Guide de conformité IA 2026

Guide de conformité IA pour les entreprises et les particuliers (2026) : AI Act, DSA et RGPD

> **De quoi s'agit-il.** Un dossier pratique et vérifié sur ce que les autorités européennes et espagnoles vont exiger à toute personne qui utilise l'intelligence artificielle, possède un site web ou traite des données. Il est conçu pour qu'un chef d'entreprise, un travailleur indépendant ou un particulier sache ce qui lui s'applique, ce que les régulateurs vont examiner à la loupe, où se trouvent les pièges et comment se préparer sans dépenser trop ni minimiser les risques.
>
> **Avertissement.** Il s'agit d'informations rigoureuses, pas de conseils juridiques individuels. Le cadre légal de 2026 est en mouvement (nous l'indiquons là où c'est nécessaire). Clôture de cette édition : juin 2026.

---

1. TL;DR : est-ce que cela me concerne ?

Réponse courte : **presque certainement oui, mais probablement moins que tu ne le crains et d'une façon différente de ce que tu imagines.**

- **Tu utilises de l'IA dans ton entreprise** (un chatbot, un outil qui rédige, qui note des CV, qui génère des images) ? Le **règlement européen sur l'IA (AI Act)** te s'applique, presque toujours dans sa version la plus légère, ainsi que le **RGPD** si cette IA touche des données personnelles.
- **Tu as un site web ou une application où d'autres publient** (commentaires, avis, un marketplace, un forum) ? Le **règlement sur les services numériques (DSA)** te s'applique, en général uniquement pour ses obligations de base.
- **Tu es indépendant ou professionnel et tu crées du contenu avec de l'IA** (vidéos, voix, images) ? Les **obligations de transparence** te s'appliquent (indiquer qu'il s'agit de contenu synthétique). En **usage purement personnel et non professionnel**, l'AI Act ne t'impose pas ces obligations de « responsable du déploiement », mais les interdictions et d'autres règles restent applicables (droits d'auteur, honneur, protection des données).

Les trois règlements coexistent et se complètent. Tu ne choisis pas : ceux qui correspondent à ta situation te s'appliquent simultanément. Le reste du dossier est la carte pour savoir lesquels et quoi faire.

---

2. Le cadre en une page

Règlement	Ce qu'il régit	À qui il s'adresse principalement
AI Act (règlement UE 2024/1689)	L'**utilisation et la commercialisation des systèmes d'IA**, par niveaux de risque	Qui fabrique de l'IA (fournisseur) et qui l'utilise professionnellement (responsable du déploiement)
DSA (règlement UE 2022/2065)	Les **services intermédiaires numériques** et la modération de contenus de tiers	Hébergeurs, marketplaces, plateformes, moteurs de recherche
RGPD (règlement UE 2016/679)	Le **traitement de données personnelles** (y compris quand une IA le fait)	Toute personne qui traite des données de personnes physiques

Idée clé : l'**AI Act** regarde *ce que fait le système d'IA* ; le **RGPD** regarde *quelles données personnelles il touche* ; le **DSA** regarde *ce qui se passe avec le contenu que des tiers publient sur ton service*. Un même projet peut activer les trois.

---

3. Le calendrier (et le délai qui a bougé)

L'AI Act s'applique de façon **échelonnée** (article 113). Ce qui est déjà obligatoire et exigible :

Date	Ce qui entre en jeu	État
1 août 2024	Entrée en vigueur	Sans obligations encore
2 fév. 2025	**Pratiques interdites (art. 5)** + **culture de l'IA (art. 4)**	✅ En vigueur et exigible
2 août 2025	Obligations des **modèles d'usage général (GPAI)**, gouvernance et **régime de sanctions (arts. 99-100)**	✅ En vigueur
2 août 2026	**Haut risque de l'annexe III** + **transparence (art. 50)** + évaluations d'impact + bacs à sable réglementaires	Date par défaut
2 août 2027	Haut risque intégré dans les **produits réglementés (annexe I)**	Date par défaut

Encadré : le délai qui a bougé

Voici la nuance que presque personne ne rapporte correctement. La Commission européenne a proposé en novembre 2025 le **« Digital Omnibus »** (COM(2025)836), un ensemble de mesures qui **propose de reporter l'entrée en vigueur du régime de haut risque** :

- **Annexe III** (biométrie, emploi, éducation, services essentiels, etc.) : du 2 août 2026 à **fin 2027** (les sources indiquent le 2 décembre 2027).
- **Annexe I** (IA intégrée dans des produits réglementés) : du 2 août 2027 à **2028** (autour du 2 août 2028).

