AYI NEDJIMI Consultants

RGPD et AI Act : Guide Complet pour les Organisations en ...

Catégorie : Conformité Lecture : 37 min Publié le : 14/02/2026 Auteur : Ayi NEDJIMI

Guide complet RGPD et AI Act (Règlement IA) 2026 : articulation des deux règlements européens, classification des systèmes IA par niveau de risque.

RGPD et AI Act : Guide Complet pour les Organisations en ... constitue un enjeu majeur pour les professionnels de la sécurité informatique et les équipes techniques. Ce guide détaillé sur rgpd comprendre reglement ia ria propose une méthodologie structurée, des outils éprouvés et des recommandations opérationnelles directement applicables. L'objectif est de fournir aux praticiens — consultants, ingénieurs sécurité, administrateurs systèmes — les connaissances et les techniques nécessaires pour aborder ce sujet avec rigueur. Chaque section s'appuie sur des retours d'expérience terrain et intègre les évolutions les plus récentes du domaine. Les recommandations présentées sont adaptées aux environnements d'entreprise et tiennent compte des contraintes opérationnelles réelles.

Table des Matieres

1 Introduction au Règlement IA (AI Act)

Le **Règlement européen sur l'Intelligence Artificielle** (Règlement UE 2024/1689), communément désigné sous le nom d'AI Act, représente une avancée législative majeur dans l'histoire de la régulation technologique mondiale. Adopté définitivement le 13 mars 2024 par le Parlement européen à une majorité écrasante de 523 voix pour, 46 contre et 49 abstentions, puis publié au Journal officiel de l'Union européenne le 12 juillet 2024, ce texte fondateur est entré en vigueur le **1er août 2024**. Il constitue le premier cadre juridique horizontal et contraignant au monde entièrement dédié à la régulation des systèmes d'intelligence artificielle, instaurant un ensemble cohérent de règles harmonisées applicables sur l'ensemble du territoire de l'Union européenne. Guide complet RGPD et AI Act (Règlement IA) 2026 : articulation des deux règlements européens, classification des systèmes IA par niveau de risque. Ce guide

couvre les aspects essentiels de RGPD : méthodologie structurée, outils recommandés et retours d'expérience opérationnels. Les professionnels y trouveront des recommandations directement applicables.

L'ambition du législateur européen est double et s'inscrit dans la continuité de l'approche réglementaire qui a fait ses preuves avec le RGPD. D'une part, il s'agit de **protéger les droits fondamentaux** des citoyens européens face aux risques inhérents au déploiement massif de systèmes d'IA — discriminations algorithmiques, atteintes à la vie privée, manipulation de l'information, surveillance de masse. D'autre part, le règlement vise à **préserver et stimuler l'innovation** en créant un cadre de confiance qui facilite l'adoption responsable de l'IA par les entreprises, les administrations et les citoyens. Cette dualité se traduit par une approche fondée sur le risque, où l'intensité des obligations réglementaires est proportionnelle au niveau de danger que le système d'IA fait peser sur les personnes et la société.

Notre avis d'expert
Comment démontrez-vous l'accountability exigée par le RGPD en cas de contrôle ?

La structure du règlement est imposante : **113 articles** répartis en 13 chapitres, complétés par **13 annexes** techniques détaillant les exigences opérationnelles. Le texte couvre l'intégralité de la chaîne de valeur de l'IA, depuis la conception et le développement des modèles jusqu'à leur déploiement en production, en passant par la mise sur le marché, la distribution et l'utilisation par les organisations. Le champ d'application territorial est extraterritorial, à l'instar du RGPD : toute organisation, qu'elle soit établie dans l'Union européenne ou en dehors, est soumise au règlement dès lors que son système d'IA est mis sur le marché ou mis en service au sein de l'UE, ou que les résultats produits par le système sont utilisés dans l'UE. Cette portée oblige les acteurs mondiaux de l'IA — OpenAI, Anthropic, Google DeepMind, Meta — à intégrer les exigences européennes dans leur stratégie de conformité globale.

Calendrier d'Entrée en Application

Le calendrier de mise en application du Règlement IA est progressif et s'étale sur plus de trois ans, reconnaissant la complexité des ajustements nécessaires pour les organisations. Depuis le **2 février 2025**, les interdictions relatives aux pratiques IA inacceptables définies à l'article 5 sont pleinement applicables : manipulation subliminale, exploitation des vulnérabilités, notation sociale par les autorités publiques et identification biométrique en temps réel dans l'espace public (sauf exceptions encadrées pour les forces de l'ordre). Les obligations concernant les **modèles d'IA à usage général (GPAI)**, catégorie dans laquelle entrent les LLM comme GPT-4, Claude, Gemini, Llama et Mistral, entreront en vigueur le **2 août 2025**. C'est une date charnière pour les fournisseurs de modèles de fondation, qui devront avoir mis en place leur documentation technique, leur politique de droit d'auteur et leur résumé des données d'entraînement.

Les exigences relatives aux **systèmes à haut risque** listés en Annexe III — recrutement, crédit, santé, éducation, justice, migration, infrastructures critiques — s'appliqueront à partir du **2 août 2026**. Les systèmes à haut risque intégrés dans des produits déjà réglementés par la législation d'harmonisation de l'Union (Annexe I : dispositifs médicaux, machines, jouets, équipements radio, aviation civile) bénéficieront d'un délai supplémentaire jusqu'au **2 août 2027**. Enfin, les obligations relatives aux codes de conduite

volontaires pour les systèmes à risque minimal entreront en vigueur le 2 août 2025, bien que leur adoption reste facultative. Ce calendrier progressif impose aux organisations une planification rigoureuse : en février 2026, nous nous trouvons à un point critique où les interdictions sont déjà en vigueur et les obligations GPAI sont à six mois de l'échéance.

Acteurs Concernés et Rôles Définis

Le Règlement IA distingue plusieurs catégories d'acteurs, chacune assortie d'obligations spécifiques. Les **fournisseurs** (providers) sont les personnes physiques ou morales qui développent un système d'IA ou un modèle GPAI, ou qui font développer un tel système, et le mettent sur le marché ou en service sous leur propre nom ou marque. Les **déployeurs** (deployers) sont les personnes physiques ou morales qui utilisent un système d'IA sous leur propre autorité, dans un cadre professionnel, à l'exclusion de l'utilisation personnelle à des fins non professionnelles. Les **importateurs** sont les personnes physiques ou morales établies dans l'UE qui mettent sur le marché un système d'IA portant le nom ou la marque d'un fournisseur établi hors de l'UE. Les **distributeurs** sont les acteurs de la chaîne d'approvisionnement, autres que le fournisseur ou l'importateur, qui rendent un système d'IA disponible sur le marché de l'UE. Cette catégorisation est essentielle car elle détermine la répartition des responsabilités en matière de conformité : le fournisseur porte la charge principale de la documentation technique et de l'évaluation de conformité, tandis que le déployeur est responsable de l'utilisation conforme du système et de la surveillance humaine en conditions opérationnelles.

Sanctions prévues par le Règlement IA :

- ▶**Pratiques interdites (Art. 5) :** jusqu'à 35 millions EUR ou 7% du CA annuel mondial
- ▶**Systèmes haut risque (Art. 6-49) :** jusqu'à 15 millions EUR ou 3% du CA annuel mondial
- ▶**Informations incorrectes :** jusqu'à 7,5 millions EUR ou 1% du CA annuel mondial
- ▶**PME et startups :** plafonds proportionnels réduits pour ne pas entraver l'innovation

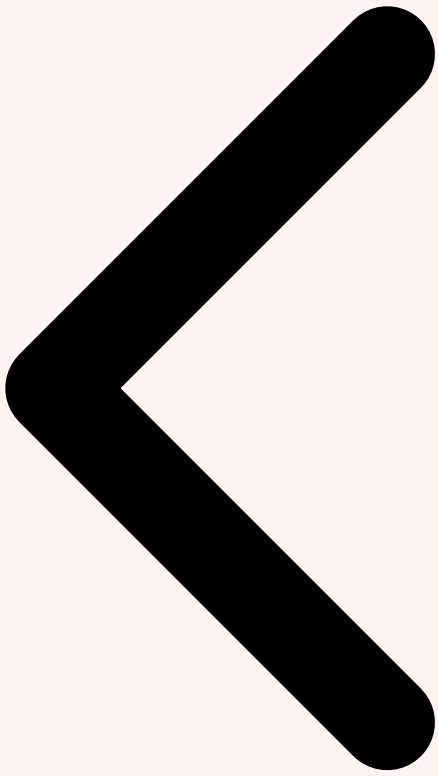
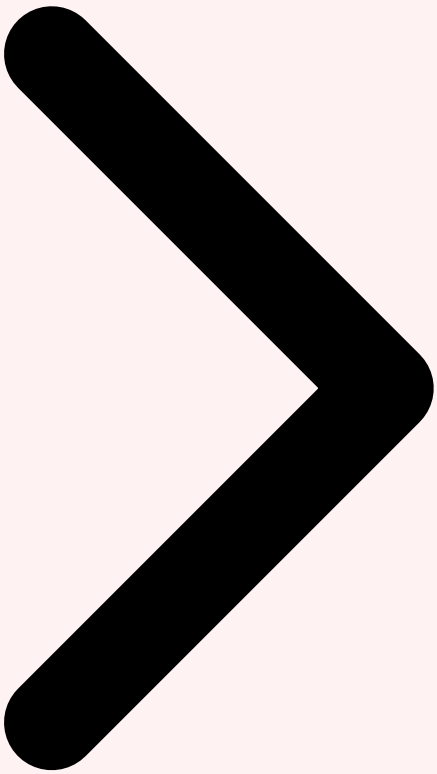


Table des Matieres Introduction AI Act Classification des Risques



Element	Description	Priorite
Prevention	Mesures proactives de reduction de la surface d'attaque	Haute
Detection	Surveillance et alerting en temps reel	Haute
Reponse	Procedures d'incident response et remediation	Critique
Recovery	Plan de reprise et continuite d'activite	Moyenne

Cas concret

L'entrée en vigueur de NIS2 en octobre 2024 a élargi le périmètre des organisations soumises à des obligations de cybersécurité en Europe. Les secteurs essentiels et importants doivent désormais notifier les incidents significatifs dans les 24 heures et maintenir des mesures de gestion des risques proportionnées.

