LE RÉCAP

AI Act européen : obligations pratiques pour une PME SaaS intégrant un LLM en 2026

Synthèse · approfondi

Document généré par IA

2026-07-28

AI Act européen : obligations pratiques pour une PME SaaS intégrant un LLM en 2026

Synthèse · approfondi

Sujet demandé : AI Act européen : obligations pratiques pour une PME SaaS qui intègre un LLM en 2026

Généré le 2026-07-28 · Le Récap

Document de synthèse opérationnelle pour une PME SaaS intégrant un LLM en 2026 sous le régime de l'AI Act. Il cartographie le périmètre juridique à jour (2024–2026), la catégorisation des LLM, les obligations concrètes et les jalons de mise en conformité, avec chiffres et sources primaires. La dernière section met en lumière les controverses et points d'attention stratégiques.

1. Résumé exécutif — constats clés

À compter du 2 août 2026, les obligations transversales de transparence (chatbots, contenus générés, deepfakes, émotion/biométrie) s'appliquent à large échelle, y compris aux PME SaaS qui déploient des LLM dans l'UE, avec une courte grâce ciblée pour le marquage des contenus déjà sur le marché avant cette date [30][31][32]. Les systèmes à haut risque voient leurs échéances étagées jusqu'au 2 décembre 2027 (Annexe III) et au 2 août 2028 (Annexe I, produits réglementés), à la suite du « Digital/AI Omnibus » adopté en 2026 [31][32][4].

- Périmètre et calendrier: AI Act en vigueur depuis le 1er août 2024; application générale dès le 2 août 2026; prohibitions applicables depuis le 2 février 2025; règles GPAI dès le 2 août 2025; transparence dès le 2 août 2026; haut risque décalé à 2027/2028 [2][5][6][30][31].
- Risque financier: amendes jusqu'à 7% du CA mondial ou 35 M€ pour pratiques interdites; barème dégressif pour autres manquements, avec plafond SME spécifique [1][14].
- GPAI/LLM: seuil de présomption de « risque systémique » à 10^25 FLOP; notification à la Commission; obligations accrues (évaluations, sécurité, résilience, résumé public de l'entraînement via le gabarit 2025) [50][7][8][9].
- Transparence (Art. 50): divulgation d'interaction homme-IA (chatbots), marquage machine-lisible des contenus générés/manipulés, signalement des deepfakes; grâce technique limitée pour le marquage de certains systèmes déjà sur le marché avant le 2 août 2026 [30][31][32].
- Évaluation de conformité: pour haut risque (Annexes I/III), auto-évaluation basée sur Annexe VI ou évaluation par organisme notifié (Annexe VII); dossier technique Annexe IV; enregistrement base UE (Art. 71) selon cas [33][1][16].

- Post-marché: plan et système de surveillance (Art. 72); signalement des incidents graves dans les 15 jours (délais plus courts en cas de décès/infractions massives) [34][35].
- Inter-cadres: articulation avec RGPD/EDPB, DSA, Data Act (accès/switching cloud/interop.), CRA, NIS2 et réglementation sectorielle (MDR, Machinery, etc.) — convergence mais complexité pour PME [10][11][15][16][17][18][46][47].
- Standards/harmonisation: programme CEN-CENELEC JTC 21; premières livraisons attendues 2026; ISO/IEC 42001 et NIST AI RMF comme trames de gouvernance complémentaires (sans présomption de conformité AIA) [20][21][22][23].
- Charge estimée: l'IA Act (évaluation d'impact 2021) estimait des coûts fixes additionnels par système haut risque de 6–7 k€, plus 3–7,5 k€ pour la conformité; le paquet Omnibus 2025–2026 vise des allégements ciblés pour PME (p. ex. documentation) [15][31].
- Assurance et responsabilité: refonte de la directive sur la responsabilité du fait des produits adoptée en 2024; le marché cyber/E&O évolue vite avec des lacunes de couverture AI spécifiques; D&O sous tension [26][43][44][10].

Recommandations prioritaires 2026 (PME SaaS LLM)

- Cartographier l'usage des LLM par cas d'usage et publics exposés; assigner le niveau de risque (interdit/haut risque/transparence) par finalité; décider si GPAI (et si « systémique ») [1][5][6][50].
- Déployer un dispositif « Article 50-ready »: détection/marquage machine-lisible de génération (texte/son/image/vidéo), disclosure chatbots, gestion deepfakes; vérifier la grâce limitée [30][31][32].
- Mettre en place une gouvernance de conformité AI: AIMS (ISO/IEC 42001), registre des modèles, QMS/RMS AIA (Annexe IV/VI), revue sécurité/robustesse, logs/trace (Art. 12/Annexe IV) [23][1][33].

