GUIDE PRATIQUE · ÉDITION 2026

AI Act 2026 : gouverner, auditer et sécuriser vos systèmes d'IA

À destination des DPO, RSSI, Data Leaders et Responsables Formation

Mis à jour — août 2026 · Basé sur le Règlement (UE) 2024/1689, modifié par le Règlement (UE) 2026/1744 (Digital Omnibus)

ÉDITO

Le report n'est pas une pause, c'est une fenêtre

Le 2 août 2026 marque une nouvelle étape de l'AI Act, mais pas celle initialement prévue : les obligations de **transparence (Art. 50)** — étiquetage des chatbots, deepfakes et contenus générés par IA — entrent en application. En revanche, le règlement **Digital Omnibus (UE) 2026/1744**, entré en vigueur le 27 juillet 2026, a reporté l'application complète des systèmes « haut risque » (Annexe III) au **2 décembre 2027**.

Ce guide s'adresse à trois fonctions directement exposées — DPO, RSSI et Data Leaders — ainsi qu'aux Responsables Formation chargés de monter en compétences leurs équipes. Il est conçu pour être pratique, sourcé et directement actionnable : des obligations claires, un calendrier à jour, des étapes d'audit concrètes, et un plan de formation calibré par profil.

LE CALENDRIER À JOUR

Le calendrier AI Act en un coup d'œil

Date	Ce qui s'applique
1er août 2024	Entrée en vigueur du Règlement (UE) 2024/1689
2 février 2025	Interdiction des pratiques d'IA à risque inacceptable (Art. 5) — **déjà sanctionnable**. Littératie IA obligatoire (Art. 4) — **applicable dès cette date**, et non août 2025.
2 août 2025	Désignation des autorités nationales compétentes + obligations GPAI (modèles fondation)
27 juillet 2026	**Entrée en vigueur du Digital Omnibus (UE) 2026/1744** — révision du calendrier d'application
2 août 2026	**Obligations de transparence (Art. 50)** : chatbots, agents conversationnels, deepfakes et contenus générés par IA doivent être clairement identifiés. Délai de transition jusqu'au 2 décembre 2026 pour les systèmes déjà commercialisés.
2 décembre 2027	**Application complète des systèmes haut risque Annexe III** : documentation technique, gestion des risques, gouvernance des données, supervision humaine.
2 août 2028	Application des règles liées à l'Annexe I pour les systèmes d'IA intégrés dans des produits réglementés (dispositifs médicaux, machines, jouets).

> **Point d'attention —** la littératie IA (Art. 4) et l'interdiction des pratiques inacceptables (Art. 5) sont déjà en vigueur depuis le 2 février 2025. Ne pas attendre 2027 pour démarrer votre audit interne : l'obligation de formation renforce directement l'urgence du segment Formation/RH.

CLASSIFICATION

Les 4 niveaux de risque

Niveau	Définition	Exemples sectoriels
Risque inacceptable	Interdit — pratiques incompatibles avec les droits fondamentaux	Scoring social, manipulation subliminale, reconnaissance émotionnelle en milieu professionnel (hors exceptions)
Haut risque — Annexe III	Autorisé mais soumis à obligations strictes (Art. 9 à 15) — pleinement applicable au 2 décembre 2027	Outil de recrutement IA, scoring crédit, diagnostic médical IA, contrôle d'accès biométrique
Risque limité	Obligations de transparence uniquement — applicable au 2 août 2026	Chatbot, générateur de contenu, deepfake à usage créatif
Risque minimal	Aucune obligation spécifique AI Act	Filtre anti-spam, recommandation de playlist, IA de jeu vidéo

Comment qualifier votre système ? Le critère déterminant est l'usage : un outil RH qui trie des CV et influence une décision d'embauche est classé haut risque Annexe III, quel que soit son niveau technique — et même si l'échéance d'application complète est désormais 2027, mieux vaut anticiper.

GOUVERNANCE DES DONNÉES

L'Article 10 décrypté

L'article 10 impose aux fournisseurs de systèmes d'IA haut risque des obligations précises sur la qualité et la gouvernance des données d'entraînement, de validation et de test. Ces obligations deviendront pleinement opposables au 2 décembre 2027, mais leur mise en œuvre demande plusieurs mois de préparation — les anticiper dès maintenant reste recommandé.