2 Classification des Systèmes IA : La Pyramide des Risques

L'architecture réglementaire du Règlement IA repose sur un principe fondamental de **proportionnalité fondée sur le risque**. Plutôt que d'imposer un régime uniforme à l'ensemble des systèmes d'IA — ce qui aurait été à la fois disproportionné pour les applications inoffensives et insuffisant pour les systèmes dangereux — le législateur européen a opté pour une classification pyramidale à quatre niveaux. Cette approche, inspirée du cadre réglementaire existant pour les produits de sécurité (marquage CE, directives machines, dispositifs médicaux) et de la logique du RGPD en matière de protection des données personnelles, permet de concentrer les obligations les plus exigeantes sur les systèmes présentant le plus grand potentiel de dommage, tout en préservant un espace de liberté pour l'innovation dans les cas à faible risque.

Pour les organisations déployant des systèmes d'IA, la **classification correcte de chaque système** constitue la pierre angulaire de toute démarche de conformité. Une erreur de classification peut avoir des conséquences juridiques majeures : classer un système à haut risque dans la catégorie risque limité expose l'organisation à des sanctions pouvant atteindre 15 millions d'euros ou 3% du chiffre d'affaires mondial, mais également à une responsabilité civile en cas de dommage causé par un système insuffisamment encadré. À l'inverse, sur-classifier un système à risque minimal impose des coûts de conformité inutiles qui grèvent la compétitivité de l'organisation. La classification doit être documentée, motivée et régulièrement révisée à mesure que le système évolue et que son contexte d'utilisation se transforme.

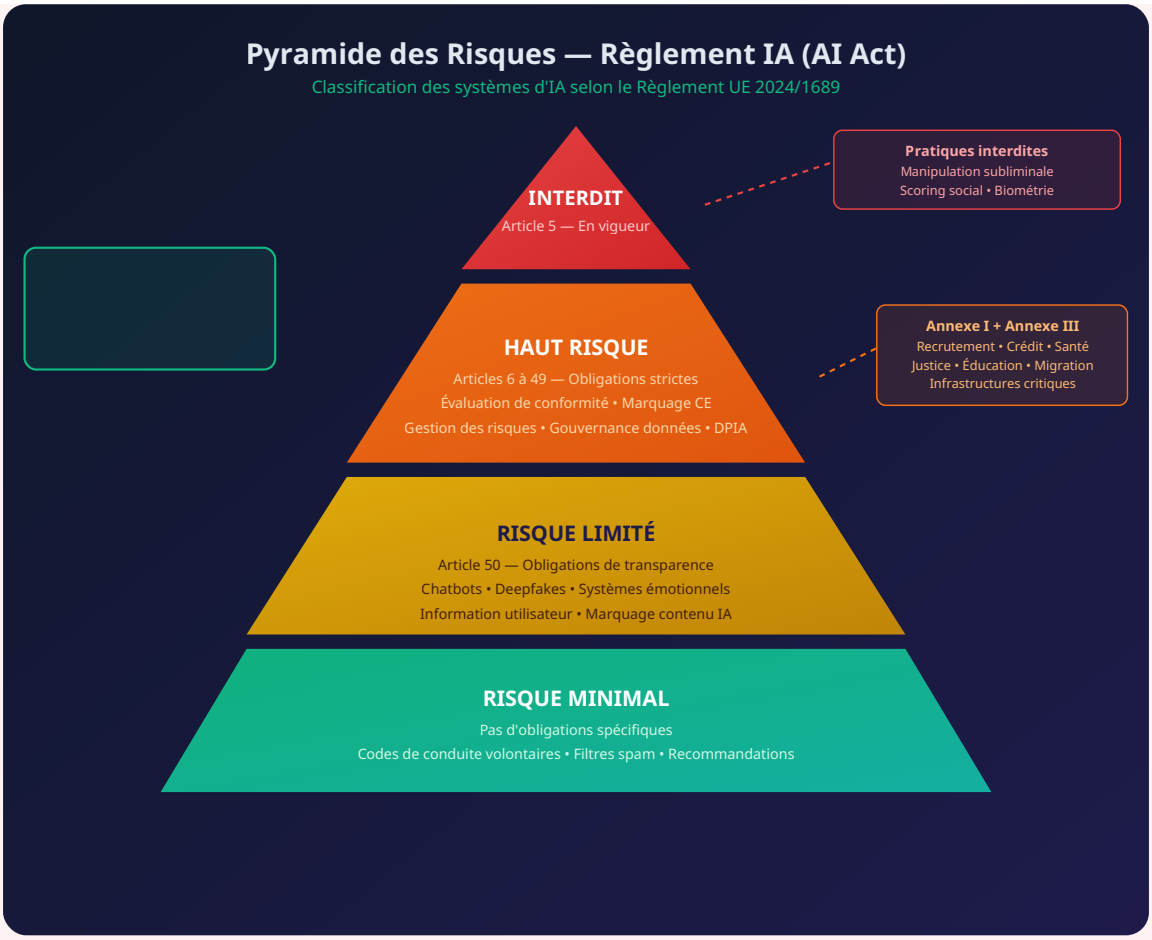


Figure 1 — Pyramide des 4 niveaux de risque du Règlement IA et liens avec le RGPD

Niveau Interdit : Les Pratiques IA Inacceptables (Article 5)

Au sommet de la pyramide, le **niveau interdit** regroupe les pratiques d'IA jugées incompatibles avec les valeurs fondamentales de l'Union européenne. L'article 5, pleinement applicable depuis le 2 février 2025, énumère huit catégories de systèmes d'IA strictement prohibés. Parmi les interdictions les plus structurantes pour les organisations, on retrouve les systèmes utilisant des **techniques subliminales, manipulatrices ou trompeuses** au-delà de la conscience d'une personne, dans le but d'altérer significativement son comportement d'une manière qui cause ou est raisonnablement susceptible de causer un préjudice significatif. Les systèmes exploitant les **vulnérabilités** liées à l'âge, au handicap ou à la situation socio-économique d'une personne sont également interdits. La **notation sociale** (social scoring) par les autorités publiques — c'est-à-dire l'évaluation et la classification des personnes en fonction de leur comportement social ou de caractéristiques personnelles — est prohibée. L'identification biométrique en temps réel dans les espaces accessibles au public est interdite, sauf exceptions strictement encadrées pour les forces de l'ordre dans des cas de terrorisme, d'enlèvement ou de recherche de victimes.

Votre conformité ISO 27001 se traduit-elle par une amélioration réelle de votre sécurité ?

Pour les organisations déployant des systèmes d'IA fondés sur des LLM, ces interdictions ont des implications pratiques directes. Un chatbot commercial conçu pour **manipuler psychologiquement** les utilisateurs en exploitant leurs biais cognitifs pour maximiser les achats impulsifs pourrait tomber sous le coup de l'article 5. Un système de scoring interne évaluant les collaborateurs sur la base de leur comportement social numérique (publications sur les réseaux sociaux, interactions informelles) s'apparenterait à une notation sociale prohibée. Les organisations doivent réaliser un audit systématique de leurs déploiements IA existants pour vérifier qu'aucun ne franchit la ligne rouge des pratiques interdites, car les sanctions sont les plus sévères du règlement : jusqu'à 35 millions d'euros ou 7% du chiffre d'affaires annuel mondial.

Niveau Haut Risque : Le Cœur du Dispositif Réglementaire (Articles 6-49)

Le deuxième niveau de la pyramide constitue le **cœur opérationnel du Règlement IA** et concentre la majorité des obligations de conformité. Un système d'IA est classé à haut risque dans deux cas de figure distincts définis à l'article 6. Premièrement, lorsqu'il est utilisé comme **composant de sécurité** d'un produit couvert par la législation d'harmonisation de l'Union listée en Annexe I (dispositifs médicaux, machines industrielles, jouets, ascenseurs, équipements sous pression, équipements radio, aviation civile, véhicules à moteur, systèmes ferroviaires). Deuxièmement, lorsqu'il entre dans l'une des **huit catégories sensibles** définies en Annexe III : identification biométrique et catégorisation des personnes physiques, gestion et exploitation des infrastructures critiques (énergie, transports, eau, gaz, télécommunications, numérique), éducation et formation professionnelle, emploi et gestion des travailleurs, accès aux services publics essentiels et aux prestations sociales, activités répressives, gestion des migrations et contrôle aux frontières, administration de la justice et processus démocratiques. Pour approfondir, consultez Cyber Resilience Act 2026 : Guide Anticipation Produits Connectés.

L'articulation avec le RGPD est ici fondamentale. La grande majorité des systèmes IA à haut risque traitent nécessairement des **données personnelles** au sens du RGPD : données biométriques dans le cadre de l'identification, données de ressources humaines dans le recrutement, données de santé dans le diagnostic médical, données judiciaires dans l'aide à la décision de justice. Les organisations sont donc confrontées à une **double obligation de conformité** : satisfaire simultanément aux exigences de l'AI Act et à celles du RGPD. La réalisation d'une DPIA (Data Protection Impact Assessment) au titre de l'article 35 du RGPD sera systématiquement requise pour les systèmes IA à haut risque traitant des données personnelles, puisque ces systèmes remplissent par nature les critères du « profilage systématique et extensif » ou de la « surveillance systématique à grande échelle » visés par les lignes directrices du Comité européen de la protection des données.

Niveau Risque Limité : L'Obligation de Transparence (Article 50)

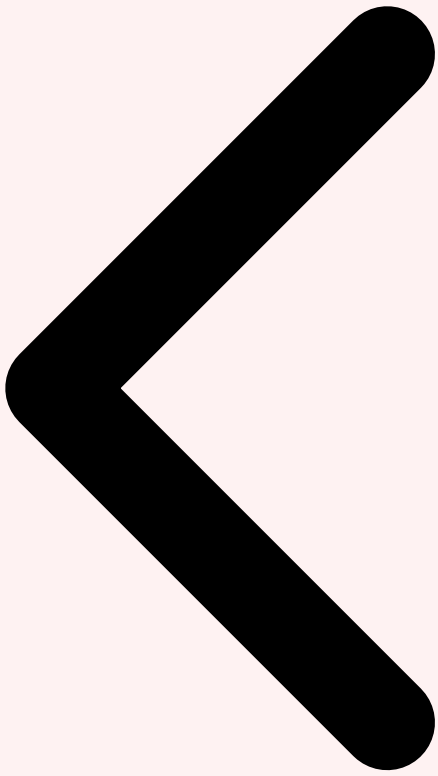
Le troisième niveau concerne les systèmes d'IA présentant un **risque limité**, pour lesquels l'obligation principale est celle de transparence telle que définie à l'article 50 du règlement. Cette obligation vise trois catégories de systèmes. Les **systèmes d'interaction** conçus pour communiquer directement avec des personnes physiques (chatbots, assistants vocaux, agents conversationnels) doivent informer clairement les utilisateurs qu'ils interagissent avec un système d'IA, sauf lorsque cela est évident au vu des circonstances et du contexte d'utilisation. Les **systèmes de génération de contenu synthétique** — texte, images, audio, vidéo — doivent marquer les contenus produits de manière lisible par machine, conformément aux standards techniques en cours d'élaboration. Les systèmes de **reconnaissance des émotions** et de **catégorisation biométrique** doivent informer les personnes exposées de leur fonctionnement. Pour les LLM déployés en interface utilisateur, cette obligation est quasi-systématique : tout chatbot alimenté par un modèle de fondation doit signaler sa nature artificielle aux utilisateurs.