Attention : en juin 2026, il s'agit d'une **proposition en cours d'examen législatif** (procédure 2025/0359(COD)), **pas du droit en vigueur** : le texte n'a pas encore été adopté définitivement ni publié au Journal officiel de l'UE, et les dates exactes peuvent changer au cours de la négociation. Le Digital Omnibus « déplace l'horloge, pas l'architecture » : il ne modifie pas les obligations de fond, seulement leur date d'entrée en vigueur.

Que faire avec ça : planifie de façon conservatrice vers août 2026, car le report n'est pas encore certain, mais garde à l'esprit que tu auras probablement plus de temps que ne l'indique le calendrier par défaut. Vérifie la date définitive avant de prendre des décisions importantes. Source : Digital Omnibus, Commission européenne.

Ce qui compte vraiment aujourd'hui : **les interdictions et l'obligation de formation sont en vigueur depuis février 2025.** Ce n'est pas du futur.

---

4. L'AI Act par niveaux de risque

L'AI Act classe les systèmes d'IA en quatre niveaux. Ta première tâche est de savoir dans lequel tombe chaque outil que tu utilises.

Risque inacceptable (interdit), art. 5

Huit pratiques interdites depuis février 2025, sans possibilité de mitigation. Celles qui concernent le plus les entreprises :

- Manipulation subliminale ou exploitation de vulnérabilités pour altérer le comportement de façon préjudiciable.
- **Notation sociale** (social scoring) des personnes.
- **Reconnaissance des émotions au travail et dans les établissements scolaires** (sauf raisons médicales ou de sécurité).
- **Catégorisation biométrique** selon des caractéristiques sensibles (race, religion, orientation, etc.).
- Création de bases de données de reconnaissance faciale par **scraping massif** d'internet ou de caméras.

Si l'un de tes outils fait l'une de ces choses, la réponse n'est pas de « mitiger » : c'est de retirer l'outil.

Haut risque (annexe III + annexe I)

Systèmes dans huit domaines sensibles : biométrie, infrastructures critiques, **éducation**, **emploi et ressources humaines** (filtrage de CV, décisions de promotion), services essentiels (dont le **scoring de crédit**), application de la loi, migration et justice. Si tu en fabriques un, les obligations sont importantes : gestion des risques, gouvernance des données, documentation technique, journaux de bord, supervision humaine, robustesse, évaluation de conformité, **marquage CE** et enregistrement dans une base de données de l'UE.

Si tu l'utilises seulement (tu es « responsable du déploiement »), tes obligations sont plus limitées mais bien réelles : l'utiliser conformément aux instructions, une **supervision humaine** désignée, conserver des **journaux de bord (minimum 6 mois)**, **informer les représentants des travailleurs** et, dans certains cas, réaliser une **analyse d'impact sur les droits fondamentaux (FRIA, art. 27)**.

Risque limité (transparence), art. 50

Le niveau où tomberont la plupart des PME. Obligation principale : **informer**.

- Un **chatbot** doit s'identifier comme IA (« tu parles avec un assistant automatique »).
- Qui **fabrique** un système générant du contenu synthétique doit le marquer dans un format lisible par machine (art. 50.2). Qui **publie un deepfake** doit **révéler qu'il a été**

généré ou manipulé avec de l'IA (art. 50.4), avec des nuances pour les œuvres créatives, satiriques ou artistiques.

Ces obligations de transparence s'appliquent à partir d'**août 2026**. Attention : le report du Digital Omnibus concerne le **régime de haut risque** (chapitre III), pas ces obligations de l'art. 50 (sauf une transition spécifique pour les systèmes génératifs déjà sur le marché). Les anticiper est une bonne pratique et la réglementation sur les consommateurs l'exige souvent déjà.

Risque minimal

Filtres anti-spam, jeux vidéo, systèmes de recommandation triviaux. Sans obligations spécifiques de l'AI Act.

> **Modèles d'usage général (GPAI) :** si tu utilises ChatGPT, Claude, Gemini ou des outils similaires, *tu* n'en es pas le fournisseur, donc les obligations GPAI (documentation technique, résumé des données d'entraînement, politique de droits d'auteur ; et pour les plus puissants, red-teaming et rapport d'incidents) incombent à l'entreprise qui les fabrique, pas à toi. Tu es concerné en tant que *deployer* du niveau correspondant à l'usage.