- Pour GPAI/LLM: publier le résumé d'entraînement selon le gabarit 2025; politique TDM opt-out et copyright; gestion des droits; cartographie domaines/datasets [8][9][18].
- Préparer PMM et incident-reporting: plan Art. 72, procédures de remontée à l'autorité de surveillance nationale; tests de crise « dry-run » [34][35][36].
- Contractualiser la chaîne d'approvisionnement: DPA RGPD (Art. 28), annexes AI Act (obligations techniques/perf. et transparence), SLA sécurité/DR, droits d'audit, désengagement cloud (Data Act) [11][15][39][41].
- Sécuriser via référentiels: NIST AI RMF (MAP/MEASURE/MANAGE), ISO/IEC 42001 (AIMS) et futurs standards JTC 21 (présomption de conformité quand au JOUE) [22][23][20].
- Planifier l'enregistrement (Art. 71) et l'évaluation de conformité (module interne vs organisme notifié) selon périmètre; surveiller les actes d'exécution/guides Commission [16][31][33].
- Budgeter 12–24 mois: 0,5–1,5 ETP conformité/AI safety; 30–120 k€ d'intégration (marquage, journaux, tests red teaming, doc), modulé par risque/maturité [15][22][31].
- Couvrir le risque résiduel: ajuster polices cyber/E&O/média/D&O; vérifier exclusions IA; envisager garanties AI dédiées [43][44].

> *« Non-compliance with Article 5 may reach EUR 35,000,000 or 7% of worldwide turnover. »*
>
> — AI Act, Article 99 (2024) [1]

Message clé: en 2026, une PME SaaS intégrant un LLM doit prioriser la conformité Art. 50, la gouvernance AIMS/QMS et la traçabilité, tout en planifiant le haut risque pour 2027/2028 [30][31][32][33].

2. Contexte réglementaire et périmètre d'application (mise à jour 2024–2026)

L'AI Act (Règlement (UE) 2024/1689) est publié au JOUE le 12 juillet 2024 et entré en vigueur le 1er août 2024. Il s'applique de manière échelonnée jusqu'en 2028; les prohibitions s'appliquent dès le 2 février 2025; l'essentiel des obligations générales s'applique à partir du 2 août 2026 [1][2][4]. Le « Digital/AI Omnibus » adopté en 2025–2026 ajuste des échéances et clarifie l'articulation sectorielle (Annexe I) et certaines procédures (sandboxes, enregistrements), notamment en repoussant l'application des règles haut risque (Annexe III au 2 décembre 2027; Annexe I au 2 août 2028) [31][4] [32].

Architecture: approche par risque (interdit, haut risque, obligations GPAI, transparence), appuyée par la normalisation (CEN-CENELEC JTC 21) et la présomption de conformité via normes harmonisées au JOUE (Art. 40). La gouvernance s'articule autour de l'AI Office (décision de création janvier 2024), du Board et des autorités nationales de surveillance (MSA), avec pouvoirs renforcés pour GPAI et coordination des évaluations/contrôles [1] [20][25][36][37].

Périmètre territorial/matériel: le règlement s'applique aux fournisseurs et déployeurs qui placent/emploient des systèmes IA sur le marché de l'UE, indépendamment du siège. Les LLM/GPAI sont soumis à des obligations spécifiques (Art. 53–56) et, s'ils sont utilisés dans des cas d'usage Annexe III (p. ex. emploi, éducation, services essentiels), l'application devient « haut risque » avec évaluation de conformité et enregistrement (Art. 71) [1][5][6] [16].

Textes connexes et articulation

- RGPD et autorités: l'EDPB rappelle la cohérence RGPD/AI Act et précise l'usage des données pour développement/déploiement des modèles; CNIL

publie Q&R et recommandations pratiques (LLM, sous-traitance, sécurité) [10][11][12][13].

- Data Act: accès/portabilité des données, switching des services de traitement (cloud), interopérabilité des espaces de données et smart contracts; application principale depuis le 12 septembre 2025 (échéanciers additionnels pour switching) [15][39][41].
- DSA: obligations des plateformes et VLOP/VLOSE; utile si l'application SaaS inclut des fonctions d'hébergement/distribution de contenus générés par IA [16].
- Cyber Resilience Act (CRA): exigences sécurité-by-design pour produits à éléments numériques; complémentarité avec exigences robustesse/ sécurité de l'AI Act [17].
- NIS2: durcissement cybersécurité pour secteurs essentiels/ importants; transposition nationale hétérogène en 2024–2026, ce qui ajoute une couche de conformité variable selon pays [18].
- Réglementation sectorielle: MDR (logiciels DM, guidances 2025), Machinery (applicable 20/01/2027) — mécanisme d'articulation avec l'AI Act via Annexe I et procédures d'évaluation combinées [46][47][31].