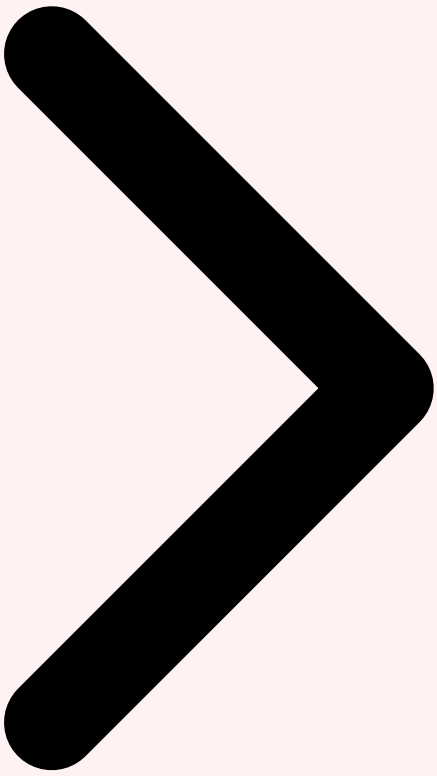
Niveau Risque Minimal : Liberté et Codes de Conduite Volontaires

La base de la pyramide, qui couvre la **grande majorité des systèmes d'IA** actuellement déployés, ne fait l'objet d'aucune obligation spécifique au titre du Règlement IA. Les filtres anti-spam, les moteurs de recommandation de contenu, les systèmes d'optimisation logistique, les outils de traduction automatique ou les assistants de rédaction interne entrent typiquement dans cette catégorie. Le règlement encourage toutefois l'adoption volontaire de **codes de conduite** reprenant les bonnes pratiques en matière de transparence, d'équité, de robustesse et de supervision humaine. Il convient cependant de rappeler que la classification dans la catégorie risque minimal ne dispense pas du respect des autres réglementations applicables, notamment le RGPD pour tout traitement de données personnelles, les règles de protection des consommateurs, le droit de la concurrence et les réglementations sectorielles spécifiques. Un système d'IA à risque minimal au sens de l'AI Act peut parfaitement poser des problèmes majeurs au regard du RGPD s'il traite des données personnelles sans base légale adéquate ou sans respect du principe de minimisation.

⚠ **Point de vigilance RGPD :**

Un système classé à risque minimal par l'AI Act n'est pas automatiquement conforme au RGPD. Le traitement de données personnelles par un système d'IA, quel que soit son niveau de risque AI Act, doit toujours respecter les principes fondamentaux du RGPD : licéité, loyauté, transparence, limitation des finalités, minimisation des données, exactitude, limitation de la conservation, intégrité, confidentialité et responsabilité. L'analyse de conformité doit couvrir les deux règlements de manière conjointe.





3 Obligations par Niveau de Risque : Articles 5, 6, 9-15 Détaillés

La compréhension détaillée des obligations associées à chaque niveau de risque constitue le socle indispensable de toute démarche de conformité au Règlement IA. Pour les organisations opérant des systèmes d'IA, et tout particulièrement celles qui déploient simultanément des systèmes relevant de catégories de risque différentes, la maîtrise précise du périmètre de chaque obligation, de son calendrier d'application et de ses modalités pratiques de mise en œuvre est un prérequis opérationnel. Cette section détaille les exigences article par article, en mettant en lumière les implications concrètes pour les équipes techniques et juridiques et les points d'articulation avec le RGPD.

Article 9 : Système de Gestion des Risques

L'article 9 impose aux fournisseurs de systèmes IA à haut risque la mise en place d'un **système de gestion des risques** continu et itératif, opérant tout au long du cycle de vie du système. Ce système doit être conçu comme un processus vivant, régulièrement mis à jour,

et non comme un exercice ponctuel de documentation. Concrètement, il doit permettre l'**identification et l'analyse** des risques connus et raisonnablement prévisibles que le système d'IA peut poser pour la santé, la sécurité ou les droits fondamentaux des personnes, en tenant compte de la finalité prévue du système et de ses conditions de mauvaise utilisation raisonnablement prévisible. L'**estimation et l'évaluation** de ces risques doivent intégrer des données empiriques issues de tests en conditions réelles ou simulées, et pas uniquement des analyses théoriques. Les **mesures de gestion des risques** adoptées doivent viser l'élimination ou la réduction maximale des risques par conception et développement appropriés (privacy by design), et à défaut, la mise en œuvre de mesures d'atténuation proportionnées. Enfin, le système de gestion des risques doit évaluer **l'efficacité** de ces mesures et documenter les risques résiduels jugés acceptables.

Mise en pratique

Pour les systèmes fondés sur des LLM, la gestion des risques prend une dimension particulière en raison de la nature probabiliste et parfois imprévisible de ces modèles. Les risques spécifiques à documenter incluent les **hallucinations** (génération d'informations factuellement incorrectes présentées avec aplomb), les **biais algorithmiques** reproduisant ou amplifiant les discriminations présentes dans les données d'entraînement, les risques de **fuite de données personnelles** mémorisées par le modèle (model memorization), les vulnérabilités aux **attaques adversariales** (prompt injection, jailbreaking, data poisoning) et les risques liés à la **dérive du modèle** (model drift) en production. L'articulation avec l'article 35 du RGPD est directe : l'analyse d'impact relative à la protection des données (DPIA) constitue un sous-ensemble naturel du système de gestion des risques exigé par l'article 9 de l'AI Act, et les deux exercices peuvent être conduits conjointement pour éviter les redondances et assurer la cohérence.

Article 10 : Gouvernance des Données d'Entraînement

L'article 10 établit des exigences strictes en matière de **gouvernance des données** utilisées pour l'entraînement, la validation et le test des systèmes IA à haut risque. Les pratiques de gouvernance des données doivent porter sur la conception des jeux de données, la collecte des données, les opérations de préparation (étiquetage, nettoyage, enrichissement, agrégation), la formulation d'hypothèses pertinentes, l'évaluation préalable de la disponibilité, de la quantité et de l'adéquation des jeux de données nécessaires, et l'examen au regard des biais possibles susceptibles d'affecter les droits fondamentaux des personnes. Les jeux de données doivent être **pertinents, suffisamment représentatifs**, exempts d'erreurs dans la mesure du possible, et complets au regard de la finalité prévue. Ils doivent tenir compte des caractéristiques géographiques, contextuelles, comportementales et fonctionnelles spécifiques au cadre dans lequel le système est destiné à être utilisé.

L'intersection avec le RGPD est ici particulièrement sensible. L'article 10, paragraphe 5, autorise explicitement le traitement de **catégories particulières de données personnelles** (données sensibles au sens de l'article 9 du RGPD : origine raciale ou ethnique, opinions politiques, convictions religieuses, données de santé, orientation sexuelle) dans la stricte

mesure où cela est nécessaire pour la détection et la correction des biais, sous réserve de garanties appropriées. Cette disposition crée une base légale spécifique qui complète — sans remplacer — les exigences du RGPD. Les organisations doivent néanmoins satisfaire aux conditions cumulatives : le traitement doit être strictement nécessaire à la détection de biais, les données sensibles ne peuvent être utilisées que sous forme de proxy ou dans un environnement contrôlé et sécurisé, des mesures techniques et organisationnelles appropriées doivent être en place (pseudonymisation, chiffrement, contrôle d'accès strict), et le traitement doit être documenté et justifié dans la DPIA.

Articles 11-12 : Documentation Technique et Journalisation

L'article 11 impose la tenue d'une **documentation technique exhaustive** dont le contenu minimal est détaillé en Annexe IV du règlement. Cette documentation doit être établie avant la mise sur le marché ou la mise en service du système et doit être maintenue à jour tout au long de son cycle de vie. Elle comprend une description générale du système (finalité, fournisseur, version, interactions avec d'autres systèmes), une description détaillée des éléments du système (architecture du modèle, algorithmes, choix de conception, hypothèses), la documentation complète des données (origine, méthodes de collecte, étiquetage, taille des jeux de données, caractéristiques et lacunes connues), les métriques de performance utilisées et les résultats des tests, une description du système de gestion des risques et les modifications apportées tout au long du cycle de vie. Pour un LLM déployé en contexte à haut risque et basé sur un modèle GPAI tiers (OpenAI, Anthropic), le déployeur doit compléter la documentation du fournisseur avec ses propres spécifications : architecture RAG, fine-tuning, prompts système, filtres de sécurité et contexte applicatif spécifique.

L'article 12 complète cette exigence par l'obligation de configurer des **mécanismes de journalisation automatique (logging)** permettant le traçage des opérations du système pendant toute sa durée d'utilisation. Les journaux doivent enregistrer les événements pertinents avec une granularité suffisante pour identifier les situations de risque et faciliter la surveillance post-commercialisation. Pour un LLM, cela implique concrètement de logger chaque requête utilisateur, chaque réponse générée, les métadonnées contextuelles (identifiant utilisateur, horodatage, version du modèle, paramètres d'inférence), les scores de confiance lorsqu'ils sont disponibles, et les interventions de filtrage ou de modération. L'articulation avec le RGPD impose cependant une vigilance particulière : la journalisation ne doit pas conduire à un traitement disproportionné de données personnelles. Le principe de **minimisation** (article 5(1)(c) du RGPD) s'applique : les logs ne doivent contenir que les informations strictement nécessaires aux finalités de conformité et de surveillance, avec des durées de conservation limitées et des mesures de pseudonymisation appropriées.

