Balise

Êtes-vous en règle avec le RGPD et l'IA ?

Guide d'autodiagnostic gratuit, en 10 questions

Accompagné par Balise
Diagnostic indicatif, ne constitue pas un avis juridique. Contact : gildo@gildopandi.fr

Pourquoi maintenant

Le RGPD s’applique depuis 2018. Le règlement européen sur l’IA s’ajoute à lui : il s’applique dans sa quasi-totalité depuis le 2 août 2026.

Les échéances à retenir :

• Le RGPD (règlement (UE) 2016/679) s'applique depuis le 25 mai 2018.

• Le règlement européen sur l'IA (règlement (UE) 2024/1689, « AI Act ») s'applique dans sa quasi-totalité depuis le 2 août 2026, dont l'article 50 (informer qu'on échange avec une IA ; signaler les contenus réalistes générés par IA).

• Seule exception pour l'article 50 : le marquage lisible par machine des contenus générés par IA (paragraphe 2, obligation des fournisseurs) est reporté au 2 décembre 2026.

• L'article 4 du règlement sur l'IA, dans sa rédaction issue du règlement (UE) 2026/1744, impose aux fournisseurs et déployeurs de prendre des mesures pour favoriser le développement de la maîtrise de l'IA (obligation de moyens, applicable).

• Le volet RGPD de l'Omnibus n'est pas adopté : le registre des traitements et le délai de 72 heures de notification des violations sont inchangés.

• Les pratiques d'IA interdites (article 5) s'appliquent depuis le 2 février 2025.

• Le règlement « Digital Omnibus » (UE) 2026/1744 a reporté les obligations des systèmes d'IA à haut risque au 2 décembre 2027 (annexe III) et au 2 août 2028 (annexe I).

Les 8 domaines à vérifier

1. Inventaire des outils IA
2. Données personnelles dans les outils IA
3. Chatbots et contenus générés (article 50)
4. Registre des traitements et bases légales
5. Information des personnes, site web, cookies
6. Sous-traitants et transferts hors UE
7. Droits des personnes et violations de données
8. Sécurité, charte d'usage de l'IA et formation

10 questions pour vous situer

Répondez à chaque question. Si la réponse ressemble à l'exemple d'alerte, la piste d'action est indiquée juste en dessous.

Q01 · Inventaire des outils IA

Avez-vous une liste des outils d'IA utilisés dans l'entreprise ?

Exemple d'alerte : Une liste existe, mais elle n'est pas à jour

Piste d'action : Mettre à jour la liste en interrogeant chaque service, puis fixer une révision annuelle.

Q06 · Données personnelles dans les outils IA

Des salariés utilisent-ils des outils d'IA avec leurs comptes personnels ou gratuits pour leur travail ?

Exemple d'alerte : Oui, c'est toléré ou fréquent

Piste d'action : Fournir des comptes professionnels pour les usages utiles et interdire par écrit l'usage de comptes personnels avec des données de l'entreprise.

RGPD, art. 5(1)(f) et art. 32 ; art. 28 lorsque les données sont transmises à un prestataire

Q07 · Données personnelles dans les outils IA

Quelles données sont saisies dans les outils d'IA ?

Exemple d'alerte : Des données sensibles (santé, opinions, religion, origine, appartenance syndicale)

Piste d'action : Suspendre ces saisies jusqu'à vérification d'une exception applicable, de la sécurité de l'outil et de la nécessité d'une analyse d'impact.

RGPD, art. 9 et art. 35

Q11 · Chatbots et contenus générés (article 50)

Avez-vous un chatbot ou un assistant IA qui échange avec vos clients ou prospects (site web, messagerie, téléphone) ?

Exemple d'alerte : Oui, mais sans indication claire que c'est une IA

Piste d'action : Ajouter dès le premier message une mention du type « Vous échangez avec un assistant automatisé » et vérifier ce point avec l'éditeur du chatbot.

Règlement (UE) 2024/1689, art. 50(1)

Q13 · Chatbots et contenus générés (article 50)

Publiez-vous des images, vidéos ou voix réalistes générées ou modifiées par IA (visuels de personnes, voix de synthèse, montages) ?

Exemple d'alerte : Oui, sans mention

Piste d'action : Ajouter une mention visible « contenu généré par IA » sur les contenus concernés, y compris ceux déjà publiés.

Règlement (UE) 2024/1689, art. 50(4)

Q16 · Registre des traitements et bases légales

Avez-vous un registre des traitements de données personnelles ?

Exemple d'alerte : Oui, mais il n'est pas à jour ou n'inclut pas les outils d'IA

Piste d'action : Compléter le registre avec les traitements réalisés à l'aide d'outils d'IA et mettre à jour les autres fiches.

RGPD, art. 30

Q21 · Information des personnes, site web, cookies

Votre site web a-t-il une politique de confidentialité à jour ?

Exemple d'alerte : Oui, mais elle est ancienne ou ne parle pas de l'IA

Piste d'action : Mettre à jour la politique de confidentialité en décrivant les traitements réalisés avec des outils d'IA.

RGPD, art. 13

Q22 · Information des personnes, site web, cookies

Sur votre site, le bandeau cookies permet-il de refuser aussi facilement que d'accepter ?

Exemple d'alerte : Il y a un bandeau, mais refuser est plus compliqué qu'accepter

Piste d'action : Ajouter un bouton « Tout refuser » au même niveau et de même apparence que « Tout accepter ».

Loi n° 78-17 du 6 janvier 1978, art. 82

Q33 · Droits des personnes et violations de données

En cas de fuite, de piratage ou de perte de données, savez-vous que la CNIL doit être prévenue dans les 72 heures, et avez-vous une procédure ?

Exemple d'alerte : Nous connaissons le délai, mais il n'y a pas de procédure

Piste d'action : Rédiger une procédure d'une page : qui alerter, comment évaluer le risque, comment notifier la CNIL et informer les personnes.

RGPD, art. 33 et art. 34

Q36 · Sécurité, charte d'usage de l'IA et formation

Avez-vous une charte d'usage de l'IA qui fixe les règles pour les salariés ?

Exemple d'alerte : En cours de rédaction, ou règles seulement orales

Piste d'action : Finaliser une charte courte et la faire signer ou l'annexer au règlement intérieur.

Règlement (UE) 2024/1689, art. 4, dans sa rédaction issue du règlement (UE) 2026/1744

Et ensuite ?

Ce guide vous donne des repères, il ne remplace pas un diagnostic. Pour un état des lieux complet de votre entreprise, faites le diagnostic gratuit en 3 minutes : https://balise-rgpd.fr/diagnostic

Pour aller plus loin : l'Audit Flash analyse en détail les 40 questions de la grille et livre un rapport avec un plan d'action à 30, 60 et 90 jours.

Diagnostic indicatif, ne constitue pas un avis juridique.
Ce guide est établi à partir de la grille d'analyse de Balise. Il est indicatif et ne constitue pas un avis juridique. Balise accompagne les entreprises, sans se substituer à un conseil juridique.