Il faut désormais demander :

> *Avons-nous la maîtrise opérationnelle de nos usages d'IA ?*

Cette question recouvre des réalités très concrètes :

- les outils d'IA officiellement déployés ;
- les copilotes intégrés aux suites bureautiques ;
- les fonctionnalités IA activées dans les logiciels SaaS ;
- les outils RH de tri, d'évaluation ou de *matching* ;
- les chatbots clients ou internes ;
- les générateurs de textes, d'images, de vidéos et de voix ;
- les agents connectés aux données de l'entreprise ;
- les API de modèles utilisées dans les produits ;
- les prestataires qui utilisent de l'IA dans leurs livrables ;
- les modèles open source ou *open weights* hébergés en interne.

L'enjeu n'est pas d'interdire ces usages. Il est de savoir les identifier, les classer, les expliquer, les superviser et les documenter.

2. Ce que l'AI Act change vraiment

L'AI Act repose sur une logique de risque. Le règlement distingue quatre niveaux : les risques **inacceptables** (pratiques interdites, art. 5), les systèmes à **haut risque** (art. 6 et annexe III), les risques liés à la **transparence** (art. 50), et les systèmes à **risque minimal** ou nul. Les pratiques jugées inacceptables sont interdites ; les systèmes à haut risque sont soumis à des exigences strictes ; certains systèmes ou contenus doivent respecter des obligations de transparence ; la majorité des systèmes à risque minimal ne fait pas l'objet d'obligations spécifiques nouvelles au titre du règlement.

Ce modèle est souvent présenté de manière théorique. Mais pour les entreprises, il produit une conséquence très pratique : un même outil peut relever d'obligations très différentes selon son usage réel.

Un modèle de langage utilisé pour reformuler des textes marketing n'a pas le même profil de risque qu'un outil utilisé pour filtrer des candidatures, orienter des élèves, évaluer un salarié, décider d'un accès au crédit, analyser un comportement dans un espace public ou assister une décision médicale.

Ce n'est donc pas le modèle qui détermine le risque, mais ce que l'entreprise en fait : la question centrale est l'usage — les personnes concernées et les effets produits — et non la seule technologie.

Pour situer un usage concret, quelques questions suffisent à orienter sa qualification :

- le système interagit-il directement avec des personnes (chatbot, agent) ?
- génère-t-il ou manipule-t-il du texte, de l'image, de l'audio ou de la vidéo ?
- est-il employé en RH, recrutement, éducation, crédit, assurance, santé, sécurité ou service public ?
- prend-il, oriente-t-il ou influence-t-il une décision concernant une personne ?
- est-il intégré dans un produit soumis à une réglementation de sécurité ?
- l'entreprise agit-elle comme fournisseur, intégrateur, distributeur ou simple déployeur ?
- repose-t-il sur un modèle d'IA à usage général tiers, ou sur un modèle entraîné en interne ?

Une réponse positive aux deux premières questions oriente vers les obligations de transparence ; aux questions sur les domaines sensibles et les décisions, vers le haut risque ; les deux dernières déterminent la part d'obligations « fournisseur » que l'entreprise endosse.

3. Le calendrier consolidé de l'AI Act

Le calendrier de l'AI Act est progressif. Il résulte de la combinaison de l'article 113 du règlement et du réaménagement opéré, pour le haut risque, par le Digital Omnibus. La date du 2 août 2026 est essentielle, mais elle ne résume pas le règlement.

DATE	CE QUI S'APPLIQUE OU DEVIENT CENTRAL	CE QUE LES DÉCIDEURS DOIVENT RETENIR
1er août 2024	Entrée en vigueur du règlement (UE) 2024/1689.	Le compte à rebours a commencé. Le texte est adopté et directement applicable selon son calendrier progressif.
2 février 2025	Application des interdictions (art. 5), des définitions et de l'obligation de culture IA (art. 4).	Les organisations doivent déjà former les personnes qui utilisent ou supervisent des systèmes d'IA et bannir les pratiques interdites.

DATE	CE QUI S'APPLIQUE OU DEVIENT CENTRAL	CE QUE LES DÉCIDEURS DOIVENT RETENIR
2 août 2025	Application des règles de gouvernance et des obligations relatives aux modèles d'IA à usage général (chap. V) ; désignation des autorités nationales.	Les fournisseurs de modèles généralistes sont directement concernés ; les entreprises utilisatrices doivent suivre ce que leurs fournisseurs documentent.
2 août 2026	Entrée en application générale : obligations de transparence (art. 50), supervision pleine des modèles GPAI, début du pouvoir de sanction de la Commission sur les GPAI.	Chatbots, *deepfakes*, contenus générés ou manipulés, interactions avec des systèmes IA : les entreprises doivent être prêtes.
2 décembre 2027	Application des règles sur les systèmes à haut risque de l'annexe III (biométrie, infrastructures critiques, éducation, emploi, services essentiels, répression, migration, asile et contrôle aux frontières, justice), après réaménagement par le Digital Omnibus.	Le haut risque ne disparaît pas : son calendrier est repoussé à une date désormais fixe.
2 août 2028	Application des règles sur les systèmes à haut risque intégrés à des produits réglementés (annexe I : machines, jouets, ascenseurs, dispositifs médicaux…).	Les industriels et fabricants de produits réglementés doivent raisonner cycle de vie, conformité produit et documentation technique.