---

5. DSA : est-ce que j'ai une « plateforme » ? (et pourquoi probablement pas)

Le DSA fait plus peur qu'il ne le devrait aux PME. Ce qui compte vraiment :

- **Site web d'entreprise sans contenu de tiers :** le DSA **ne te s'applique pas**, car tu n'es pas un « service intermédiaire » (le DSA ne réglemente que ceux qui hébergent ou transmettent du contenu de tiers). Tes obligations viennent du RGPD et de la réglementation sur les consommateurs, pas du DSA.
- **Site avec commentaires ou avis :** tu deviens un « hébergeur ». Obligations de base : **mécanisme de notification et de retrait de contenu illicite** (notice & action, art. 16) et **motiver** quand tu supprimes quelque chose (art. 17).
- **Marketplace ou forum :** tu es une « plateforme en ligne », mais voici le soulagement : l'**article 19 exempte les microentreprises et les petites entreprises** (moins de 50 salariés et moins de 10 M€) des obligations les plus lourdes (système formel de réclamations, résolution extrajudiciaire, rapports de transparence). **Cela ne t'exempte pas** du notice & action ni de motiver les retraits.
- **Très grande plateforme (VLOP) :** à partir de 45 millions d'utilisateurs dans l'UE. Audits, évaluation des risques, supervision directe de la Commission. Ce n'est pas ton cas si tu lis ceci.

Sanctions : jusqu'à **6 % du chiffre d'affaires mondial annuel** (art. 74). Pour les grandes plateformes (VLOP), elles sont imposées par la Commission européenne ; pour les autres services intermédiaires, elles sont fixées par les autorités nationales (art. 52), également jusqu'à ces 6 %. Le DSA s'applique **pleinement depuis le 17 février 2024**.

> **Un fait que presque personne ne mentionne :** en Espagne, l'autorité du DSA est la **CNMC** (coordinateur des services numériques), mais la Commission européenne **a poursuivi l'Espagne devant la Cour de justice de l'UE en mai 2025** (IP/25/1081) parce que la CNMC ne dispose **pas encore de pleins pouvoirs de sanction**. Le DSA est directement applicable malgré tout, mais le régime administratif de sanctions en Espagne est en attente. Traduction : l'obligation existe, le bâton national est encore en train d'être mis en place.

Ne confonds pas le DSA avec le RGPD (données) ni avec le DMA (grandes plateformes et concurrence) : ce sont des règlements distincts.

---

6. Qui surveille et ce qu'ils vont examiner à la loupe

Autorités :

Autorité	Domaine
AI Office (Commission européenne)	Modèles d'usage général (GPAI) ; coordination UE
AESIA (Agence espagnole de supervision de l'IA, La Corogne)	Pratiques interdites, haut risque général, transparence
AEPD	Données personnelles, **biométrie**, décisions automatisées (art. 22 RGPD)
CNMC	DSA et dimension concurrentielle des algorithmes

L'AESIA existe et est opérationnelle (créée par le RD 729/2023), et a déjà clôturé le **premier bac à sable réglementaire IA de l'UE**. Son plein pouvoir de sanction dépend de la future **loi organique espagnole sur le bon usage et la gouvernance de l'IA**, qui en juin 2026 est encore **en cours d'examen, pas en vigueur**.

Priorités de contrôle (ce qu'ils vont examiner en premier) :

1. Pratiques **interdites** (notation sociale, biométrie, manipulation). Déjà sanctionnable.
2. **Transparence** : chatbots et deepfakes sans avertissement.
3. Systèmes de **haut risque sans conformité** (RH, scoring) sans documentation ni supervision humaine.
4. **Intersection avec le RGPD** : base juridique, décisions automatisées, évaluations d'impact.

5. **Réclamations de personnes concernées** : souvent, l'inspection commence par une plainte.

---

7. Sanctions : combien ça fait mal

AI Act (art. 99), chiffres vérifiés :

Conduite	Régime général (le montant le plus élevé)	PME (le montant le plus bas)
Pratiques interdites (art. 5)	**35 M€ ou 7 %** du chiffre d'affaires mondial	le plus bas des deux
Manquement à d'autres obligations	**15 M€ ou 3 %**	le plus bas des deux
Fournir des informations incorrectes aux autorités	**7,5 M€ ou 1 %**	le plus bas des deux

Deux nuances importantes et peu connues : le plafond pour les informations incorrectes est de **1 %** (pas 1,5 %, comme le répètent certaines sources), et pour **les PME et les startups, c'est le montant le plus bas** des deux qui s'applique (à l'inverse des grandes entreprises). Détail dans l'article 99.

