Checklist de conformité IA

Checklist d’auto-évaluation : ton entreprise est-elle prête pour l’AI Act, le DSA et le RGPD ?

> Une page pour savoir où tu en es. Coche chaque case avec honnêteté. Si tu en as plus de 3 sans coche, il est temps de s’y mettre. Information générale, pas de conseil juridique individuel. Édition : juin 2026.

Étape 1. Quels règlements te concernent ? (tri en 1 minute)

- ☐ **J’utilise de l’IA dans mon activité** (chatbot, génération de texte/image, outils qui décident ou notent) : l’**AI Act** me s’applique.
- ☐ **Cette IA touche des données de personnes** (clients, salariés, prospects) : le **RGPD** me s’applique aussi.
- ☐ **J’ai un site web/une application où des tiers publient** (commentaires, avis, marketplace, forum) : le **DSA** me s’applique aussi.
- ☐ **Mon site ne contient que du contenu propre**, sans contenu de tiers : le **DSA ne me s’applique pas**.

Étape 2. Niveau de risque de ton IA (AI Act)

- ☐ J’ai vérifié qu’**aucun** de mes outils ne fait quelque chose d’**interdit** (notation sociale, reconnaissance des émotions au travail, catégorisation biométrique sensible, scraping facial massif).
- ☐ Je sais si j’utilise une IA à **haut risque** (RH/filtrage de CV, scoring de crédit, biométrie). Si c’est le cas, j’ai une évaluation, une documentation et une supervision.
- ☐ Mes **chatbots et contenus générés avec de l’IA** avertissent qu’il s’agit d’une IA (transparence, art. 50).

Étape 3. Données et contrats (RGPD)

- ☐ J’ai une **base juridique** claire pour chaque traitement avec IA (art. 6 RGPD).
- ☐ J’ai signé le **contrat de sous-traitance (DPA)** avec chaque fournisseur d’IA (OpenAI, Anthropic, Google, etc.) **avant** de lui confier des données personnelles.

- [ ] J'ai vérifié le **mécanisme de transfert international** si le fournisseur est hors de l'UE.
- [ ] J'ai réalisé une **DPIA** là où il y a du profilage, des données sensibles ou des décisions automatisées significatives.
- [ ] Là où il y a des **décisions automatisées**, une personne peut les comprendre et les annuler (art. 22 RGPD).

Étape 4. Personnes (salariés et personnes concernées)

- [ ] J'ai dispensé une **formation documentée** sur l'IA au personnel qui l'utilise (art. 4 AI Act, déjà en vigueur).
- [ ] J'ai **informé les salariés** (ou leurs représentants) des usages de l'IA qui les affectent.
- [ ] Il existe un **canal visible** pour qu'une personne concernée puisse réclamer ou contester une décision.

Étape 5. Gouvernance et registres (accountability)

- [ ] J'ai un **inventaire** de mes outils d'IA (fournisseur, finalité, données, base juridique, DPA).
- [ ] J'ai une **politique interne d'utilisation de l'IA** qui m'est propre (pas copiée d'une autre entreprise).
- [ ] Je conserve des **journaux de bord** des décisions pertinentes.
- [ ] J'ai un **protocole d'incidents** (y compris la notification à l'AEPD dans les 72 h en cas de violation).
- [ ] Je révise cet inventaire **au moins une fois par an**.

Étape 6. Si j'ai un site web/une application avec du contenu de tiers (DSA)

- [ ] J'ai un **point de contact** et des conditions d'utilisation claires.
- [ ] J'ai un mécanisme de **notification et de retrait** de contenu illicite (notice & action).
- [ ] Quand je supprime du contenu, j'**explique le motif** à l'utilisateur.
- [ ] Je n'utilise pas de **pratiques trompeuses** (dark patterns) ni de publicité non identifiée.

Les 5 pièges les plus sanctionnés

1. IA dans les RH sans évaluation des risques ni base juridique.
2. Décisions automatisées sans intervention humaine réelle.
3. Chatbots ou deepfakes sans avertissement qu'il s'agit d'une IA.
4. Utiliser une IA tierce sans DPA signé.
5. « IA-washing » : promettre des capacités IA que le système n'a pas.

Tu as laissé des cases non cochées ? Ce sont tes tâches prioritaires. Commence par l'inventaire (Étape 5) : sans savoir quelle IA tu utilises, tu ne peux pas satisfaire le reste.

Dossier complet, sources et détail par règlement : (lien vers l'article). Information générale, pas de conseil juridique individuel.