Articles 13-14 : Transparence et Surveillance Humaine

L'article 13 impose que les systèmes IA à haut risque soient conçus de manière à permettre aux **déployeurs d'interpréter les résultats** produits et de les utiliser de manière appropriée. Les informations fournies doivent être concises, complètes, correctes et claires, et inclure les caractéristiques, capacités et limites du système, les métriques de

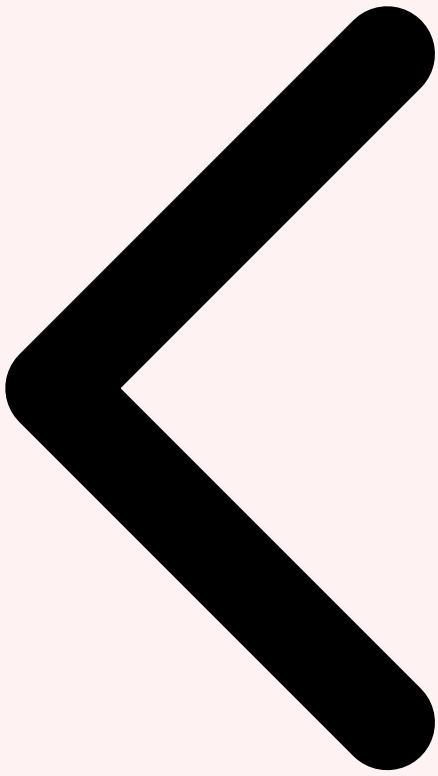
performance pertinentes, les conditions prévisibles de mauvaise utilisation, les spécifications relatives aux données d'entrée, et la description des mesures de surveillance humaine. L'article 14 constitue l'une des dispositions les plus structurantes du règlement : l'obligation de **surveillance humaine** (human oversight). Les systèmes IA à haut risque doivent être conçus de telle sorte qu'ils puissent être surveillés efficacement par des personnes physiques pendant leur période d'utilisation. Les mesures de surveillance humaine doivent permettre à la personne en charge de comprendre les capacités et limites du système, de détecter et corriger les anomalies, et de pouvoir **décider de ne pas utiliser le système, d'interrompre, d'annuler ou d'inverser** le résultat produit. Cette exigence va bien au-delà du simple « human-in-the-loop » technique : elle exige un contrôle humain effectif, informé et significatif, ce qui suppose une formation adéquate des opérateurs et des interfaces de contrôle adaptées. Pour approfondir, consultez SBOM 2026 : Obligation de Sécurité et Guide Complet Software Bill of Materials.

Article 15 : Exactitude, Robustesse et Cybersécurité

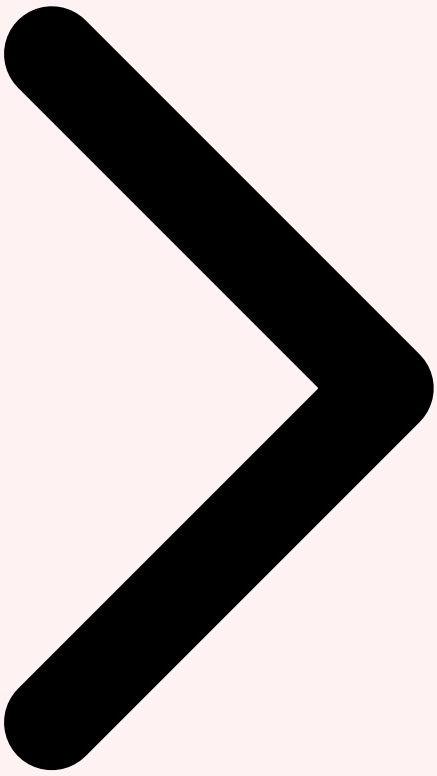
L'article 15 clôt le socle d'exigences techniques en imposant que les systèmes IA à haut risque atteignent un **niveau approprié d'exactitude, de robustesse et de cybersécurité** tout au long de leur cycle de vie. L'exactitude doit être déclarée dans les informations d'accompagnement et documentée par des métriques appropriées. La robustesse technique couvre la résilience face aux erreurs, aux défaillances et aux incohérences dans les données d'entrée, ainsi que la résistance aux tentatives de manipulation par des tiers non autorisés. Les mesures de cybersécurité doivent protéger le système contre les **vulnérabilités spécifiques aux systèmes d'IA** : data poisoning (empoisonnement des données d'entraînement), prompt injection (injection de commandes dans les entrées utilisateur), model extraction (vol du modèle par requêtes systématiques), adversarial examples (exemples adversariaux conçus pour tromper le modèle) et model inversion (reconstruction des données d'entraînement à partir du modèle). Pour les LLM, cette obligation implique le déploiement de mécanismes de détection et de filtrage des prompt injections, de garde-fous contre le jailbreaking, de rate limiting pour prévenir l'extraction, et de monitoring continu pour détecter les comportements anormaux indicateurs d'une attaque en cours.

Synthèse des obligations par niveau de risque :

- ▶**Interdit :** Audit immédiat des systèmes existants, suppression de toute pratique prohibée (Art. 5)
- ▶**Haut risque :** Gestion des risques (Art. 9), gouvernance données (Art. 10), documentation (Art. 11-12), transparence (Art. 13), surveillance humaine (Art. 14), cybersécurité (Art. 15)
- ▶**Risque limité :** Information de l'utilisateur, marquage des contenus synthétiques, notification des systèmes émotionnels (Art. 50)
- ▶**Risque minimal :** Codes de conduite volontaires, respect des réglementations existantes (RGPD, droit des consommateurs)



Classification des Risques Obligations par Niveau RGPD et AI Act



4 RGPD et IA : Articulation des Deux Règlements

L'articulation entre le **Règlement Général sur la Protection des Données (RGPD)** et le **Règlement IA (AI Act)** constitue l'un des défis juridiques et opérationnels les plus complexes auxquels les organisations doivent faire face en 2026. Ces deux textes fondamentaux du droit numérique européen ne sont ni redondants ni contradictoires : ils sont complémentaires et se renforcent mutuellement. Le RGPD, en vigueur depuis le 25 mai 2018, encadre le traitement des données personnelles selon une logique centrée sur les droits des personnes concernées et la responsabilité des responsables de traitement. Le Règlement IA, quant à lui, encadre la conception, le développement et le déploiement des systèmes d'intelligence artificielle selon une logique de classification par le risque. Lorsqu'un système d'IA traite des données personnelles — ce qui est le cas de la quasi-totalité des déploiements en entreprise — les deux règlements s'appliquent simultanément et de manière cumulative.

Le considérant 10 du Règlement IA est explicite sur ce point : le règlement « n'affecte pas l'application du [RGPD] » et doit être lu « en combinaison avec » celui-ci. L'article 2, paragraphe 7, précise que le règlement s'applique « sans préjudice du [RGPD] ». Cela signifie concrètement qu'un système d'IA conforme à l'AI Act peut parfaitement être en infraction avec le RGPD, et inversement. Les deux conformités doivent être établies de manière indépendante mais coordonnée. Pour les organisations, cela implique une **gouvernance intégrée** associant les équipes juridiques, les DPO (Data Protection Officers), les équipes IA et les fonctions de conformité dans un dispositif unique et cohérent.

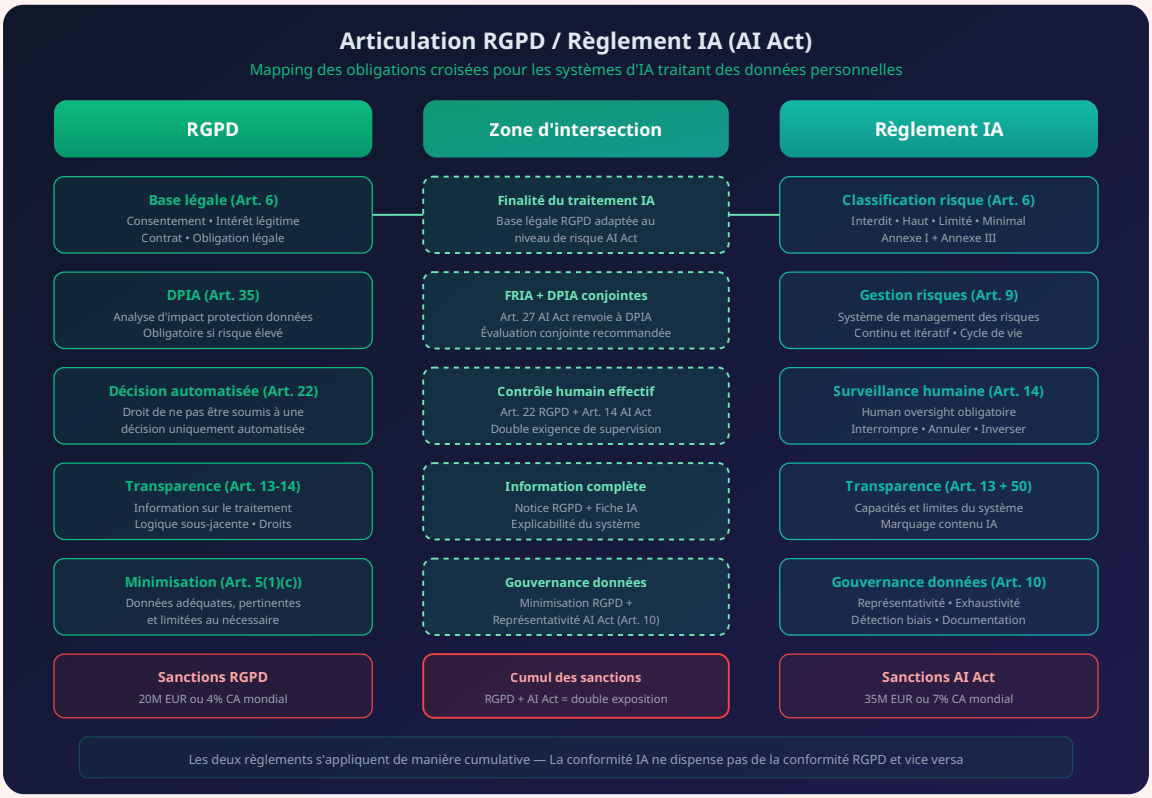


Figure 2 — Mapping des obligations croisées entre le RGPD et le Règlement IA (AI Act)

Base Légale du Traitement IA sous le RGPD

Toute utilisation d'un système d'IA traitant des données personnelles doit reposer sur l'une des **six bases légales** de l'article 6 du RGPD. Le choix de la base légale appropriée dépend du contexte de déploiement et du niveau de risque AI Act du système. Le **consentement** (article 6(1)(a)) est rarement adapté aux systèmes IA à haut risque en raison de la difficulté à garantir un consentement véritablement libre, spécifique, éclairé et univoque lorsque les mécanismes décisionnels du système sont opaques. L'**intérêt légitime** (article 6(1)(f)) est la base légale la plus couramment invoquée pour les déploiements IA, mais elle nécessite une mise en balance rigoureuse avec les intérêts, droits et libertés des personnes concernées — une mise en balance que le niveau de risque AI Act du système influence directement. Plus le risque AI Act est élevé, plus la démonstration de la proportionnalité de l'intérêt légitime est exigeante. La **nécessité contractuelle** (article 6(1)(b)) ne peut être invoquée que lorsque le traitement IA est objectivement nécessaire à l'exécution du contrat, et non

simplement utile ou opportun. L'**obligation légale** (article 6(1)(c)) peut constituer une base pertinente lorsque le déploiement du système IA est imposé par une réglementation sectorielle (par exemple, les obligations de vigilance en matière de lutte anti-blanchiment).