Les 5 obligations concrètes

- **Origine et traçabilité :** documenter la source des données, les processus de collecte, et pour les données personnelles, la finalité initiale de collecte
- **Préparation et traitement :** encadrer les opérations d'annotation, d'étiquetage, de nettoyage et d'enrichissement
- **Détection et correction des biais :** examiner les données pour identifier les biais susceptibles d'affecter les droits fondamentaux ou de produire des discriminations
- **Représentativité statistique :** garantir que les jeux de données reflètent les populations cibles et les contextes d'usage réels
- **Identification des lacunes :** documenter les insuffisances de données et les mesures correctives envisagées

Ce que cela implique pour vos Data Engineers

L'article 10 n'est pas une simple formalité documentaire. Il impose une discipline opérationnelle sur chaque pipeline : traçabilité des versions, logs d'annotation, registres de biais détectés et corrigés. Les outils ETL et les notebooks de préparation doivent produire une documentation auditable.

Ce que cela implique pour votre DPO

L'article 10 croise directement le RGPD : finalité de collecte, minimisation, droits des personnes. Le DPO doit s'assurer que la DPIA existante couvre les nouvelles finalités liées à l'IA, et que le registre de traitements reflète les usages IA.

MÉTHODE

Checklist d'audit en 4 étapes

Même reportée à 2027 pour le haut risque, cette checklist reste la meilleure façon de se préparer sans attendre et d'être prêt bien avant l'échéance.

> **Deux cas à traiter explicitement :** les PME de moins de 750 salariés et 150 M€ de chiffre d'affaires peuvent bénéficier d'exigences documentaires allégées ; les systèmes déjà déployés auprès d'autorités publiques disposent d'un horizon spécifique jusqu'au 2 août 2030.

☐ Étape 1 — Cartographie des systèmes IA (SaaS inclus)

Avez-vous listé tous les outils intégrant une composante IA, y compris les solutions SaaS tierces (RH, CRM, sécurité) ? Savez-vous distinguer les systèmes où vous êtes fournisseur de ceux où vous êtes déployeur ?

☐ Étape 2 — Qualification du rôle (fournisseur / déployeur)

Modifiez-vous un modèle IA tiers pour un usage spécifique ? Pour les systèmes haut risque où vous êtes déployeur, avez-vous obtenu la documentation technique et la déclaration de conformité du fournisseur ?

☐ Étape 3 — Classification du niveau de risque

Le système figure-t-il dans l'Annexe III (recrutement, crédit, biométrie, infrastructure critique, éducation, justice, migration) ? Avez-vous documenté le raisonnement de la classification retenue ?

☐ Étape 4 — Gap analysis (documentation, Art. 9, Art. 10, logs, contrats)

Disposez-vous de la documentation technique requise (Art. 11) ? Le système de gestion des risques (Art. 9) est-il formalisé ? Les logs de supervision humaine sont-ils conservés pour la durée réglementaire ?

SANCTIONS

Le régime de sanctions

Niveau	Montant maximum	Infractions concernées
Niveau 1	**35 000 000 € ou 7 % du CA mondial**	Violation des pratiques interdites (Art. 5) — déjà applicable
Niveau 2	15 000 000 € ou 3 % du CA mondial	Non-conformité aux obligations des systèmes haut risque — opposable au 2 décembre 2027
Niveau 3	7 500 000 € ou 1 % du CA mondial	Fourniture d'informations inexactes, incomplètes ou trompeuses aux autorités compétentes

Ce qui est déjà sanctionnable aujourd'hui

Depuis le 2 février 2025, les pratiques interdites de l'article 5 sont pleinement sanctionnables (scoring social, manipulation subliminale, catégorisation biométrique à distance en temps réel dans les espaces publics). À compter du 2 décembre 2026, le Digital Omnibus ajoute une interdiction visant les systèmes d'IA générant des contenus intimes non consentis et du matériel pédocriminel. Si votre organisation déploie de tels systèmes, le risque juridique est immédiat — indépendamment du report des obligations haut risque.

GOUVERNANCE

Le rôle du DPO : périmètre et limites

Ce que le DPO apporte naturellement

- **Cartographie et registre :** l'habitude de recenser les traitements est directement transposable à l'inventaire des systèmes IA
- **DPIA → FRIA :** la méthodologie de la DPIA se transpose à la Fundamental Rights Impact Assessment exigée pour certains systèmes haut risque
- **Accountability :** la culture de documentation et de traçabilité du DPO est exactement ce que demande l'AI Act pour les systèmes haut risque

Ce qui dépasse son périmètre classique

- **Article 9 — Gestion des risques :** implique une évaluation technique de la fiabilité, de la robustesse et de la sécurité — compétence RSSI et technique
- **Article 10 — Documentation des données :** requiert une maîtrise des pipelines de données, des métriques de biais et des propriétés statistiques des jeux de données
- **Classification des systèmes :** la qualification du niveau de risque nécessite une lecture croisée technique/juridique que le DPO seul ne peut assumer

COMPÉTENCES ÉMERGENTES

Les 3 nouveaux rôles à former

Nos formations AI Act s'organisent en trois parcours : Gouverner — piloter la conformité et la gouvernance de l'IA. *Profil : DPO / Juriste conformité.* **Implémenter** — déployer et sécuriser un système de management de l'IA. *Profils : Data Leader et RSSI.* **Auditer** — évaluer la conformité et préparer un audit de certification. *Profil : Auditeur IA.*

Ces trois rôles ne correspondent pas à une formation unique du catalogue : ils se construisent en combinant des certifications existantes. Pour chacun, le parcours de formation associé est indiqué ci-dessous — et repris dans le plan de montée en compétences de la page suivante.

Data Steward IA

Tient à jour l'inventaire des jeux de données des systèmes IA haut risque, garantit la traçabilité de l'origine et des versions, pilote les revues de biais. Ancrage : Art. 10, Art. 11.

Comment le former : parcours **Implémenter** (voir ci-dessus) → profil **Data Leader** dans le plan de montée en compétences.

Auditeur de systèmes IA

Conduit les audits internes de conformité (gap analysis, tests de robustesse), vérifie la documentation technique et le système de gestion des risques. Ancrage : Art. 9, Art. 11, Art. 12.

Comment le former : parcours **Auditer** (voir ci-dessus) → profil **Auditeur IA** dans le plan de montée en compétences.

Référent Conformité IA

Coordonne le dispositif de conformité AI Act en transversal (DPO, RSSI, Métiers, Direction), anime le programme de littératie IA (Art. 4). Ancrage : Art. 4, coordination DPO/RSSI.

Comment le former : parcours **Gouverner** (voir ci-dessus) → profil **DPO / Juriste** dans le plan de montée en compétences

PLAN DE FORMATION

Plan de montée en compétences recommandé

Chaque profil actuel indique, le cas échéant, le rôle émergent qu'il permet de tenir (→)

Profil → rôle émergent	Parcours	Formation(s) recommandée(s)	Durée
DPO / Juriste *→ Référent Conformité IA*	Gouverner	AIGP + ISO/IEC 42001 Foundation	4 jours
RSSI	Implémenter	ISO/IEC 42001 F + LI, puis AAISM ou GK840108	6 à 8 jours
Data Leader *→ Data Steward IA*	Implémenter	ISO/IEC 42001 Foundation + Lead Implementer	6 jours
Auditeur IA *→ Auditeur de systèmes IA*	Auditer	ISO/IEC 42001 Foundation + Lead Auditor [+ AAIA]	6 à 8 jours
Resp. Formation	Transverse	EXIN BCS AI Essentials ou GKINTIA	1 jour

→ Consulter le catalogue complet des formations AI Act & gouvernance de l'IA

Global Knowledge vous accompagne dans cette transition

Se mettre en conformité avec l'AI Act n'est pas qu'une affaire de texte réglementaire — c'est une question de compétences à construire, souvent en combinant plusieurs certifications complémentaires. C'est précisément ce que nos formateurs font au quotidien depuis plus de 30 ans, aux côtés des équipes IT, cybersécurité et conformité.

Sur l'AI Act, nous couvrons l'ensemble du parcours — de la gouvernance à l'audit, en passant par la mise en œuvre opérationnelle — et pouvons vous accompagner dans le choix des formations les plus adaptées. Pour les entreprises éligibles membres d'OPCO Atlas, la formation GKINTIA peut éventuellement faire l'objet d'un financement dédié.

→ Une question sur votre propre niveau d'exposition ? Parlons-en.

SOURCES ET RÉFÉRENCES

- **Règlement (UE) 2024/1689** — Articles 4, 5, 9, 10, 11, 12, 50, 99 (Journal officiel de l'Union européenne)
- **Règlement (UE) 2026/1744** — « Digital Omnibus » sur l'IA, publié au JOUE le 24 juillet 2026, entré en vigueur le 27 juillet 2026
- **Calendrier officiel AI Act** — AI Act Service Desk, Commission européenne
- **CNIL** — Le DPO à l'heure de l'IA (mai 2026)