DSA : jusqu'à **6 %** du chiffre d'affaires mondial annuel (la Commission européenne pour les grandes plateformes ; les autorités nationales pour les autres services intermédiaires).

RGPD : jusqu'à **20 M€ ou 4 %**. En Espagne, l'AEPD a traité des centaines de procédures de sanction en 2024 ; l'IA figure parmi ses défis déclarés.

---

8. Les pièges (erreurs typiques qui sont sanctionnées)

Classés par gravité réglementaire :

1. **IA dans les RH sans évaluation.** Filtrer des CV ou décider des promotions avec de l'IA est du haut risque : cela exige une base juridique, une évaluation d'impact et une supervision. Le faire à l'aveugle constitue une triple infraction.
2. **Décisions automatisées sans intervention humaine réelle** (art. 22 RGPD). La personne humaine doit pouvoir comprendre et annuler le système, pas simplement valider ce que la machine dit.
3. **Biométrie sans base juridique renforcée** (art. 9 RGPD). Dans le domaine du travail, en Espagne, le consentement du salarié n'est pas considéré comme valide en raison du rapport de pouvoir.
4. **Chatbot qui n'avertit pas qu'il est une IA** (art. 50).
5. **Utiliser une IA tierce sans contrat de sous-traitance (DPA) signé** avant de lui confier des données personnelles. La responsabilité repose sur toi, pas sur le fournisseur.

6. **Scraping massif de données personnelles pour l'IA** sans test de mise en balance. L'avis 28/2024 du Comité européen de la protection des données est clair : l'intérêt légitime ne l'emporte pas automatiquement.
7. **Deepfakes et contenu synthétique sans étiquetage.**
8. **Ne pas informer les salariés** d'un usage de l'IA qui les affecte (art. 64 du statut des travailleurs espagnol + arts. 13-14 RGPD).
9. **« IA-washing » :** vendre des capacités que le système n'a pas (publicité trompeuse).
10. **Copier la politique IA d'une autre entreprise.** Cela viole le principe d'accountability et aggrave la sanction en cas d'inspection.

---

9. Bonnes pratiques et mauvaises pratiques

Aspect	Mauvais	Bien
Inventaire IA	Informel, « je sais ce que j'utilise »	Registre avec fournisseur, finalité, données et base juridique par outil
Décisions automatiques	Sans révision humaine possible	Personne désignée pouvant annuler + canal de contestation visible
Chatbot	Se présente comme une personne	« Je suis un assistant IA » dès le premier message
Contenu avec IA	Sans étiquette	Étiquette visible + marquage technique dans les métadonnées
Fournisseur IA	API sans DPA signé	DPA signé avant le premier appel avec des données personnelles
Formation	« Ils savent déjà utiliser l'IA »	Registre signé, proportionnel au risque, mis à jour
Supervision	« Le système est très bon »	Personne qui comprend et peut annuler ; documenté
Incidents	Attendre la plainte du client	Protocole : détecter, évaluer, notifier à l'AEPD dans les 72 h

Le fil conducteur est le **principe d'accountability (responsabilité proactive)** : il ne suffit pas de se conformer, il faut **pouvoir le démontrer et le justifier** devant l'autorité avec une documentation vivante.

---

10. Comment préparer ton entreprise : checklist par phases

Bloc A. Inventaire (à faire maintenant). Liste de tous les outils d'IA que tu utilises : fournisseur, pour quoi, quelles données il touche, base juridique et si un DPA est signé.

Bloc B. Base juridique et contrats (avant de traiter des données). Une base juridique du RGPD (art. 6) par traitement ; **DPA signé** avec chaque fournisseur d'IA (OpenAI, Anthropic et Google en proposent un) ; vérifie le mécanisme de transfert international (cadre UE-États-Unis ou clauses contractuelles types).

Bloc C. Évaluations d'impact (avant le déploiement). Réalise une **DPIA** en cas de profilage, de catégories spéciales ou de décisions automatisées significatives. Ajoute une **FRIA** (art. 27) si tu es un **organisme public**, une **entité privée qui fournit des services publics**, ou si tu utilises une IA à haut risque pour **évaluer la solvabilité ou le scoring de crédit** de personnes ou pour les **assurances vie et santé** (annexe III.5).

Bloc D. Transparence (avant août 2026). Avertissement « tu parles avec une IA » dans les chatbots ; étiquette du contenu généré avec de l'IA ; mécanisme pour contester les décisions automatisées.

Bloc E. Formation (art. 4, déjà en vigueur). Formation documentée et signée par salarié, proportionnelle au risque de son poste. Aucune certification officielle n'est exigée, mais il faut en conserver la trace.