L'Article 22 du RGPD et l'Article 14 de l'AI Act : La Double Exigence de Contrôle Humain

L'articulation entre l'**article 22 du RGPD** et l'**article 14 du Règlement IA** crée un cadre de protection renforcé en matière de décision automatisée. L'article 22 du RGPD établit le droit fondamental de toute personne de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire. Ce droit n'est pas absolu : il admet des exceptions lorsque la décision est nécessaire à la conclusion ou à l'exécution d'un contrat, autorisée par le droit de l'Union ou d'un État membre, ou fondée sur le consentement explicite de la personne. Cependant, même dans ces cas d'exception, le responsable de traitement doit mettre en œuvre des mesures appropriées pour sauvegarder les droits et libertés de la personne, au minimum le droit d'obtenir une intervention humaine, d'exprimer son point de vue et de contester la décision.

L'article 14 de l'AI Act va plus loin en imposant une **surveillance humaine structurelle** intégrée dès la conception du système. Tandis que l'article 22 du RGPD se concentre sur le droit individuel de la personne affectée par la décision, l'article 14 de l'AI Act impose une obligation systémique au fournisseur et au déployeur du système. La combinaison des deux textes crée un régime particulièrement exigeant : non seulement la personne affectée doit pouvoir contester la décision et obtenir une intervention humaine (RGPD), mais le système lui-même doit être conçu pour permettre une surveillance humaine effective à tout moment de son fonctionnement (AI Act). Pour les LLM déployés dans des contextes de décision automatisée — scoring de crédit, pré-sélection de candidatures, aide à la décision judiciaire, évaluation médical — cette double exigence impose concrètement la mise en œuvre d'un **circuit de validation humaine** intégré dans le workflow applicatif, avec des mécanismes de recours clairement définis et accessibles aux personnes affectées.

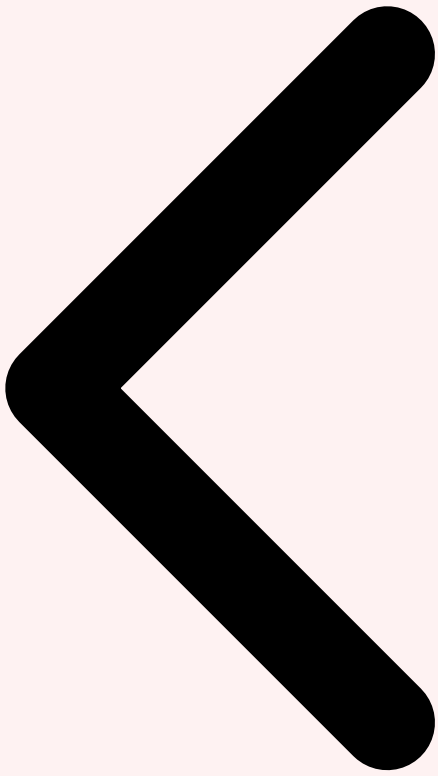
DPIA et FRIA : L'Évaluation d'Impact Conjointe

L'article 27 du Règlement IA impose aux déployeurs de systèmes IA à haut risque la réalisation d'une **évaluation d'impact sur les droits fondamentaux (FRIA — Fundamental Rights Impact Assessment)** avant la mise en service du système. Cette obligation est distincte mais complémentaire de l'obligation de DPIA (Data Protection Impact Assessment) prévue à l'article 35 du RGPD. La FRIA doit couvrir une description des processus du déployeur dans lesquels le système sera utilisé, une description de la période et de la fréquence d'utilisation prévues, les catégories de personnes physiques et groupes susceptibles d'être affectés, les risques spécifiques de préjudice susceptibles d'affecter ces catégories, une description de la mise en œuvre des mesures de surveillance humaine, et les mesures à prendre en cas de matérialisation des risques identifiés. En pratique, la FRIA et la DPIA peuvent et doivent être **conduites conjointement** pour les systèmes IA traitant

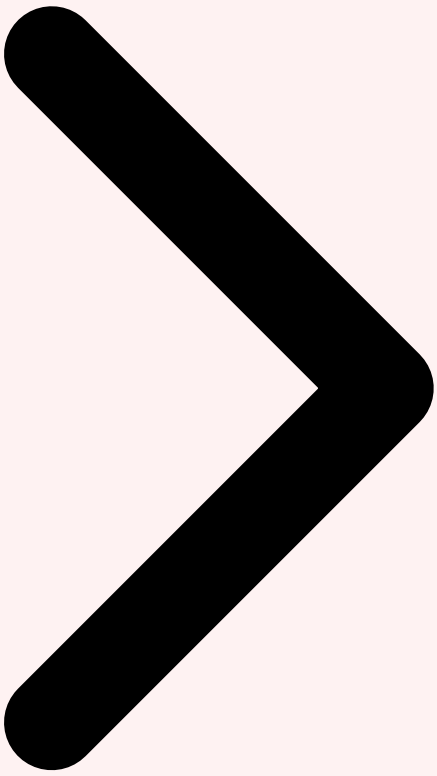
des données personnelles, en s'appuyant sur une méthodologie intégrée qui couvre à la fois les risques pour la protection des données et les risques plus larges pour les droits fondamentaux (non-discrimination, liberté d'expression, dignité humaine, accès à la justice). Cette approche conjointe évite les redondances documentaires et assure la cohérence des mesures d'atténuation.

⚠ **Piège courant : la « conformité AI Act » sans le RGPD**

De nombreuses organisations commettent l'erreur de traiter la conformité AI Act de manière isolée, en négligeant les implications RGPD. Un système d'IA parfaitement conforme aux exigences de l'AI Act (documentation technique, gestion des risques, surveillance humaine) peut néanmoins violer le RGPD s'il traite des données personnelles sans base légale adéquate, sans information suffisante des personnes concernées, sans respect du droit d'opposition ou de rectification, ou sans DPIA là où elle est requise. Les autorités de contrôle (CNIL en France, autorités de surveillance AI Act) sont amenées à coopérer et à partager leurs constats. Une infraction détectée par l'une peut déclencher un contrôle par l'autre. L'exposition financière combinée peut atteindre **55 millions d'euros ou 11% du CA mondial** (7% AI Act + 4% RGPD).



Obligations par Niveau RGPD et AI Act GPAI et LLM



5 Obligations Spécifiques : GPAI et LLM (Articles 51-56)

Le chapitre V du Règlement IA (articles 51 à 56) introduit un cadre réglementaire spécifiquement conçu pour les **modèles d'IA à usage général (General-Purpose AI — GPAI)**, une catégorie qui englobe de facto tous les grands modèles de langage (LLM) actuels : GPT-4 et ses successeurs (OpenAI), Claude (Anthropic), Gemini (Google DeepMind), Llama (Meta), Mistral (Mistral AI), et l'ensemble des modèles de fondation capables d'accomplir une grande variété de tâches distinctes. Cette innovation législative reconnaît la spécificité des modèles de fondation, qui ne sont pas des systèmes d'IA autonomes mais des composants technologiques susceptibles d'être intégrés dans une multitude d'applications en aval, chacune pouvant relever d'un niveau de risque différent. La distinction entre le **fournisseur du modèle GPAI** (OpenAI, Anthropic) et le **fournisseur ou déployeur du système IA en aval** (l'entreprise qui intègre le modèle dans une application métier) est fondamentale pour la répartition des obligations de conformité.

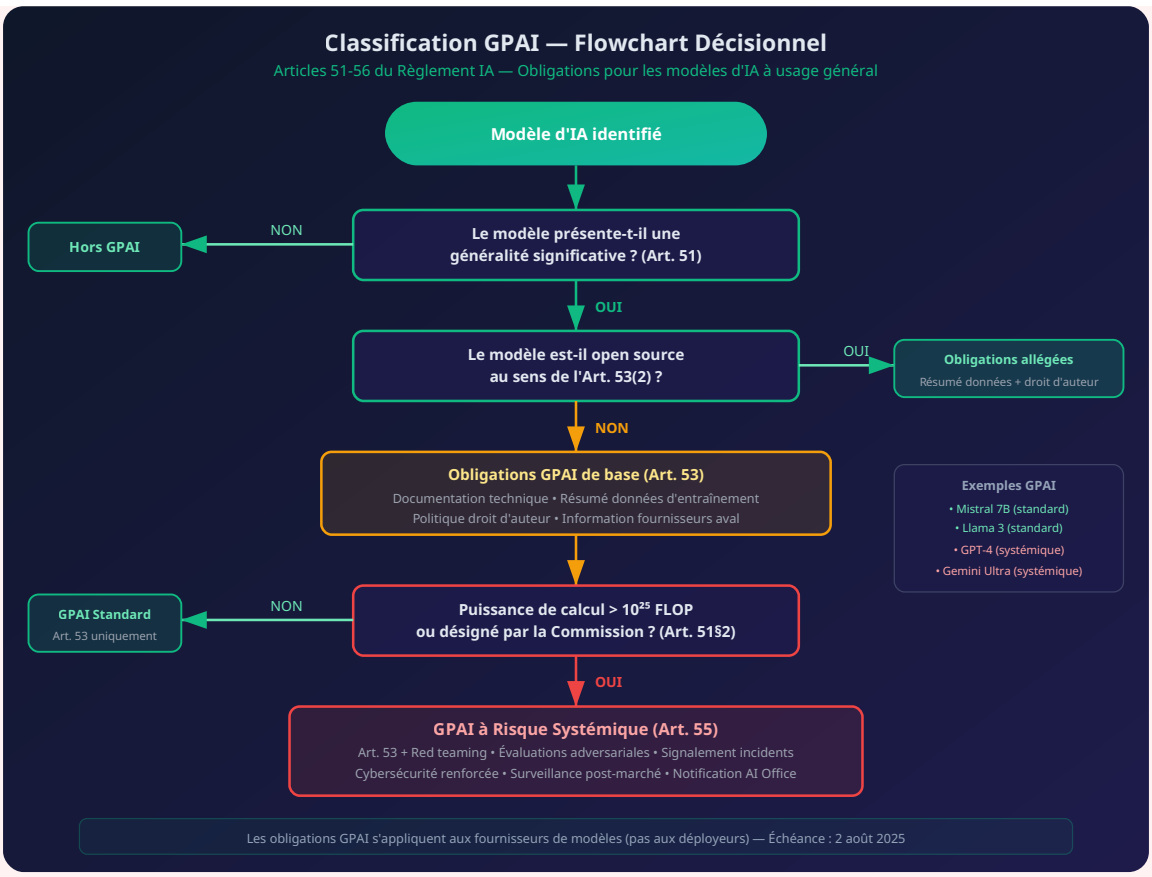


Figure 3 — Flowchart décisionnel de classification GPAI et obligations associées (Articles 51-56) Pour approfondir, consultez Sécurité LLM Adversarial : Attaques, Défenses et Bonnes.