Chiffres et jalons: l'UE confirme les règles GPAI au 2 août 2025, la transparence au 2 août 2026 (avec grâce ciblée), la base de données haut risque (Art. 71) et les sandboxes (Art. 57) avec un calendrier réaliste 2026–2027. Les sanctions atteignent 35 M€/7% pour pratiques interdites [6][30][31][32][33][48].

> *« The first harmonised standards are expected to be published by CEN and CENELEC in 2026. »*
>
> — Commission, AI Act standardisation FAQs (2026) [20]

> Zone d’incertitude 2026: disponibilité des normes harmonisées et outillage (gabarits, guides), et mise en service effective de la base UE Art. 71; suivre les mises à jour Commission/Conseil [20][31][32].

3. Catégorisation des LLM et conséquences juridiques

Un LLM peut relever de quatre régimes: (i) interdit (si l'usage correspond à une pratique prohibée, p. ex. manipulation cognitive/biométrie interdite), (ii) haut risque si utilisé dans une finalité Annexe III (ex. recrutement, éducation, allocation de services essentiels), (iii) GPAI (modèle d'usage général) et, le cas échéant, GPAI « risque systémique » au-delà d'un seuil de calcul, (iv) obligation de transparence (Art. 50) pour interactions directes et contenus générés, même si non haut risque [1][30][50].

GPAI/LLM et « risque systémique »

Les modèles d'usage général (GPAI) doivent : documenter et publier un résumé « suffisamment détaillé » des données d'entraînement (gabarit adopté en juillet 2025), mettre en œuvre des contrôles de sécurité/robustesse et, pour les modèles à risque systémique, conduire des évaluations renforcées et notifications. La présomption de « high impact capabilities » est fixée à 10^25 FLOP cumulés d'entraînement; la Commission peut désigner en-dessous selon critères d'Annexe XIII (évaluations, échelle d'usage, outillage accessible, etc.) [8][9][7][50].

Conséquences pratiques pour une PME SaaS: si vous intégrez un LLM tiers (API/hosté), vous êtes en général « déployeur ». Vos obligations varient selon finalité: un assistant interne client-support impose transparence (Art. 50) et mesures RGPD; un outil de présélection candidats basculera en haut risque (Annexe III, emploi) avec obligations renforcées (QMS/RMS, documentation Annexe IV, enregistrement, évaluation de conformité) [1][30][16].

Pratiques interdites et jurisprudence/autorités

Les pratiques interdites (Art. 5) exposent à des amendes jusqu'à 35 M€/7% [1]. Les autorités de protection des données ont déjà pris des positions structurantes vis-à-vis des LLM: l'EDPB précise les principes d'usage des données pour modèles; la CNIL publie des recommandations; en Italie,

l’affaire ChatGPT a illustré la dynamique contentieuse et l’ajustement des mesures au fil des mois (dont une décision judiciaire de 2026) [11][13][27][28].

Controverses et zones grises (2026)

- Seuil 10^25 FLOP: jugé pratique mais critiqué (risque d’optimisation stratégique; corrélation imparfaite avec capacités/risques). Débats académiques et revues sectorielles persistent [7][24][51].
- Définition des « deepfakes » et frontières éditoriales: précisions Commission en cours; articulation avec exceptions éditoriales et contexte artistique [30][31].
- Portée exacte des obligations des déployeurs intégrant des LLM tiers (journalisation, explicabilité, contrôle humain) hors haut risque: interprétations à clarifier via guides et normes [1][20].

> Règle opérationnelle: classer par finalité d’usage et exposition risques; vérifier si l’usage tombe dans Annexe III; sinon, appliquer Art. 50 et RGPD a minima; si GPAI « systémique », anticiper obligations accrues [1][6][30][50].

4. Obligations opérationnelles clés pour une PME SaaS intégrant un LLM

Transparence (Art. 50) et expérience utilisateur

Dès le 2 août 2026: (i) divulguer l'interaction avec un système IA (chatbots/assistants), (ii) marquer de manière détectable/machine-lisible les contenus générés/manipulés, (iii) signaler distinctement les deepfakes (avec exceptions encadrées), (iv) informer pour l'émotion/biométrie (si licite). Une grâce technique limitée existe pour le marquage de certains systèmes déjà sur le marché avant le 2 août 2026 (jusqu'au 2 décembre 2026) [30][31][32].

Données d'entraînement, copyright et TDM

Fournisseurs de GPAI: publier un résumé d'entraînement conforme au gabarit 2025 (sources, périodes, domaines, jeu synthétique/IA, etc.). La conformité copyright repose sur les exceptions TDM (Directive 2019/790) avec opt-out machine-lisible des ayants droit; la Commission étudie un registre TDM centralisé (2026). Les déployeurs doivent auditer la chaîne d'approvisionnement (licences/droits, opt-out respectés) [8][9][18].

Documentation, registre et conformité

Pour haut risque: dossier technique (Annexe IV), QMS/RMS (Annexe VI/VII), enregistrement dans la base UE (Art. 71) lorsque requis, instructions d'usage et surveillance post-marché (Art. 72), évaluation de conformité (module interne vs organisme notifié). Pour non-haut-risque: documentation proportionnée (logs, données, tests, limites), politiques de transparence et de sûreté [1][16][33][34].

Sécurité/robustesse et surveillance post-marché

Mettre en place un PMM (plan + système) pour collecter et analyser des signaux en vie réelle (drift, biais, dégradations). Déclarer tout incident grave

aux autorités dans les 15 jours (ou plus court selon gravité). Synchroniser avec RGPD (DPIA/violations), NIS2 (incidents), CRA (vulnérabilités) [34][35][17][18].

Charges et chiffrages indicatifs (PME)

- Coûts fixes par système haut risque: 6–7 k€ (obligations), 3–7,5 k€ (conformité), selon l'IAE Commission (2021); Omnibus 2025–2026 vise des réductions ciblées (documentation, PME) [15][31].
- Investissements 2026 Art. 50: détection/marquage, UI/UX disclosure, pipelines watermarking, MRM/QA — 20–60 k€ pour une intégration LLM dans une app SaaS moyenne (ordre de grandeur; dépend fortement du scope) [22][30][31].
- GPAI résumé d'entraînement: extraction de métadonnées et revue juridique/copyright — 5–20 k€ (selon complexité/volumétrie), plus coûts de gouvernance continue [8][9][18].
- PMM/Incident reporting: instrumentation, alerting, procédures et formation — 10–30 k€ + 0,2–0,5 ETP [34][35][22].

> *« Providers must ensure that their AI systems meet the transparency obligations … before placing those systems on the market. »*
>
> — Commission, Transparency under Article 50 (2026) [30]

> Conseil: aligner votre outillage interne sur NIST AI RMF (MAP-MEASURE-MANAGE) et ISO/IEC 42001, en anticipant les normes harmonisées JTC 21 pour activer la présomption de conformité dès leur publication au JOUE [22][23][20].

5. Gouvernance interne, gestion des risques et conformité (conformity assessment)

Modèle de gouvernance (PME SaaS)

- Rôles: Product Owner (cas d'usage/classification), Tech Lead (sécurité/robustesse), AI Safety/Compliance Lead (QMS/RMS, Annexe IV), DPO (RGPD), Sécurité (NIS2/CRA), Juridique/Contrats.
- Comité IA (mensuel): arbitrages risques, trajectoires de conformité, suivi incidents/PMM, évolution du périmètre et substantial modifications (identité du système au fil des versions) [34][18].
- Politiques: cycle de vie données (ingestion/finetune/inférence), explicabilité/limites, red teaming, dataset governance, copyright/TDM, sandbox si pertinent [8][9][48][49].

Méthodes AIA/TRA et métriques

Méthodologiquement, l'adossement à NIST AI RMF 1.0 (cartographier, mesurer, gérer) et à une AIMS (ISO/IEC 42001) offre une trame d'auditabilité et d'amélioration continue, tout en anticipant les normes harmonisées 2026. Indicateurs: robustesse (taux d'erreur par classe), biais (différentiels), sécurité (résilience aux prompt injections/data poisoning), gouvernance données (traçabilité, TDM opt-out), performance produit (SLA/UX) [22][23][20].

Conformity assessment (modules) et preuves

Pour haut risque Annexe III (standalone): procédure interne Annexe VI quand les normes harmonisées couvrent l'ensemble des exigences; sinon, organisme notifié (Annexe VII) avec évaluation du QMS et du dossier technique. Pour Annexe I (produits réglementés), combinaisons avec les procédures sectorielles. Dans tous les cas: preuves documentaires (Annexe IV), instructions d'utilisation, enregistrement (Art. 71) si applicable [33][16][1].

Post-marché: PMM obligatoire (Art. 72) avec plan détaillé (gabarit d'exécution par acte d'exécution annoncé), remontée incidents (Art. 73) et mécanismes correctifs (mises à jour, retraits). Synchroniser RGPD (DPIA, droits), NIS2 (incidents), CRA (coordination vulnérabilités) [34][35][17][18].

> *« The first harmonised standards are expected to be published by CEN and CENELEC in 2026. »*
>
> — Commission, AI Act standardisation FAQs (2026) [20]

> Point d'attention: l'identité du système (quand une mise à jour constitue une « modification substantielle ») est un enjeu de traçabilité et de re-conformité. Documenter versioning, data lineage, et contrôles d'équivalence [18][34].

6. Aspects contractuels, responsabilité et assurances

Clauses à intégrer dans la chaîne (modèle/infra/intégration)

- Transparence/usage: disclosed use d'IA (Art. 50), limites et scénarios non couverts, droits sur prompts/contenus générés, politiques de marquage, obligations de non contournement TDM opt-out [30][18].
- Protection des données: DPA RGPD (Art. 28), transferts, privacy-by-design, logs/traçabilité (durées, sécurité), DPIA partagée quand pertinent (emploi/éducation) [11][12][13].
- Sécurité/QMS: exigences CRA-like (gestion vulnérabilités, SBOM si applicable), NIS2 (notification), red teaming/évaluations régulières; métriques de performance/sûreté annexées [17][18].
- Droits d'audit et information: accès aux informations techniques nécessaires au respect AI Act (Annexe IV), aux résumés d'entraînement GPAI et aux rapports d'incidents (Art. 73) [8][33][35].
- Réversibilité cloud (Data Act): clauses de switching (90 jours max. de transition, suppression données, assistance), interopérabilité (standards, export formats) [41][39].

Responsabilité civile et pénale potentielle

La directive responsabilité produits (2024) modernisée couvre les produits défectueux y compris logiciels, avec incidences sur la chaîne (fournisseur modèle, intégrateur, déployeur). L'initiative sur la responsabilité IA non-contractuelle de 2022 a été retirée en 2025, laissant aux droits nationaux le soin de combler certaines lacunes (faute/préjudice/causalité), ce qui accroît la valeur des clauses d'allocation de risques et de la gouvernance probatoire (logs/PMM) [26][11].

Assurances: état du marché (2025–2026) et stratégie PME

Le risque IA monte dans les baromètres; des lacunes persistent entre cyber/E&O/média/D&O et les expositions IA (hallucinations, biais, IP, dérives agents). Les assureurs et réassureurs publient des cadres; les autorités prudentielles attirent l'attention sur les risques d'accumulation et les ambiguïtés de couverture. Recommandations: revue des exclusions IA, endossements spécifiques (génération/IA agents), scénarios de sinistres, et alignement avec contrôles AI Act (traçabilité, PMM) [43][44].

> *« AI rose from 10th place worldwide in 2025 to 2nd place in 2026 »*
> — Allianz Risk Barometer 2026 (2026) [43]

> Aligner contrats et assurance sur la réalité technique (LLM tiers vs modèle finetuné), l'observabilité (logs), et les processus (PMM, red teaming), pour démontrer diligence raisonnable et réduire l'aléa moral [33][34][35].

7. Mise en œuvre opérationnelle : feuille de route et check-list 12–24 mois

Feuille de route priorisée (T0 = août 2026)

Trimestre	Livrables clés	Repères & sources
T-1 à T0 (mai–août 2026)	Cartographie usages LLM; classification (Annexe III/Art. 50/GPAI); plan Art. 50 (disclosure/marquage); gap analysis doc (Annexe IV) et sécurité	Art. 50; AI Act; Omnibus; NIST/ ISO [1][30][31][22] [23]
T0–T+1 (août–nov. 2026)	Déploiement marquage machine-lisible; politiques deepfakes; MRM/QA; PMM draft; contrats fournisseurs (DPA, clauses AI/Data Act switching)	Transparence; Data Act; PMM [30][39] [34][41]
T+2–T+3 (déc. 2026–mars 2027)	Tests red teaming; procédures incidents (Art. 73); préparation enregistrement Art. 71 (si haut risque) ; plan sandbox (si applicable)	Art. 71/72/73; Sandboxes [33][34] [35][48][49]
T+4–T+6 (avril–sept. 2027)	Évaluation de conformité (Annexe VI/VII) pour cas Annexe III; intégration normes harmonisées (lors publication) ; audit interne AIMS (ISO 42001)	JTC 21; Conformité [20][21][23][33]
T+7–T+8 (oct. 2027–janv. 2028)	Enregistrement EU DB (si requis); go-live haut risque Annexe III (2 déc. 2027); durcir PMM/assurance	Calendrier Omnibus [31][32]
T+9–T+12 (fév.–août 2028)	Alignement Annexe I (si concerné) ; consolidation conformité et post-marché ; bilan et itérations	Annexe I (2 août 2028) [31][47]

Check-list actionnable (CTO/GC/DSI)

- CTO: pipeline de marquage (texte/image/son/vidéo); observabilité (logs Art. 12), garde-fous prompts; inventaire modèles et versions; plans PMM/incidents [30][34].
- GC: matrices de classification (Annexe III/Art. 50); DPA RGPD; annexes AI Act dans contrats; alignement Data Act (switching/cloud); disclaimer IA dans CGU [16][39][41].
- DSI/CISO: cartographie actifs et flux; politique CRA-like; NIS2 (si secteur); processus vulnérabilités; tests red teaming; sauvegardes et reprise [17][18].
- Produit: UX disclosure cohérente; messages de contexte et limites; étiquetage deepfakes sans gêner l'usage légitime; retours utilisateurs [30][31].
- Data/AI: dataset governance; copyright/TDM; résumé d'entraînement (si GPAI); échantillons d'audit; biais/robustesse; éval. sécurité [8][9][22].

Ressources et coûts (ordre de grandeur, PME 50–150 ETP)

- Ressources: 0,5–1,5 ETP compliance/AI safety; 0,2–0,5 ETP sécurité; budget T1–T3: 40–120 k€ (Marquage/UX, observabilité, PMM, red teaming, documentation) [15][22].
- Évaluations externes (si organisme notifié): 15–60 k€ selon portée; sandbox: coûts variables (souvent subventionnés) [33][49].
- Assurance: ajustements primes/endossements selon exposition; risque IA en progression forte (baromètres 2026) [43][44].

> Financement/outillage: suivre les guides Commission (transparence, GPAI), la publication des normes JTC 21, et mobiliser les programmes UE (Digital Europe/Horizon) [6][20].

8. Points de vigilance, controverses et perspectives

Zones d'incertitude (été 2026)

- Normes harmonisées: publication en 2026 annoncée, mais couverture partielle probable; nécessité d'aligner AIMS (ISO/IEC 42001) et AI RMF en attendant la présomption de conformité [20][23][22].
- Base UE (Art. 71) et sandboxes (Art. 57): montée en régime 2026–2027; modalités pratiques (formats, interop.) encore en cours d'outillage [48][49].
- Compute threshold (10^25 FLOP): débats sur pertinence et possibilités d'évitement; possible révision/compléments par la Commission [7][24][51].
- Copyright/TDM: incertitudes d'opposabilité et de traçage des opt-out; étude Commission 2026 pour un registre centralisé [18].
- Enforcement: mosaïque nationale (MSA) et rôle AI Office (GPAI); risque d'hétérogénéité, comme aux débuts du RGPD [36][37].

Écoles de pensée (2024–2026)

- « Régulation par capacités » (compute/évals): lisible/opérationnelle, mais critiquée pour mé-ciblage des risques réels (contextuels et usages) [7][24][51].
- « Régulation par usages »: focalisation Annexe III/Art. 50, favorable aux PME déployant des LLM non-critiques, mais dépend de l'effectivité des contrôles et de l'éducation des acteurs [1][30].
- « Normalisation d'abord »: accélérer JTC 21 et reconnaître ISO/IEC 42001; risque de « compliance theatre » si les métriques/évals IA restent immatures [20][23][22].

Scénarios 12–24 mois (plausibles)

- Consolidation technique de l'Art. 50: diffusion d'outils de marquage multimodal, guides Commission et code(s) de pratique (transparence) — pression accrue sur les éditeurs LLM/API [30][31].
- Normes JTC 21 référencées au JOUE: présomption de conformité partielle pour haut risque; montée des évaluations par organismes notifiés [20][33].
- Assurance AI: émergence de polices ciblées (agents IA, hallucinations, IP) et d'agrégats; exigences de traçabilité (PMM/logs) comme prérequis assurantiel [43][44].
- Inter-cadres: harmonisation progressive Data Act (switching/interop.), DSA (modération de contenus IA), CRA (secure-by-design) [39][16][17].