Bloc F. Supervision et registres (continu). Journaux de bord des décisions, supervision humaine réelle documentée, révision annuelle de l'inventaire et protocole d'incidents (notification à l'AEPD dans les 72 h en cas de violation de données).

---

11. Pour les particuliers et les indépendants

Pas seulement les entreprises sont dans le viseur :

- **Créateurs de contenu avec IA (à titre professionnel) :** l'obligation de **révéler le contenu synthétique** (art. 50) te concerne quand tu publies des deepfakes, des voix ou des images générées dans le cadre d'une activité professionnelle. L'usage purement personnel et domestique est en grande partie hors du champ de l'AI Act, même s'il reste soumis à d'autres règles.
- **Deepfakes sans consentement :** outre la transparence, certains usages (sexuels, usurpation d'identité) sont interdits ou spécifiquement encadrés par la loi. La future loi espagnole renforce cela.
- **Droits d'auteur :** générer avec de l'IA ne te donne pas automatiquement la titularité, et utiliser des œuvres d'autrui pour créer peut avoir des conséquences.
- **Indépendants qui utilisent l'IA avec des données de clients :** les mêmes règles du RGPD et de DPA avec le fournisseur que pour une entreprise te s'appliquent.

---

12. Glossaire rapide

- **Fournisseur :** qui fabrique ou commercialise le système d'IA.
- **Responsable du déploiement (deployer) :** qui utilise le système d'IA dans son activité. La plupart des entreprises.
- **GPAI :** modèle d'IA d'usage général (les grands modèles génératifs).
- **DPIA :** analyse d'impact relative à la protection des données (RGPD, art. 35).
- **FRIA :** analyse d'impact sur les droits fondamentaux (AI Act, art. 27).
- **DPA :** contrat de sous-traitance (RGPD, art. 28).
- **VLOP :** très grande plateforme en ligne (DSA).
- **Accountability :** responsabilité proactive, capacité à démontrer la conformité.

Sources

> Pour les numéros d'article et les sanctions, la source qui fait autorité est toujours le **texte officiel sur EUR-Lex / JOUE**. Les pages d'analyse (comme artificialintelligenceact.eu) sont incluses uniquement à titre de soutien informatif, pas comme source normative.

Primaires (AI Act) - Règlement (UE) 2024/1689, texte consolidé (inclut les arts. 5, 27, 50, 99 et 113) : https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=es - Calendrier d'application (AI Act Service Desk, Commission européenne) : https://ai-act-service-desk.ec.europa.eu/en/ai-act/timeline/timeline-implementation-eu-ai-act - Digital Omnibus, proposition COM(2025)836 (Commission européenne) : https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal

Soutien informatif (non officiel) - AI Act Explorer (analyse par articles, arts. 27/50/99) : https://artificialintelligenceact.eu/es/

DSA - Règlement (UE) 2022/2065, texte en espagnol : https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:32022R2065 - Politique DSA (Commission européenne) : https://digital-strategy.ec.europa.eu/en/policies/digital-services-act - Liste des VLOP/VLOSE : https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops - CNMC, coordinateur des services numériques : https://www.cnmc.es/en/sectores-que-regulamos/servicios-digitales-dsa - Recours de la Commission contre l'Espagne (IP/25/1081) : https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1081

Espagne / RGPD - AESIA (site officiel) : https://aesia.digital.gob.es/es - RD 729/2023 (statut de l'AESIA) : https://www.boe.es/buscar/doc.php?id=BOE-A-2023-18911 - AEPD, guide d'adéquation au RGPD des traitements avec IA : https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf - AEPD, orientations sur l'IA agentique :

https://www.aepd.es/guias/orientaciones-ia-agentica.pdf - EDPB, avis 28/2024 (modèles d'IA et protection des données) : https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf

Cas - Amende du Garante italien à OpenAI (15 M€, décembre 2024). Source primaire : communiqué du *Garante per la protezione dei dati personali* (https://www.garanteprivacy.it). Couverture de presse (secondaire) : https://www.euronews.com/next/2024/12/20/italys-privacy-watchdog-fines-openai-15-million-after-probe-into-chatgpt-data-collection

---

Édition clôturée en juin 2026. Le cadre réglementaire est en évolution (en particulier, le Digital Omnibus et la loi organique espagnole sur l'IA). Vérifie les dates et l'état d'avancement avant de prendre des décisions à impact juridique. Information générale, pas de conseil juridique individuel.