Obligations de Base pour Tous les Modèles GPAI (Article 53)

L'article 53 définit un socle d'**obligations minimales** applicables à tout fournisseur de modèle GPAI, qu'il soit propriétaire ou open source (sous réserve de l'allégement prévu au paragraphe 2 pour les modèles open source). La première obligation porte sur la **documentation technique** du modèle et de son processus d'entraînement, qui doit être établie conformément à l'Annexe XI du règlement et mise à la disposition de l'AI Office et des autorités nationales compétentes sur demande. Cette documentation doit être suffisamment détaillée pour permettre aux fournisseurs de systèmes IA en aval d'exercer leurs propres obligations de conformité — un point critique dans l'écosystème des LLM, où l'opacité des fournisseurs de modèles de fondation est souvent dénoncée par les intégrateurs. La deuxième obligation concerne la mise en œuvre d'une **politique de respect du droit d'auteur** conforme à la directive (UE) 2019/790, incluant l'identification et le respect des réservations de droits formulées par les titulaires (opt-out des données d'entraînement). La troisième obligation impose la publication d'un **résumé suffisamment détaillé des données d'entraînement** selon un modèle fourni par l'AI Office, une exigence qui touche au centre de la transparence des LLM et fait l'objet de débats intenses entre les développeurs de modèles et les éditeurs de contenu.

Modèles GPAI à Risque Systémique (Articles 51 et 55)

Le Règlement IA crée une sous-catégorie de modèles GPAI présentant un **risque systémique**, soumis à un régime de surveillance renforcé comparable à celui des institutions financières systémiques. Un modèle est présumé à risque systémique lorsque la quantité cumulée de calcul utilisée pour son entraînement dépasse le seuil de **10^25 FLOP** (floating point operations). Ce seuil quantitatif, bien qu'il constitue une approximation imparfaite de la dangerosité réelle d'un modèle, a été retenu comme indicateur objectif et mesurable de la puissance du modèle. La Commission européenne conserve la possibilité de désigner un modèle comme présentant un risque systémique sur la base de critères qualitatifs complémentaires : nombre d'utilisateurs professionnels, impact sur le marché intérieur, capacités du modèle évaluées par des benchmarks standardisés, ou tout autre critère pertinent. En pratique, les modèles GPT-4 (OpenAI), Gemini Ultra (Google) et potentiellement Claude Opus (Anthropic) dépassent le seuil de 10^25 FLOP et sont donc classés comme GPAI à risque systémique.

Les obligations renforcées de l'article 55 pour les modèles GPAI à risque systémique comprennent la réalisation d'**évaluations de modèle** conformes à des protocoles standardisés, incluant des tests adversariaux (red teaming) documentés visant à identifier et à atténuer les risques systémiques. Les fournisseurs doivent évaluer et atténuer les **risques systémiques possibles**, y compris leurs sources, au niveau de l'Union — ce qui inclut les risques de désinformation à grande échelle, les risques de discrimination systématique, les risques pour la cybersécurité de l'Union et les risques pour la recherche scientifique et l'intégrité académique. Ils doivent **suivre, documenter et signaler** sans retard injustifié à l'AI Office les incidents graves et les mesures correctives adoptées. Ils doivent assurer un niveau adéquat de **protection en matière de cybersécurité** pour le modèle et son infrastructure physique. L'AI Office peut à tout moment demander des informations complémentaires et réaliser des audits sur site.

L'Exception Open Source et Ses Limites

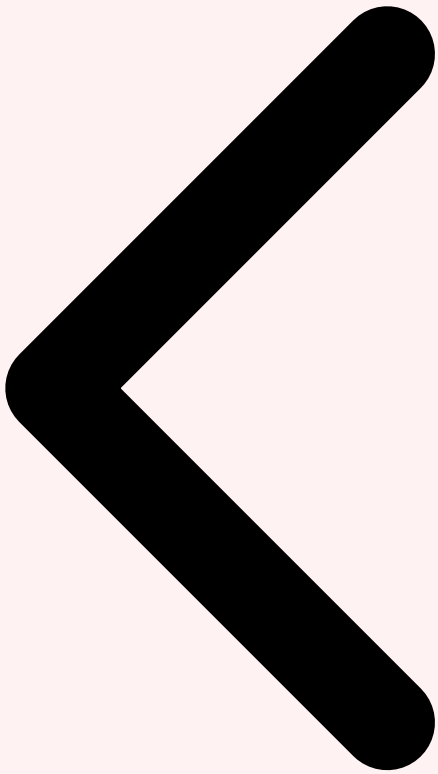
L'article 53, paragraphe 2, accorde un **traitement allégé aux modèles GPAI open source**, reconnaissant leur contribution essentielle à l'innovation et à la recherche. Un modèle GPAI est considéré comme open source lorsque ses paramètres, y compris les poids, l'architecture et les informations relatives à l'utilisation, sont rendus publiquement accessibles sous une licence libre et open source permettant l'accès, l'utilisation, la modification et la distribution du modèle. Les fournisseurs de tels modèles sont exemptés de la majorité des obligations de l'article 53, ne conservant que l'obligation de publier le résumé des données d'entraînement et la politique de droit d'auteur. Cependant, cette exception **ne s'applique pas aux modèles à risque systémique** : un modèle open source dépassant le seuil de 10^25 FLOP (comme un hypothétique Llama de très grande taille) resterait soumis à l'intégralité des obligations renforcées de l'article 55. Cette limite est significative car elle empêche les grands acteurs technologiques d'utiliser l'open source comme stratégie d'échappement réglementaire pour leurs modèles les plus puissants.

Implications pour les Déployeurs de LLM en Entreprise

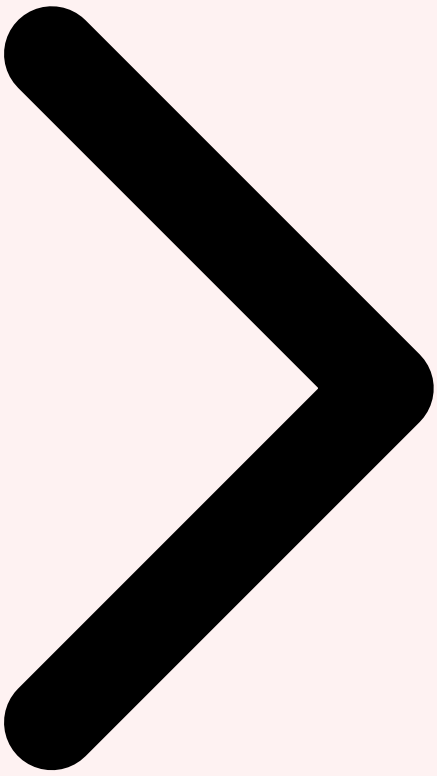
Pour les organisations qui **déploient des LLM** en tant que déployeurs ou fournisseurs de systèmes IA en aval (par opposition aux fournisseurs de modèles GPAI), les obligations GPAI ont des implications indirectes mais significatives. Premièrement, les déployeurs doivent s'assurer que leurs fournisseurs de modèles GPAI respectent effectivement leurs obligations de l'article 53 — ce qui implique de vérifier la disponibilité de la documentation technique, du résumé des données d'entraînement et de la politique de droit d'auteur. Deuxièmement, lorsqu'un déployeur utilise un modèle GPAI pour construire un système IA à haut risque, il hérite de l'obligation de documenter les spécificités de son déploiement (fine-tuning, RAG, prompts système, filtres) et de les intégrer dans la documentation technique requise par l'Annexe IV. Troisièmement, si le modèle GPAI sous-jacent est à risque systémique, le déployeur doit prendre en compte les risques systémiques identifiés par le fournisseur du modèle dans sa propre analyse de risques au titre de l'article 9. Les contrats avec les fournisseurs de modèles GPAI doivent être **renforcés contractuellement** pour inclure des clauses de conformité AI Act, d'accès à la documentation technique, de notification des incidents et de coopération en cas d'audit par les autorités de surveillance.

Checklist GPAI pour les déployeurs de LLM :

- ▶**Vérifier la documentation :** Exiger du fournisseur (OpenAI, Anthropic, Google) la documentation technique Annexe XI et le résumé des données d'entraînement
- ▶**Évaluer le risque systémique :** Vérifier si le modèle utilisé dépasse le seuil de 10^25 FLOP et intégrer les risques systémiques dans votre propre analyse
- ▶**Renforcer les contrats :** Inclure des clauses de conformité AI Act, d'accès à la documentation, de notification des incidents et de coopération audit
- ▶**Documenter votre intégration :** Compléter la documentation GPAI avec vos spécificités (RAG, fine-tuning, prompts, filtres, contexte applicatif)
- ▶**Droit d'auteur :** Vérifier la politique de respect du droit d'auteur du fournisseur et ses implications pour votre propre conformité



RGPD et AI Act GPAI et LLM Documentation et Audit



6 Conformité Pratique : Documentation et Audit

La mise en conformité avec le Règlement IA ne se réduit pas à un exercice théorique de classification des systèmes : elle exige la production d'une **documentation technique structurée et auditable**, l'implémentation de processus de gouvernance vérifiables et l'intégration de mécanismes de contrôle continu dans les workflows opérationnels de l'organisation. L'expérience acquise depuis 2018 avec le RGPD a démontré que la documentation et la capacité à démontrer la conformité (principe d'accountability) constituent la charge de travail la plus significative et la plus durable de toute démarche réglementaire. Le Règlement IA reprend et amplifie cette logique d'accountability en l'appliquant spécifiquement aux dimensions techniques, éthiques et de gouvernance propres aux systèmes d'intelligence artificielle.