Pour une PME SaaS, la stratégie gagnante reste pragmatique: se mettre « Article 50-ready » d'ici août 2026; bâtir une AIMS légère mais auditable; anticiper haut risque 2027/2028 pour les cas sensibles; contractualiser la chaîne; et institutionnaliser PMM/incidents. L'état de l'art évolue vite; suivre les pages Commission (GPAI, transparence), les publications CEN-CENELEC et les autorités (EDPB/CNIL) est essentiel [30][6][20][10][12].

Sources

Sources consultées et citées dans le document (URLs vérifiées à la génération).

1. Regulation (EU) 2024/1689 (Artificial Intelligence Act) – Official Journal (EUR-Lex, 2024-07)
   https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=en
2. AI Act enters into force (European Commission, 2024-08)
   https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_en
3. Timeline for the Implementation of the EU AI Act (AI Act Service Desk (European Commission), 2026-07)
   https://ai-act-service-desk.ec.europa.eu/en/ai-act/eu-ai-act-implementation-timeline
4. Timeline - Artificial intelligence (Council of the EU, 2026-07)
   https://www.consilium.europa.eu/en/policies/artificial-intelligence-act/timeline-artificial-intelligence/
5. AI Act | Shaping Europe's digital future (European Commission, 2026-07)
   https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
6. General-purpose AI obligations under the AI Act (European Commission, 2025-08)
   https://digital-strategy.ec.europa.eu/en/factpages/general-purpose-ai-obligations-under-ai-act
7. General-Purpose AI Models in the AI Act – Questions & Answers (European Commission, 2025-07)
   https://digital-strategy.ec.europa.eu/en/faqs/general-purpose-ai-models-ai-act-questions-answers
8. Drawing-up a General-Purpose AI Code of Practice – Template for training data summary (European Commission, 2025-07)
   https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice
9. Commission publishes guidelines for providers of general-purpose AI models (European Commission, 2025-07)
   https://digital-strategy.ec.europa.eu/en/news/commission-publishes-guidelines-providers-general-purpose-ai-models

10. Statement 3/2024 on DPAs' role in the AI Act framework (EDPB, 2024-07)
https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf

11. EDPB opinion on AI models: GDPR principles support responsible AI (EDPB, 2024-12)
https://www.edpb.europa.eu/news/edpb-opinion-on-ai-models-gdpr-principles-support-responsible-ai_en

12. Les questions-réponses de la CNIL sur l'utilisation d'un système d'IA générative (CNIL, 2024-07)
https://www.cnil.fr/fr/les-questions-reponses-de-la-cnil-sur-lutilisation-dun-systeme-dia-generative

13. IA : la CNIL publie ses premières recommandations sur le développement des systèmes d'intelligence artificielle (CNIL, 2024-04)
https://cnil.fr/fr/ia-la-cnil-publie-ses-premieres-recommandations-sur-le-developpement-des-systemes-dintelligence

14. Article 99: Sanctions (AI Act Explorer) (AI Act Service Desk (European Commission), 2024-07)
https://ai-act-service-desk.ec.europa.eu/fr/ai-act/article-99

15. Rules on fair access to and use of data (Data Act) — Summary (EUR-Lex (Summaries), 2024-01)
https://eur-lex.europa.eu/EN/legal-content/summary/rules-on-fair-access-to-and-use-of-data-data-act.html

16. The enforcement framework under the Digital Services Act (European Commission, 2026-07)
https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement

17. Cyber Resilience Act — Summary of the legislative text (European Commission, 2026-01)
https://digital-strategy.ec.europa.eu/en/policies/cra-summary

18. Commission calls on 23 Member States to fully transpose NIS2 (European Commission, 2024-10)

https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive

19. ENISA Threat Landscape 2024 (July 2023 – June 2024) (ENISA / Publications Office, 2024-10)
https://op.europa.eu/en/publication-detail/-/publication/e71394ea-85f0-11ef-a67d-01aa75ed71a1/language-cs

20. Understanding the standardisation of the AI Act (FAQs) (European Commission, 2026-06)
https://digital-strategy.ec.europa.eu/en/faqs/understanding-standardisation-ai-act

21. CEN-CENELEC decision to accelerate AI standards (JTC 21) (CEN-CENELEC, 2025-10)
https://www.cencenelec.eu/news-events/news/2025/brief-news/2025-10-23-ai-standardization/

22. NIST AI RMF Playbook (NIST, 2023-03)
https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook

23. ISO/IEC 42001:2023 — Artificial intelligence — Management system (ISO/IEC, 2023-12)
https://www.iso.org/standard/42001

24. Navigating the European Union Artificial Intelligence Act for Healthcare (npj Digital Medicine (Nature), 2024-08)
https://www.nature.com/articles/s41746-024-01213-6

25. Commission Decision of 24 January 2024 establishing the European Artificial Intelligence Office (EUR-Lex, 2024-01)
https://eur-lex.europa.eu/eli/C/2024/1459/oj/eng/pdf

26. Directive (EU) 2024/2853 — Product Liability Directive (OJ publication) (EUR-Lex, 2024-11)
https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A32024L2853

27. EDPB ChatGPT Taskforce — Report of the work undertaken (EDPB, 2024-05)
https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf

28. ChatGPT, Garante privacy — update noting 2026 court ruling (Garante per la protezione dei dati personali, 2026-03)
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085432

29. Rapport annuel 2025 (CNIL, 2026-05)
https://www.cnil.fr/sites/default/files/2026-05/rapport_annuel_2025.pdf

30. Transparency obligations under Article 50 of the AI Act (FAQs) (European Commission, 2026-07)
https://digital-strategy.ec.europa.eu/en/faqs/transparency-obligations-under-article-50-ai-act

31. Artificial intelligence: Council gives final green light to simplify and streamline rules (AI Omnibus) (Council of the EU, 2026-06)
https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/pdf/

32. AI Omnibus enters into force (European Commission, 2026-07)
https://digital-strategy.ec.europa.eu/en/news/ai-omnibus-enters-force

33. Article 43: Conformity assessment (AI Act Service Desk (European Commission), 2026-07)
https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-43

34. Article 72: Post-market monitoring by providers (AI Act Service Desk (European Commission), 2026-07)
https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-72

35. Article 73: Reporting of serious incidents (AI Act Service Desk (European Commission), 2026-07)
https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-73

36. Market Surveillance Authorities under the AI Act (European Commission, 2025-09)
https://digital-strategy.ec.europa.eu/en/policies/market-surveillance-authorities-under-ai-act

37. Governance and enforcement of the AI Act (European Commission, 2026-07)
https://digital-strategy.ec.europa.eu/en/policies/ai-act-governance-and-enforcement

38. Regulation (EU) 2022/868 (Data Governance Act) — Official Journal (EUR-Lex, 2022-06)
https://eur-lex.europa.eu/eli/reg/2022/868/oj?locale=en

39. Data Act | Shaping Europe's digital future (European Commission, 2026-07) https://digital-strategy.ec.europa.eu/en/policies/data-act

40. Results of the study on interoperability of data processing services (Data Act, Art. 35) (European Commission, 2026-02) https://digital-strategy.ec.europa.eu/en/library/results-study-interoperability-data-processing-services

41. Data Act — At a glance (European Parliament) (European Parliament Research Service, 2025-09) https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/775915/EPRS_ATA%282025%29775915_EN.pdf

42. SMEs Cybersecurity (ENISA, 2026-07) https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/smes-cybersecurity

43. Allianz Risk Barometer 2026 (Allianz Commercial, 2026-01) https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/economic-research/publications/specials/en/2026/january/allianz-risk-barometer-2026.pdf

44. Cyber insurance unpacked: the corporate digital safety net (Bank for International Settlements (FSI Insights), 2026-06) https://www.bis.org/fsi/publ/insights75.htm

45. ENISA's view on Cybersecurity in the Frontier AI Era (ENISA, 2026-07) https://www.enisa.europa.eu/sites/default/files/2026-07/ENISA%20view%20on%20cybersecurity%20in%20the%20frontier%20AI%20era_en_0.pdf

46. MDCG 2019-11 rev.1 — Qualification and classification of software (MDR/IVDR) (European Commission (DG SANTE), 2025-06) https://health.ec.europa.eu/medical-devices-sector/new-regulations/guidance-mdcg-endorsed-documents-and-other-guidance_en

47. Regulation (EU) 2023/1230 — Machinery Regulation (EUR-Lex, 2023-06) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32023R1230

48. Article 57: AI regulatory sandboxes (AI Act Service Desk (European Commission), 2026-07) https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-57

49. AI regulatory sandboxes: State of play and implementation challenges (European Parliament Research Service, 2026-03)
https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/785673/EPRS_ATA%282026%29785673_EN.pdf

50. Article 51: Classification of GPAI models as models with systemic risk (AI Act Service Desk (European Commission), 2026-07)
https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-51

51. Truly Risk-Based Regulation of Artificial Intelligence? (EJRR) (European Journal of Risk Regulation (Cambridge), 2025-11)
https://www.cambridge.org/core/services/aop-cambridge-core/content/view/E526C1D0D7368F9691082220609D60F4/S1867299X24000783a.pdf/truly_riskbased_regulation_of_artificial_intelligence_how_to_implement_the_eus_ai_act.pdf