Le réaménagement du haut risque (Digital Omnibus). Dans sa version initiale, le règlement fixait l'application des systèmes à haut risque de l'annexe III au 2 août 2026 et celle des systèmes intégrés à des produits (annexe I) au 2 août 2027. La Commission a proposé le 19 novembre 2025 un paquet de simplification, le « Digital Omnibus », qui repousse ces échéances. Le point essentiel pour un décideur : les co-législateurs ont retenu des **dates fixes** — 2 décembre 2027 et 2 août 2028 — et non un déclenchement conditionné à la disponibilité des normes, comme l'envisageait d'abord la Commission. Le report est justifié par le retard des normes harmonisées, mais il n'y est plus juridiquement subordonné.

Statut au 23 juin 2026. Le Parlement européen a donné son approbation finale au texte le 16 juin 2026 ; celui-ci est en cours d'adoption formelle par le Conseil et n'a pas encore été publié au *Journal officiel*. Tant que cette publication n'est pas intervenue — attendue avant le 2 août 2026 —, les échéances initiales restent formellement la référence, d'où l'intérêt de préparer la conformité sans attendre la confirmation des nouvelles dates. Le même paquet introduit deux précisions utiles : un délai de grâce jusqu'au 2 décembre 2026 pour le marquage des contenus (art. 50 §2) des systèmes déjà sur le marché avant le 2 août 2026, et une nouvelle interdiction visant les applications de « déshabillage » et autres outils générant des images intimes non consenties ou des contenus pédocriminels.

4. Le champ d'application : qui est concerné ?

L'AI Act concerne les acteurs publics et privés qui placent un système d'IA ou un modèle d'IA à usage général sur le marché européen, qui mettent un système en service ou qui l'utilisent dans l'Union européenne. Par son article 2, il peut donc s'appliquer à des entreprises établies hors de l'Union dès lors que la sortie produite par le système est utilisée dans l'Union.

Le règlement distingue plusieurs rôles, dont les plus importants pour les entreprises sont :

Le fournisseur (art. 3, §3) : celui qui développe ou fait développer un système d'IA et le met sur le marché ou le met en service sous son nom ou sa marque. Exemple simple : un éditeur qui développe un outil de tri de CV.

Le déployeur (art. 3, §4) : celui qui utilise un système d'IA sous son autorité, dans un cadre professionnel. Exemple simple : une banque ou une entreprise qui utilise un outil de tri de CV fourni par un éditeur.

Le fournisseur de modèle d'IA à usage général : celui qui fournit un modèle capable d'être utilisé pour de nombreuses tâches, par exemple un grand modèle génératif.

Le producteur, l'importateur ou le distributeur : acteurs de la chaîne qui peuvent être concernés lorsqu'un système d'IA est intégré dans un produit ou distribué sur le marché européen.

Cette distinction est essentielle. Beaucoup d'entreprises pensent n'être que de simples utilisatrices. Mais elles peuvent endosser le rôle de fournisseur lorsqu'elles modifient substantiellement un système, l'intègrent dans un produit, le commercialisent sous leur marque ou l'utilisent dans un contexte différent de celui prévu initialement (art. 25). La Commission rappelle notamment que l'évaluation de conformité doit être répétée si le système ou sa finalité est substantiellement modifié.

---

5. Les obligations déjà applicables depuis février 2025

5.1 Les pratiques interdites (art. 5)

Depuis le 2 février 2025, l'article 5 interdit huit catégories de pratiques. La Commission y range notamment la manipulation nocive (techniques subliminales ou trompeuses), l'exploitation de vulnérabilités liées à l'âge, au handicap ou à une situation sociale ou économique, le *scoring* social, la prédiction du risque qu'un individu commette une infraction pénale lorsqu'elle repose **uniquement sur le profilage**, le moissonnage non ciblé d'images faciales pour constituer ou étendre des bases de reconnaissance faciale, la reconnaissance des émotions au travail et dans l'éducation, certaines catégorisations biométriques visant à déduire des caractéristiques protégées, ainsi que l'identification biométrique à distance en temps réel dans des espaces publics à des fins répressives, sous réserve d'exceptions strictes.

Deux nuances sont juridiquement déterminantes et trop souvent omises : la prédiction d'infraction n'est interdite que si elle se fonde *seulement* sur le profilage ou des traits de personnalité (elle reste possible en appui d'une appréciation humaine fondée sur des faits objectifs et vérifiables) ; et la reconnaissance des émotions est interdite au travail et dans l'éducation *sauf* pour raisons médicales ou de sécurité.

Pour une entreprise, les signaux d'alerte restent clairs :

- outil prétendant détecter l'état émotionnel d'un salarié, candidat ou élève ;
- solution de *scoring* comportemental opaque ;
- outil biométrique déployé sans analyse approfondie ;
- système de surveillance automatisée des travailleurs ;
- système exploitant des vulnérabilités liées à l'âge, au handicap, à la situation sociale ou économique ;
- solution présentée comme « prédictive » dans un contexte pénal, disciplinaire ou de sécurité.

Les lignes directrices de la Commission sur les pratiques interdites (réf. C(2025) 5052 final, dont le contenu a été approuvé le 4 février 2025 et la version formelle datée du 29 juillet 2025) sont non contraignantes : elles donnent des explications juridiques et des exemples pratiques, mais l'interprétation définitive appartient à la Cour de justice de l'Union européenne.

5.2 L'obligation de culture IA (art. 4)

L'article 4 de l'AI Act impose aux fournisseurs et déployeurs de systèmes d'IA de garantir, dans la mesure du possible, un niveau suffisant de culture IA pour leur personnel et les autres personnes qui utilisent ou supervisent ces systèmes pour leur compte. Cette obligation tient compte des connaissances techniques, de

l'expérience, de l'éducation et de la formation, du contexte d'usage et des personnes concernées par les systèmes.

Une formulation que le Digital Omnibus devrait alléger. Le texte de simplification transforme l'obligation de « garantir » un niveau suffisant en une obligation de « prendre des mesures destinées à soutenir le développement » de la culture IA — une obligation de moyens, qui ne requiert pas de garantir un niveau déterminé pour chaque individu. Cette évolution n'est pas encore en vigueur : tant qu'elle n'est pas publiée au *Journal officiel*, l'article 4 s'applique dans sa rédaction initiale, en vigueur depuis le 2 février 2025. En pratique, l'enjeu reste identique.

Car il ne suffit pas d'organiser une formation générale « découverte de l'IA » : une formation utile doit être adaptée aux usages. Un service marketing qui utilise des générateurs de contenus n'a pas les mêmes besoins qu'une équipe RH qui utilise un outil de *matching*, qu'un développeur qui intègre une API de modèle, qu'un juriste qui audite des contrats fournisseurs ou qu'un manager qui supervise une décision assistée par IA.

Le Bureau européen de l'IA tient un **répertoire vivant** des pratiques de culture IA (plus de quarante initiatives recensées), mais précise expressément que la reproduction de ces pratiques ne confère *aucune* présomption de conformité à l'article 4.

---

6. Les modèles d'IA à usage général : l'autre front de conformité

Les modèles d'IA à usage général, ou *GPAI models*, peuvent être utilisés pour de nombreuses tâches et intégrés dans de nombreux systèmes. Leurs fournisseurs doivent (art. 53) tenir une documentation technique, fournir des informations aux acteurs en aval qui intègrent le modèle, mettre en place une politique de respect du droit d'auteur de l'Union, et publier un résumé suffisamment détaillé des contenus utilisés pour l'entraînement, selon un modèle fourni par le Bureau de l'IA (publié le 24 juillet 2025). Les obligations de documentation comportent une exemption partielle pour les modèles publiés en open source ; la politique de droit d'auteur et le résumé d'entraînement, eux, s'imposent à tous.

Les modèles les plus avancés peuvent être qualifiés comme présentant un **risque systémique** (art. 51), avec des obligations renforcées (art. 55) : évaluation du modèle, y compris des tests contradictoires (*adversarial testing*), évaluation et atténuation des risques systémiques, signalement des incidents graves au Bureau de l'IA, et cybersécurité. Deux seuils techniques, à ne pas confondre, structurent ce régime : un modèle est *indicativement* regardé comme « à usage général » au-delà de 10^{23} opérations en virgule flottante (FLOP) d'entraînement (lignes directrices sur le champ des obligations GPAI, C(2025) 5045 final du 18 juillet 2025) ; il est *présumé* à risque systémique au-delà de 10^{25} FLOP (art. 51 §2), présomption réfragable et susceptible d'être ajustée par la Commission.

Un calendrier propre aux modèles GPAI. Les obligations s'appliquent depuis le 2 août 2025, mais avec deux nuances utiles à un acheteur. Les modèles déjà mis sur le marché avant cette date disposent d'un délai pour s'y conformer jusqu'au 2 août 2027 (art. 111 §3) ; et le pouvoir de la Commission de sanctionner les fournisseurs de modèles (art. 101) ne s'ouvre que le 2 août 2026. Conséquence concrète : dans l'intervalle, un fournisseur peut ne mettre à disposition qu'une documentation provisoire ou incomplète — un point à vérifier explicitement, plutôt qu'à présumer conforme.

La Commission a publié le 10 juillet 2025 un **Code de bonnes pratiques GPAI**, élaboré par des experts indépendants et facilité par le Bureau de l'IA, puis reconnu « outil volontaire adéquat » par un avis de la Commission du 1er août 2025. Il comporte trois chapitres : transparence, droit d'auteur, sûreté et sécurité. Les

chapitres transparence et droit d'auteur concernent l'ensemble des fournisseurs de modèles à usage général ; le chapitre sûreté et sécurité ne vise que les fournisseurs des modèles à risque systémique (art. 55).

Pour les entreprises utilisatrices, cette partie de l'AI Act ne doit pas être lue comme un sujet réservé aux grands laboratoires. Même non fournisseur de modèle, une entreprise doit interroger ses propres dépendances :

- le modèle utilisé est-il documenté ?
- le fournisseur a-t-il signé le Code de bonnes pratiques ?
- quelles garanties sont fournies sur les données d'entraînement ?
- les données client servent-elles à l'amélioration du modèle ?
- les sorties du modèle sont-elles marquées ou détectables ?
- le modèle peut-il être modifié, remplacé ou retiré sans préavis ?
- quelles informations sont disponibles pour intégrer ce modèle dans un système conforme ?

À la mi-2026, la liste officielle des signataires du Code (mise à jour le 23 avril 2026) compte une vingtaine de signataires complets — adhérant à l'ensemble des chapitres — dont Amazon, Anthropic, Google, IBM, Microsoft, OpenAI, ainsi que les européens Mistral AI et Aleph Alpha ; xAI n'a adhéré qu'au seul chapitre sûreté et sécurité. Deux absences sont stratégiquement significatives : **Meta**, qui a publiquement refusé de signer, et les principaux laboratoires chinois (Alibaba, Baidu, DeepSeek), absents de la liste. La signature du Code n'est pas obligatoire, mais elle est devenue, pour les acheteurs, un signal de documentation et de coopération.

---

7. Août 2026 : la grande échéance de la transparence

Le 2 août 2026 est la date clé des obligations de transparence (art. 50). À compter de cette échéance :

- les personnes doivent être informées lorsqu'elles interagissent avec un système d'IA — par exemple un chatbot — sauf si cela est manifestement évident (art. 50 §1) ;
- les fournisseurs de systèmes génératifs doivent marquer leurs sorties (audio, image, vidéo, texte) dans un format lisible par machine et détectable comme généré ou manipulé par IA, « dans la mesure où cela est techniquement possible » (art. 50 §2) ;
- les déployeurs de systèmes de reconnaissance des émotions ou de catégorisation biométrique doivent informer les personnes exposées (art. 50 §3) ;
- les déployeurs doivent divulguer les *deepfakes*, ainsi que les textes générés ou manipulés par IA publiés pour informer le public sur des sujets d'intérêt public (art. 50 §4).

Le règlement prévoit des exceptions à connaître : l'information n'est pas due lorsqu'elle est évidente ; le marquage ne s'impose pas aux fonctions purement assistives d'édition qui n'altèrent pas substantiellement le contenu ; les œuvres manifestement artistiques, satiriques ou de fiction bénéficient d'une divulgation allégée ; et le texte d'intérêt public échappe à l'obligation lorsqu'il a fait l'objet d'une **revue éditoriale humaine**, une personne assumant la responsabilité de sa publication. Les divulgations doivent être faites au plus tard lors de la première interaction ou exposition (art. 50 §5).

Pour aider à la mise en œuvre, le Bureau de l'IA a facilité, sur le fondement de l'article 50 §7, un **Code de bonnes pratiques sur la transparence des contenus générés par IA**, dont la version finale a été publiée le 10 juin 2026 (les projets, fin 2025 et début 2026, étaient intitulés « marquage et étiquetage »). Volontaire, il recommande deux mécanismes de marquage — des métadonnées signées (standard C2PA) et le filigranage

imperceptible — et fixe une échéance d'interopérabilité des outils de détection au 2 février 2027 ; la fenêtre pour figurer parmi les signataires initiaux court jusqu'au 22 juillet 2026. En parallèle, la Commission a soumis à consultation, du 8 mai au 3 juin 2026, un projet de lignes directrices sur l'article 50, dont la version définitive est attendue avant le 2 août 2026. À noter : le délai de grâce du 2 décembre 2026 évoqué plus haut ne concerne que le marquage (art. 50 §2) de systèmes déjà sur le marché ; il ne constitue pas un report général de l'article 50.

Pour les entreprises, cette échéance concerne notamment :

- les chatbots de support client ;
- les assistants RH internes ;
- les agents conversationnels commerciaux ;
- les avatars vidéo ;
- les voix synthétiques ;
- les images générées pour communication ou publicité ;
- les contenus texte publiés sur des sujets d'intérêt public ;
- les systèmes de génération automatique de réponses ;
- les outils de résumé ou de reformulation exposés à des tiers ;
- les plateformes SaaS qui intègrent des fonctionnalités IA sans signalement explicite.

La question opérationnelle à poser est simple :

> *Une personne peut-elle raisonnablement croire qu'elle interagit avec un humain, ou qu'un contenu est d'origine humaine, alors qu'il est généré ou manipulé par IA ?*

Si oui, il faut analyser l'obligation de transparence.

---

8. Les systèmes à haut risque : l'échéance recule, pas la préparation

Un système est à haut risque selon deux voies (art. 6) : soit il constitue un composant de sécurité d'un produit déjà réglementé, ou est lui-même un tel produit (annexe I : machines, jouets, ascenseurs, dispositifs médicaux…) ; soit il relève d'un des usages listés à l'**annexe III** : biométrie, infrastructures critiques, éducation, emploi et gestion des travailleurs, accès aux services essentiels (dont le crédit et l'assurance santé ou vie), répression, migration, asile et contrôle aux frontières, administration de la justice et processus démocratiques.

Les **fournisseurs** de systèmes à haut risque doivent notamment mettre en place un système de gestion des risques (art. 9), une gouvernance des données (art. 10), une documentation technique (art. 11), une journalisation (art. 12), une transparence vis-à-vis du déployeur (art. 13), une supervision humaine (art. 14), des garanties d'exactitude, de robustesse et de cybersécurité (art. 15), un système de gestion de la qualité (art. 17) et une évaluation de conformité (art. 43).

Les **déployeurs** doivent utiliser le système conformément à la notice, surveiller son fonctionnement, réagir aux risques et incidents, désigner une supervision humaine suffisamment équipée, veiller à la pertinence des données d'entrée qu'ils fournissent, et, dans certains cas, informer les salariés, les représentants du personnel ou les personnes concernées (art. 26). Certains déployeurs (organismes publics, services essentiels) doivent en outre conduire une analyse d'impact sur les droits fondamentaux (art. 27). Le règlement consacre enfin un droit à l'explication des décisions individuelles lorsque la sortie d'un système à haut risque a servi à prendre une décision produisant des effets juridiques ou significatifs sur une personne (art. 86).

Comme indiqué au §3, le Digital Omnibus réaménage le calendrier : application au 2 décembre 2027 pour les usages de l'annexe III, au 2 août 2028 pour les systèmes intégrés à des produits réglementés. Ces dates sont fixes, et non conditionnées à la disponibilité des normes. Ce report ne traduit aucune baisse du niveau d'exigence : il déplace l'effort vers la préparation — documentation, gestion des risques, évaluation de conformité, dossiers de preuve — que les fournisseurs et déployeurs concernés ont tout intérêt à engager dès maintenant.

---

9. Le rôle décisif des normes harmonisées

Les normes harmonisées sont l'une des clés pratiques de l'AI Act. Elles traduisent les exigences juridiques en spécifications techniques communes et, lorsqu'elles sont référencées au *Journal officiel*, ouvrent une **présomption de conformité** (art. 40). Leur application reste volontaire, mais elles offrent une sécurité juridique importante aux entreprises. (Dans le langage courant, on parle souvent de « standards » ; le terme juridique européen est celui de normes harmonisées.)

La Commission a confié au CEN et au CENELEC, par la demande de normalisation **M/593** (décision d'exécution C(2023) 3215 du 22 mai 2023), le développement de normes dans dix domaines :

- gestion des risques ;
- gouvernance et qualité des jeux de données ;
- tenue des registres (journalisation) ;
- transparence et information des utilisateurs ;
- supervision humaine ;
- exactitude ;
- robustesse ;
- cybersécurité ;
- système de management de la qualité ;
- évaluation de conformité.

Le travail technique est mené par le comité conjoint CEN-CENELEC JTC 21. La demande a été amendée (mandat M/613, décision C(2025) 3871) pour repousser la livraison du 30 avril au 31 août 2025 — deux échéances finalement manquées. À la mi-2026, **aucune norme n'a encore été référencée au** *Journal officiel* ; le CEN-CENELEC vise désormais une disponibilité au quatrième trimestre 2026 au plus tard. La couverture normative risque donc d'arriver après la première vague d'obligations, ce qui rend d'autant plus utile le report du haut risque — et la documentation interne en attendant.

D'où une règle simple : ne pas attendre la publication des normes pour lancer le registre des usages, la cartographie et la revue contractuelle ; prévoir en revanche une mise à jour du programme de conformité dès que les normes seront référencées. Concrètement, il faut surveiller trois niveaux :

- le règlement lui-même ;
- les lignes directrices de la Commission et du Bureau de l'IA ;
- les normes harmonisées, qui deviendront la grammaire technique de la conformité.

---

10. Supervision, autorités et sanctions

L'AI Act s'accompagne d'une architecture institutionnelle utile à connaître pour identifier qui supervise, qui sanctionne et à qui l'entreprise devra répondre en cas de contrôle.

Au niveau européen : le **Bureau européen de l'IA** (*AI Office*), créé au sein de la Commission par décision du 24 janvier 2024, supervise et fait appliquer les obligations relatives aux modèles à usage général et facilite les codes de bonnes pratiques ; le **Comité européen de l'intelligence artificielle** (art. 65-66) réunit les États membres pour une application cohérente ; un **panel scientifique** d'experts indépendants (art. 68) appuie la supervision et peut émettre des alertes qualifiées (art. 90) ; un **forum consultatif** (art. 67) apporte l'expertise des parties prenantes.

Au niveau national : chaque État membre devait désigner, avant le 2 août 2025, ses **autorités nationales compétentes** et de surveillance du marché (art. 70) — plusieurs ont pris du retard. C'est l'interlocuteur de première ligne d'une entreprise pour les systèmes à haut risque et les obligations de transparence ; il convient de l'identifier pour sa propre juridiction.

Côté sanctions, deux régimes coexistent. Les amendes de l'article 99 sont prononcées par les **États membres** ; celles de l'article 101, propres aux fournisseurs de modèles à usage général, relèvent de la **Commission**, dont le pouvoir de sanction sur les GPAI s'ouvre le 2 août 2026.

MANQUEMENT	PLAFOND (LE PLUS ÉLEVÉ DES DEUX)	QUI SANCTIONNE
Pratiques interdites (art. 5)	35 M€ ou 7 % du CA mondial annuel	États membres (art. 99 §3)
Autres obligations (haut risque, transparence…)	15 M€ ou 3 % du CA mondial	États membres (art. 99 §4)
Informations incorrectes ou trompeuses aux autorités	7,5 M€ ou 1 % du CA mondial	États membres (art. 99 §5)
Fournisseurs de modèles GPAI	15 M€ ou 3 % du CA mondial	Commission européenne (art. 101)
PME et start-up	le plus *bas* des deux plafonds	art. 99 §6

Pour les grandes entreprises, le plafond retenu est le plus élevé du montant fixe ou du pourcentage ; pour les PME et start-up, c'est l'inverse, par souci de proportionnalité.

---

11. Le vrai problème des entreprises : l'IA invisible

Le principal risque des organisations n'est pas toujours le grand projet IA officiellement présenté au comité de direction. Il est souvent dans l'IA déjà là : activée par défaut dans les SaaS, testée par les métiers, employée par les prestataires, intégrée sans cartographie.

Elle se cache dans :

- les outils SaaS déjà utilisés ;
- les modules IA activés par défaut ;
- les extensions de navigateur ;
- les agents connectés aux messageries ;
- les outils de transcription d'appels ;

- les résumeurs de réunions ;
- les assistants de rédaction ;
- les solutions RH ;
- les outils d'analyse commerciale ;
- les plateformes de support client ;
- les prestataires qui utilisent l'IA sans le signaler ;
- les fichiers internes envoyés à des services externes ;
- les prototypes devenus usages récurrents.

L'AI Act transforme cette zone grise en risque de conformité.

La première brique de conformité n'est donc pas un mémo juridique. C'est un **registre des usages IA**.

Ce registre doit répondre à des questions simples :

- quel système est utilisé ?
- par quelle équipe ?
- pour quelle finalité ?
- sur quelles données ?
- avec quel fournisseur ?
- dans quel pays les données sont-elles traitées ?
- les sorties sont-elles utilisées pour décider, recommander, classer, noter, filtrer ou générer ?
- des personnes physiques sont-elles affectées ?
- le système est-il exposé à des clients, candidats, salariés, citoyens ou partenaires ?
- y a-t-il une obligation d'information ou de transparence ?
- qui supervise ?
- quelles traces sont conservées ?

Sans cette cartographie, la conformité reste théorique.

---

12. Feuille de route avant le 2 août 2026

12.1 Désigner un responsable de la cartographie IA

Il ne s'agit pas nécessairement de créer un nouveau poste. Mais il faut une personne ou une cellule clairement responsable de l'inventaire : DSI, juridique, DPO, RSSI, direction innovation ou comité IA.

L'erreur serait de laisser chaque métier décider isolément.

12.2 Créer un registre des usages IA

Le registre doit couvrir les outils internes, externes, SaaS, API, open source, génératifs, prédictifs et décisionnels.

Il doit inclure les usages officiels et les usages « *shadow AI* ».

12.3 Classer les usages en cinq catégories

Chaque usage doit être classé :

- probablement interdit ;
- potentiellement à haut risque ;
- soumis à transparence ;
- lié à un modèle d'IA à usage général ;
- risque minimal ou faible.

Ce tri n'a pas besoin d'être parfait au premier passage. Il doit être suffisamment robuste pour identifier les cas qui nécessitent une analyse approfondie.

12.4 Traiter immédiatement les cas critiques

Les cas critiques sont les usages proches des pratiques interdites ou à fort impact humain : émotion au travail, biométrie, surveillance, recrutement, crédit, assurance, santé, éducation, accès à un service essentiel, décisions automatisées ou assistance à des décisions significatives.

Ces usages doivent être gelés, audités ou encadrés avant de poursuivre.

12.5 Préparer la transparence du 2 août 2026

Chaque chatbot, agent conversationnel, avatar, voix synthétique, *deepfake* ou contenu généré à destination du public doit être identifié.

L'entreprise doit alors définir, pour chaque interface ou contenu exposé à des tiers : le message d'information, son moment d'affichage, sa formulation, sa forme visible, le marquage technique, les langues couvertes et la preuve de mise en œuvre. Livrable attendu : une règle de transparence par interface, contenu ou agent exposé.

12.6 Revoir les contrats fournisseurs IA

Chaque contrat fournisseur doit être analysé sous l'angle de l'AI Act :

- rôle du fournisseur ;
- modèle utilisé ;
- documentation disponible ;
- données traitées ;
- entraînement ou non sur les données client ;
- localisation ;
- sous-traitants ;
- logs ;
- incidents ;
- réversibilité ;
- obligations de transparence ;
- coopération en cas d'audit ou de demande d'autorité.

12.7 Former les équipes selon leur rôle

La culture IA ne doit pas être uniforme. Il faut au minimum trois niveaux :

- socle commun pour les collaborateurs exposés à l'IA ;

- formation métier pour les utilisateurs réguliers ;
- formation renforcée pour DSI, juridique, DPO, RSSI, RH, achats, data, produit et dirigeants.

12.8 Documenter la supervision humaine

Pour les usages sensibles, il faut décrire qui supervise, à quel moment, avec quelles informations, avec quel droit de contestation, avec quel pouvoir de correction et avec quelles traces.

Un « humain dans la boucle » non formé, non outillé et sans pouvoir réel de correction ne suffit pas.

12.9 Préparer un dossier de preuve minimal

Pour chaque usage IA sensible, il faut réunir :

- fiche d'usage ;
- fournisseur ;
- finalité ;
- données utilisées ;
- catégorie de risque ;
- personnes concernées ;
- documentation fournisseur ;
- information utilisateur ;
- supervision humaine ;
- mesures de sécurité ;
- logs disponibles ;
- procédure d'incident ;
- date de revue.

12.10 Organiser une revue périodique

Les systèmes d'IA évoluent vite. Un registre figé devient rapidement obsolète.

Il faut prévoir une revue trimestrielle pour les usages sensibles et une revue semestrielle pour les usages moins critiques.

---

13. Matrice opérationnelle par fonction

FONCTION	CE QU'ELLE DOIT FAIRE AVANT LE 2 AOÛT 2026
Direction générale	Nommer un sponsor IA, arbitrer les usages sensibles, intégrer l'AI Act au pilotage des risques.
DSI	Cartographier les outils, API, SaaS et intégrations IA ; contrôler les accès, les logs et les dépendances fournisseurs.
RSSI	Évaluer les risques de fuite de données, d'injection de prompt, de compromission d'agents, de dépendance API et de sécurité des modèles.
Juridique / DPO	Qualifier les rôles, revoir les contrats, articuler AI Act, RGPD, droit du travail, propriété intellectuelle et obligations sectorielles.

FONCTION	CE QU'ELLE DOIT FAIRE AVANT LE 2 AOÛT 2026
RH	Auditer les outils de recrutement, d'évaluation, de *matching*, de mobilité interne et de suivi des salariés.
Marketing / communication	Identifier les contenus générés, images, vidéos, voix, avatars, textes d'intérêt public et obligations de labellisation.
Achats	Ajouter un questionnaire AI Act aux appels d'offres et contrats fournisseurs.
Produit / SaaS	Vérifier si les fonctionnalités IA exposées aux clients déclenchent des obligations de fournisseur, de transparence ou de haut risque.
Data / IA	Documenter modèles, données, évaluations, limites, biais, monitoring, changements et incidents.
Métiers	Déclarer les usages, identifier les décisions assistées, vérifier la supervision humaine et remonter les incidents.

14. Les sept questions à poser en comité de direction

1. Avons-nous une liste complète des systèmes d'IA utilisés dans l'entreprise ?
2. Savons-nous lesquels touchent aux salariés, candidats, clients, citoyens, patients, élèves ou assurés ?
3. Savons-nous quels outils génèrent ou manipulent des contenus publiés ou envoyés à des tiers ?
4. Savons-nous quand nous devons informer qu'une personne interagit avec une IA ?
5. Nos contrats fournisseurs nous donnent-ils assez d'informations pour prouver notre maîtrise ?
6. Avons-nous formé les personnes qui utilisent ou supervisent l'IA ?
7. Pouvons-nous produire un dossier de preuve en cas d'audit, d'incident, de litige ou de demande client ?

15. Scénarios 2026–2028

Scénario 1 : la transparence devient le premier choc visible. Le premier choc pour de nombreuses entreprises ne viendra pas des systèmes à haut risque, mais des obligations de transparence. Les chatbots, contenus générés, *deepfakes*, avatars et voix synthétiques sont visibles par les clients, salariés, candidats et médias. Une erreur de signalement peut rapidement devenir un sujet de confiance ou de réputation.

Scénario 2 : la conformité devient un critère d'achat B2B. Les grands comptes, administrations, banques, assureurs, industriels et acteurs régulés vont progressivement demander à leurs fournisseurs de documenter leurs usages IA. Même les PME non directement exposées à des obligations lourdes devront répondre à des questionnaires de conformité.

Scénario 3 : le haut risque devient une affaire de normes. Le report à décembre 2027 ou août 2028 ne supprime pas le travail. Il le déplace vers les normes, la documentation, l'évaluation de conformité, la gestion des risques et les dossiers de preuve.

Scénario 4 : les agents IA compliquent la cartographie. Les agents capables d'exécuter des actions, d'appeler des outils, de lire des bases internes ou d'interagir avec plusieurs systèmes rendent la conformité plus difficile. Le risque ne tient plus seulement à une sortie générée, mais à une chaîne d'actions.

Scénario 5 : la confiance devient un avantage concurrentiel. Les entreprises capables de dire clairement « nous savons où nous utilisons l'IA, pourquoi, avec quelles garanties et sous quelle supervision » auront un avantage dans les appels d'offres, les partenariats, les relations clients et les secteurs régulés.

---

16. Recommandations pour les décideurs

1. **Ne pas attendre août 2026.** Certaines obligations sont applicables depuis février 2025 et août 2025. Le 2 août 2026 n'est pas le début du règlement, mais sa prochaine échéance visible.
2. **Commencer par le registre.** Une entreprise qui ne sait pas où elle utilise l'IA ne peut pas démontrer sa conformité.
3. **Classer vite, approfondir ensuite.** Un premier classement imparfait mais exploitable vaut mieux qu'une analyse exhaustive qui arrive trop tard.
4. **Traiter les usages RH, biométriques, clients et décisionnels en priorité.** Ce sont les zones les plus sensibles pour les droits fondamentaux et la réputation.
5. **Préparer la transparence comme un chantier produit, pas seulement juridique.** Il faut concevoir les messages, l'UX, les marquages, les logs et les preuves.
6. **Revoir les contrats fournisseurs.** Le fournisseur qui ne documente pas son IA transfère une partie du risque vers son client.
7. **Former par rôle.** La culture IA exigée par le règlement doit être contextualisée : direction, métier, RH, DSI, juridique, achats, data et produit n'ont pas les mêmes besoins.
8. **Constituer un dossier de preuve minimal.** En matière d'IA, ce qui n'est pas documenté sera difficile à défendre.

Glossaire

AI Act. Règlement (UE) 2024/1689 établissant des règles harmonisées sur l'intelligence artificielle. Il vise à encadrer les risques liés aux systèmes d'IA et aux modèles d'IA à usage général, tout en soutenant l'innovation et la confiance.

Digital Omnibus. Paquet de simplification du droit numérique proposé par la Commission le 19 novembre 2025. Son volet IA réaménage notamment le calendrier des systèmes à haut risque (dates fixes des 2 décembre 2027 et 2 août 2028) et allège l'obligation de culture IA.

Bureau européen de l'IA (*AI Office*). Structure créée au sein de la Commission (décision du 24 janvier 2024) chargée de superviser les modèles à usage général, de faciliter les codes de bonnes pratiques et d'appuyer l'application cohérente du règlement.

Système d'IA. Notion définie par le règlement et précisée par des lignes directrices de la Commission, non contraignantes et susceptibles d'évoluer avec les usages.

Fournisseur. Acteur qui développe ou fait développer un système d'IA et le met sur le marché ou en service sous son nom ou sa marque (art. 3, §3).

Déployeur. Acteur qui utilise un système d'IA sous son autorité dans un cadre professionnel (art. 3, §4).

Modèle d'IA à usage général (**GPAI**). Modèle pouvant être utilisé pour de nombreuses tâches et intégré dans de nombreux systèmes. Ses fournisseurs sont soumis à des obligations de documentation, de transparence et de respect du droit d'auteur (art. 53).

Risque systémique. Régime applicable aux modèles les plus avancés (art. 51-55). Un modèle est présumé concerné au-delà de 10^{25} FLOP d'entraînement — présomption réfragable, distincte du seuil indicatif de 10^{23} FLOP qui sert à qualifier un modèle « à usage général ».

Système à haut risque. Système relevant de l'annexe I (produits réglementés) ou de l'annexe III (usages sensibles : emploi, éducation, crédit, biométrie, justice…), soumis à des exigences strictes (art. 6 et suivants).

Deepfake (**hypertrucage**). Contenu image, audio ou vidéo généré ou manipulé par IA donnant l'apparence d'une personne, d'un objet, d'un lieu ou d'un événement réel. Sa diffusion peut être soumise à une obligation de divulgation visible (art. 50 §4).

Marquage et filigranage (*watermarking*). Techniques rendant un contenu généré par IA détectable comme tel — métadonnées signées (standard C2PA) ou signal imperceptible inséré dans le contenu — au cœur des obligations de transparence de l'article 50 §2.

Culture IA. Niveau de compétences et de compréhension que les fournisseurs et déployeurs doivent garantir aux personnes qui utilisent ou supervisent des systèmes d'IA pour leur compte (art. 4).

Norme harmonisée. Norme technique européenne traduisant les exigences du règlement en spécifications opérationnelles. Référencée au *Journal officiel*, elle ouvre une présomption de conformité (art. 40).

Présomption de conformité. Effet juridique par lequel un système conforme à une norme harmonisée référencée est réputé satisfaire aux exigences correspondantes du règlement, sauf preuve contraire.

Évaluation de conformité. Processus permettant de démontrer qu'un système à haut risque respecte les exigences applicables avant sa mise sur le marché ou sa mise en service (art. 43).

Supervision humaine. Mécanisme par lequel une ou plusieurs personnes suffisamment formées et habilitées surveillent l'utilisation d'un système d'IA, comprennent ses limites, peuvent intervenir et corriger les effets indésirables (art. 14).

Sources de référence

Cette note s'appuie sur les sources officielles suivantes, à suivre pour ses mises à jour :

- **Texte et calendrier.** Règlement (UE) 2024/1689 (AI Act), *Journal officiel* du 12 juillet 2024 ; article 113 (calendrier d'application) ; articles 99 et 101 (sanctions) ; article 111 §3 (modèles GPAI antérieurs au 2 août 2025).
- **Digital Omnibus.** Proposition de la Commission COM(2025) 836 du 19 novembre 2025 ; accord politique du Conseil et du Parlement (7 mai 2026) ; approbation finale du Parlement européen le 16 juin 2026 (423 voix pour, 57 contre, 174 abstentions) ; texte en cours d'adoption formelle par le Conseil, non encore publié au *Journal officiel* ; dates fixes du 2 décembre 2027 (annexe III) et du 2 août 2028 (annexe I).
- **Pratiques interdites et culture IA.** Lignes directrices sur les pratiques interdites (C(2025) 5052 final, 29 juillet 2025 ; contenu approuvé le 4 février 2025) ; répertoire vivant des pratiques de culture IA du Bureau de l'IA.
- **Modèles à usage général.** Code de bonnes pratiques GPAI (10 juillet 2025) et avis de la Commission du 1er août 2025 ; lignes directrices sur le champ des obligations GPAI (C(2025) 5045 final, 18 juillet 2025) ; modèle de résumé des données d'entraînement (24 juillet 2025) ; liste officielle des signataires (mise à jour du 23 avril 2026).

- **Transparence.** Article 50 du règlement ; Code de bonnes pratiques sur la transparence des contenus générés par IA (10 juin 2026) ; projet de lignes directrices sur l'article 50 (8 mai 2026, consultation close le 3 juin 2026).
- **Normes harmonisées.** Demande de normalisation M/593 (décision C(2023) 3215 du 22 mai 2023), amendée par M/613 (C(2025) 3871) ; travaux du CEN-CENELEC JTC 21 ; page de normalisation de la Commission.
- **Gouvernance et application.** Bureau européen de l'IA (décision de la Commission du 24 janvier 2024) ; Comité européen de l'IA (art. 65-66) ; panel scientifique (art. 68) et alertes qualifiées (art. 90) ; autorités nationales compétentes (art. 70) ; cadre réglementaire de l'IA et FAQ « Navigating the AI Act » de la Commission.

L'AI Act ne demande pas aux entreprises de ralentir l'adoption de l'IA, mais de savoir ce qu'elles déploient, pourquoi, quels risques elles acceptent et quelles preuves elles peuvent produire. Sur ce terrain, la conformité deviendra autant un critère de confiance, d'achat et de différenciation qu'une obligation réglementaire.

Cette note s'inscrit dans la série de publications de référence d'IntelligenceArtificielle.com consacrées aux transformations structurelles du marché de l'IA, à destination des décideurs économiques, publics et institutionnels. Elle constitue une information générale à jour au 23 juin 2026 et ne constitue pas un avis juridique ; elle est appelée à être enrichie au fil des évolutions réglementaires, lignes directrices, normes harmonisées et clarifications pertinentes.

Note de référence publiée par la société IntelligenceArtificielle.com. Cette ressource est citée et référencée notamment depuis actuia.com. Information générale à jour au 23 juin 2026, ne constituant pas un avis juridique.