Le Dossier Technique selon l'Annexe IV

L'Annexe IV du Règlement IA détaille le **contenu minimum de la documentation technique** requise pour les systèmes IA à haut risque. Ce dossier technique doit être préparé avant la mise sur le marché ou la mise en service du système, maintenu à jour tout au long de son cycle de vie, et mis à la disposition des autorités de surveillance sur demande dans un délai raisonnable. Le dossier comprend plusieurs volets complémentaires. Le premier volet est une **description générale du système** incluant sa finalité prévue, le nom et les coordonnées du fournisseur, la version du système, les modalités d'interaction avec d'autres systèmes logiciels ou matériels, les versions pertinentes des logiciels utilisés, et une description de l'architecture matérielle sur laquelle le système est destiné à fonctionner. Le deuxième volet porte sur la **description détaillée des éléments du système** : le processus de développement, les choix de conception, l'architecture computationnelle du modèle (pour un LLM : architecture transformer, nombre de paramètres, dimensions d'embedding, nombre de couches d'attention), les algorithmes d'entraînement, les hypothèses formulées et les compromis réalisés.

Le troisième volet concerne la **documentation des données** : description des jeux de données d'entraînement, de validation et de test, origine des données, méthodes de collecte, opérations de préparation (étiquetage, nettoyage, enrichissement, augmentation), taille des jeux de données, caractéristiques pertinentes, lacunes connues et mesures prises pour les combler. Le quatrième volet détaille les **métriques de performance** utilisées, les résultats des tests de validation et les benchmarks de référence. Le cinquième volet décrit le **système de gestion des risques** et ses résultats. Pour un LLM déployé en contexte à haut risque et basé sur un modèle GPAI tiers, le déployeur devenu fournisseur du système en aval doit compléter la documentation du fournisseur de modèle (documentation Annexe XI) avec ses propres spécifications : architecture RAG (chunks, embedding model, retrieval strategy), pipeline de fine-tuning (hyperparamètres, données spécifiques, métriques de convergence), prompts système et instructions, chaîne de filtrage et de modération, configuration de l'inférence (température, top-p, max tokens), et documentation complète du contexte applicatif et de la finalité prévue.

Évaluation de Conformité (Articles 43-44)

Avant la mise sur le marché d'un système IA à haut risque, le fournisseur doit procéder à une **évaluation de conformité** selon l'une des procédures prévues aux articles 43 et 44. Pour la majorité des systèmes relevant de l'Annexe III, l'évaluation peut être réalisée par le fournisseur lui-même selon la procédure de **contrôle interne** décrite à l'Annexe VI. Cette auto-évaluation exige la vérification systématique de la conformité du système de management de la qualité (article 17), l'examen de la documentation technique pour démontrer le respect des articles 8 à 15, et la vérification de la conformité du système aux spécifications techniques applicables. Pour les systèmes IA utilisés dans le cadre de l'**identification biométrique à distance**, une évaluation par un organisme notifié (tiers accrédité) est obligatoire, ce qui implique des délais et des coûts supplémentaires

significatifs. Une fois l'évaluation réussie, le fournisseur appose le **marquage CE** et établit une déclaration UE de conformité, engageant sa responsabilité juridique quant au respect du règlement.

L'évaluation de conformité doit intégrer l'ensemble des interactions avec le RGPD. Si le système traite des données personnelles, la DPIA doit être réalisée ou mise à jour préalablement à l'évaluation de conformité AI Act. Les mesures de protection des données (chiffrement, pseudonymisation, contrôle d'accès, minimisation, durées de conservation) doivent être documentées dans le dossier technique et vérifiées lors de l'évaluation. Les **organismes notifiés**, désignés par les autorités nationales conformément aux articles 28 à 39 du règlement, doivent disposer de compétences à la fois en intelligence artificielle, en cybersécurité et en protection des données — une exigence de polyvalence qui pose des défis significatifs en matière de formation et de recrutement des auditeurs.

Système de Management de la Qualité (Article 17)

L'article 17 impose aux fournisseurs de systèmes IA à haut risque la mise en œuvre d'un **système de management de la qualité (SMQ)** documenté, systématique et proportionné à la taille de l'organisation et à la complexité des systèmes concernés. Le SMQ doit couvrir un périmètre exhaustif : stratégie de conformité réglementaire, techniques et procédures de conception et développement des systèmes IA, procédures de test et de validation (y compris les tests avant et après déploiement), spécifications techniques et normes utilisées, systèmes et procédures de gestion des données, système de gestion des risques de l'article 9, surveillance post-commercialisation (article 72), procédures de signalement d'incidents graves (article 73), et gestion de la communication avec les autorités de surveillance, les organismes notifiés et les déployeurs. Pour les organisations disposant déjà d'une certification **ISO 27001** (management de la sécurité de l'information) ou **ISO 42001** (management de l'intelligence artificielle), l'intégration des exigences de l'AI Act dans le SMQ existant constitue l'approche la plus efficiente, permettant de capitaliser sur les processus, la documentation et la culture d'amélioration continue déjà en place.

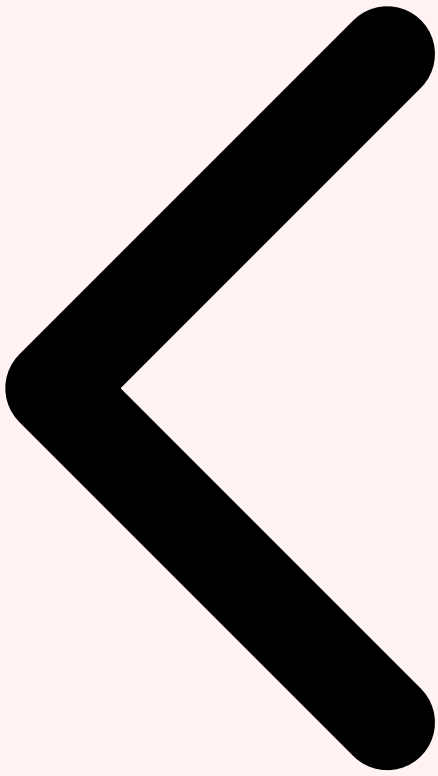
Surveillance Post-Commercialisation et Signalement

La conformité ne s'arrête pas à la mise sur le marché : l'article 72 impose une **surveillance post-commercialisation** active et documentée, intégrée dans le SMQ. Le fournisseur doit collecter, documenter et analyser en continu les données pertinentes fournies par les déployeurs ou collectées via d'autres sources (monitoring automatisé, retours utilisateurs, rapports d'incidents, veille sectorielle), afin d'évaluer la conformité continue du système aux exigences du règlement. Pour les systèmes fondés sur des LLM, cette surveillance inclut le **monitoring des performances du modèle** en production (détection de la dérive du modèle, évolution des métriques de qualité des réponses), l'analyse des retours utilisateurs et des plaintes, la détection des comportements inattendus ou dangereux (hallucinations critiques, contenu nuisible, biais discriminatoires émergents), et la veille sur les nouvelles vulnérabilités et techniques d'attaque adversariale. L'article 73 complète ce dispositif par l'obligation de **signalement des incidents graves** aux autorités de

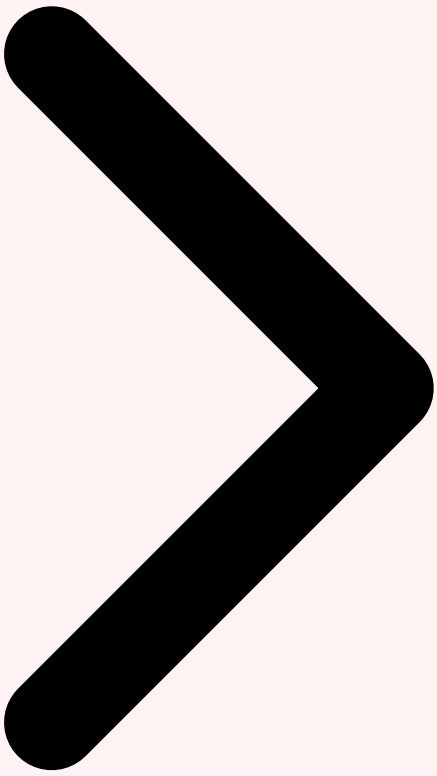
surveillance nationales dans un délai de 15 jours suivant leur identification, avec une notification immédiate en cas de risque pour la santé ou la sécurité des personnes. Pour approfondir, consultez ISO 42001 Lead Auditor : Auditer un Systeme de Management.

Documentation requise — Checklist synthétique :

- ▶**Dossier technique (Annexe IV) :** Description système, architecture modèle, données d'entraînement, métriques performance, gestion risques
- ▶**DPIA (Art. 35 RGPD) :** Analyse d'impact protection données, intégrée avec la FRIA (Art. 27 AI Act)
- ▶**Registre des systèmes IA :** Inventaire centralisé, classification par niveau de risque, responsables identifiés
- ▶**SMQ (Art. 17) :** Système de management qualité couvrant l'ensemble du cycle de vie IA
- ▶**Déclaration UE de conformité :** Après évaluation de conformité réussie (auto-évaluation ou organisme notifié)
- ▶**Plan de surveillance post-marché :** Monitoring continu, signalement incidents, revues périodiques



GPAI et LLM Documentation et Audit Roadmap Conformité



7 Roadmap de Mise en Conformité : 4 Phases Opérationnelles

La mise en conformité simultanée avec le RGPD et le Règlement IA constitue un **programme de transformation pluriannuel** qui ne peut être traité comme un projet ponctuel. En février 2026, les organisations se trouvent dans une fenêtre stratégique critique : les interdictions de l'article 5 sont en vigueur depuis un an, les obligations GPAI entreront en application dans six mois (août 2025), et les exigences relatives aux systèmes à haut risque suivront un an plus tard (août 2026). La roadmap suivante propose une approche structurée en quatre phases, conçue pour les organisations déployant des systèmes d'IA fondés sur des LLM et traitant des données personnelles, intégrant de manière cohérente les exigences des deux règlements.

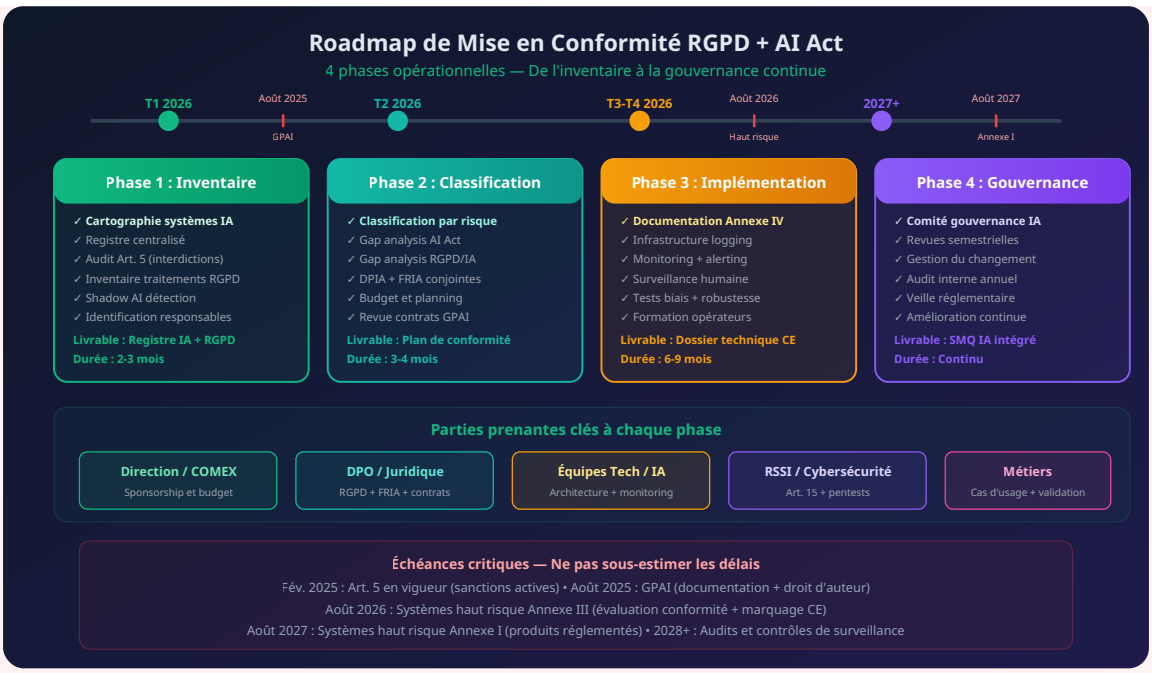


Figure 4 — Roadmap de mise en conformité RGPD + AI Act en 4 phases opérationnelles

Phase 1 : Inventaire et Cartographie (T1 2026 — Immédiat)

La première phase, à engager immédiatement, consiste à réaliser un **inventaire exhaustif et croisé** de tous les systèmes d'IA déployés ou en développement et de tous les traitements de données personnelles associés. Cet inventaire doit couvrir quatre dimensions : les systèmes développés en interne (modèles entraînés, fine-tuned ou hébergés), les solutions SaaS intégrant des composants IA (Microsoft Copilot, Salesforce Einstein, ServiceNow, etc.), les modèles GPAI utilisés via API (OpenAI, Anthropic, Google, Mistral, Cohere), et les usages informels de l'IA par les collaborateurs (**shadow AI** — utilisation de ChatGPT, Claude ou d'autres outils sans validation par l'organisation). Pour chaque système identifié, documentez la finalité prévue, les données personnelles traitées (catégories, volume, sources), les personnes physiques affectées (collaborateurs, clients, candidats, patients, citoyens), le fournisseur du modèle sous-jacent, la base légale RGPD invoquée et le niveau de risque AI Act préliminaire. Constituez un **registre centralisé des systèmes IA**, idéalement intégré au registre des traitements RGPD (article 30), qui servira de base à l'ensemble de la démarche de conformité. Identifiez pour chaque système un responsable métier et un responsable technique. Réalisez en priorité un audit des pratiques interdites de l'article 5 pour vérifier qu'aucun système existant ne franchit la ligne rouge.

Phase 2 : Classification et Gap Analysis (T2 2026)

La deuxième phase consiste à **classifier formellement chaque système** selon les quatre niveaux de risque de l'AI Act et à réaliser une analyse d'écarts (gap analysis) conjointe AI Act/RGPD. Pour chaque système classé à haut risque, évaluez le niveau de maturité actuel par rapport aux neuf obligations principales des articles 9 à 15 et de l'article 17, ainsi qu'aux exigences RGPD applicables. Réalisez les **DPIA et FRIA conjointes** pour tous les systèmes à haut risque traitant des données personnelles. Quantifiez les écarts identifiés

en termes d'effort (jours-homme), de coûts et de délais. Révisez les contrats avec les fournisseurs de modèles GPAI pour intégrer les clauses de conformité AI Act. Priorisez les actions en fonction des dates d'entrée en application et de la criticité des systèmes. Déterminez si certains systèmes doivent être redessinés, abandonnés ou remplacés par des alternatives moins risquées ou mieux documentées.

Phase 3 : Implémentation Opérationnelle (T3-T4 2026)

La troisième phase est la plus intensive : elle consiste à **implémenter concrètement les mesures de conformité** identifiées lors du gap analysis. Pour les systèmes à risque limité, les actions prioritaires sont la mise en œuvre de notifications de transparence conformes à l'article 50, le marquage des contenus synthétiques et la mise à jour des notices d'information RGPD. Pour les systèmes à haut risque, le programme comprend le déploiement de l'infrastructure de **logging et monitoring** (article 12), l'implémentation de pipelines de tests automatisés pour l'évaluation continue des biais et de la robustesse (article 15), la rédaction de la documentation technique complète selon l'Annexe IV, la mise en œuvre des circuits de **surveillance humaine** intégrés dans les workflows applicatifs (article 14), la formation des opérateurs humains, l'implémentation du système de gestion des risques itératif (article 9), et la préparation de l'évaluation de conformité et du marquage CE. Parallèlement, mettez en œuvre les mesures RGPD complémentaires : finalisation des DPIA, mise en conformité des notices d'information, implémentation des mécanismes d'exercice des droits (accès, rectification, effacement, opposition, intervention humaine au titre de l'article 22), et renforcement des mesures techniques de protection (chiffrement, pseudonymisation, contrôle d'accès).

Phase 4 : Gouvernance Continue et Amélioration (2027+)

La quatrième phase installe un régime de **gouvernance continue** conçu pour durer au-delà de la mise en conformité initiale. Mettez en place un **comité de gouvernance IA** transverse regroupant la direction générale, le DPO, le RSSI, les responsables juridiques, les équipes IA et les responsables métiers. Ce comité, qui se réunit au minimum trimestriellement, supervise l'ensemble du portefeuille de systèmes IA de l'organisation, valide les nouvelles classifications, examine les incidents et les résultats de monitoring, et arbitre les arbitrages entre innovation et conformité. Définissez un processus de **revue périodique** (au minimum semestrielle) de chaque système à haut risque, intégrant l'analyse des données de monitoring, les retours utilisateurs, les incidents signalés, l'évolution du contexte réglementaire et les résultats des audits internes. Implémentez un processus de **gestion du changement** pour tout nouveau déploiement ou toute modification significative d'un système IA existant, incluant une évaluation préalable de classification AI Act et de conformité RGPD. Préparez-vous aux **audits** des autorités de surveillance nationales (en France, coordination CNIL/autorité AI Act à désigner) en maintenant à jour l'ensemble de la documentation et du registre. Enfin, participez aux travaux de normalisation (CEN/CENELEC, ISO) et aux consultations de l'AI Office pour anticiper l'évolution des standards et des bonnes pratiques.

⚠ **Erreurs fréquentes à éviter :**

- ▶**Traiter AI Act et RGPD en silos :** Les deux règlements s'appliquent de manière cumulative — une gouvernance intégrée est indispensable
- ▶**Sous-estimer le shadow AI :** Les usages non contrôlés de ChatGPT/Claude par les collaborateurs peuvent constituer des violations RGPD et AI Act
- ▶**Négliger la documentation :** 70% de l'effort de conformité réside dans la documentation — commencez dès maintenant
- ▶**Confondre classification modèle et système :** La classification AI Act porte sur le système (application), pas sur le modèle sous-jacent
- ▶**Ignorer les obligations GPAI en aval :** En tant que déployeur, vous devez vérifier la conformité de vos fournisseurs de modèles

En synthèse — Les 5 principes fondamentaux :

- ▶**1. Proportionnalité :** Les obligations sont proportionnelles au risque — concentrez vos investissements sur les systèmes à haut risque
- ▶**2. Cumulativité :** RGPD et AI Act s'appliquent simultanément — une conformité IA sans conformité RGPD est illusoire
- ▶**3. Accountability :** Documentez tout — la capacité à démontrer la conformité est aussi importante que la conformité elle-même
- ▶**4. Continuité :** La conformité est un processus continu, pas un projet ponctuel — intégrez-la dans votre SMQ
- ▶**5. Anticipation :** Les normes harmonisées et les lignes directrices de l'AI Office viendront préciser les exigences — suivez leur évolution de près

Besoin d'un accompagnement expert ?

Nos consultants en cybersécurité et IA vous accompagnent dans vos projets. Devis personnalisé sous 24h.

Références et ressources externes

- CNIL — Le RGPD — Guide pratique du règlement général sur la protection des données
- ISO 27001 — Norme internationale de management de la sécurité de l'information
- CNIL — Commission nationale de l'informatique et des libertés
- ENISA — Agence européenne pour la cybersécurité
- EUR-Lex — Portail du droit de l'Union européenne

Pour approfondir ce sujet, consultez notre outil open-source rgpd-compliance-checker qui facilite la vérification automatisée de conformité RGPD.

Questions frequentes

Comment ce sujet impacte-t-il la securite des organisations ?

Ce sujet a un impact significatif sur la securite des organisations car il touche aux fondamentaux de la protection des systemes d'information. Les entreprises doivent evaluer leur exposition, appliquer des mesures preventives adaptees et former leurs equipes pour faire face aux risques associes a cette problematique.

Quelles sont les bonnes pratiques recommandees par les experts ?

Pourquoi est-il important de se former sur ce sujet en 2026 ?

En 2026, la maitrise de ce sujet est devenue incontournable face a l'evolution constante des menaces et des exigences reglementaires. Les professionnels de la cybersecurite doivent maintenir leurs competences a jour pour proteger efficacement les actifs numeriques de leur organisation et repondre aux obligations de conformite.

Sources et références : CNIL · ANSSI

Conclusion

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr