FATIMA GHILASSENE, AVOCATE

Droit du Numérique — RGPD — Intelligence Artificielle

Fournisseurs et déployeurs de solutions d'IA

Comment anticiper les risques éthiques et juridiques ?

Guide pratique à l'usage des entreprises et de leurs conseils

Mise à jour : juin 2026

Pourquoi ce guide ?

Concevoir ou déployer un système d'intelligence artificielle n'est plus une démarche purement technique. Depuis l'entrée en vigueur progressive du **Règlement européen sur l'IA (AI Act, Règlement 2024/1689)** et les exigences constantes du **RGPD**, la conformité juridique est devenue un préalable à toute mise sur le marché.

Ce guide décrypte, de manière opérationnelle, les obligations qui incombent respectivement aux **fournisseurs** (ceux qui conçoivent les systèmes) et aux **déployeurs** (ceux qui les utilisent dans leurs processus métiers). Il propose des analyses jurisprudentielles actualisées et des recommandations pratiques.

⚠ **Note liminaire : l**es dispositions substantielles de l'AI Act applicables aux systèmes à haut risque (articles 8 à 15) n'entrent pleinement en vigueur qu'en août 2026. Ce guide présente l'état du droit applicable à la date de publication et l'état du droit à venir, distincts de manière explicite.

I. Sécuriser l'entraînement des modèles : le défi des données massives

Le développement d'une IA performante repose sur la qualité et la quantité de ses données d'entraînement. Dès lors que ces données incluent des informations relatives à des personnes physiques identifiées ou identifiables, le **RGPD s'applique de plein droit dès la phase de R&D**, même avant toute commercialisation.

A. Choisir la bonne base légale (art. 6 RGPD)

En conformité avec la doctrine de la CNIL et les lignes directrices du CEPD, deux bases légales sont principalement envisagées pour la phase d'entraînement :

- **L'intérêt légitime (art. 6-1 f)** : fréquemment invoqué pour la R&D. Il exige un test de mise en balance (Legitimate Interest Assessment — LIA) démontrant que l'innovation poursuivie ne porte pas une atteinte disproportionnée aux droits fondamentaux des personnes concernées.
- **Le consentement (art. 6-1 a)** : indispensable lorsque les données sont collectées directement auprès des utilisateurs à des fins d'amélioration du modèle, ou lorsque le traitement porte sur des données sensibles au sens de l'article 9 du RGPD.

B. Appliquer une minimisation stricte des données (art. 5-1 c RGPD)

Le principe de minimisation impose de mettre en œuvre, avant la phase d'apprentissage, des techniques de pseudonymisation, de filtrage drastique et d'anonymisation irréversible. Cette étape conditionne la liceité de l'ensemble du traitement.

Jurisprudence — Clearview AI : la fin du mythe du web scraping libre

La CNIL, suivie par ses homologues italienne et grecque, a sanctionné la société **Clearview AI** d'une amende de **20 millions d'euros** pour avoir aspiré des milliards de photographies depuis internet pour entraîner un système de reconnaissance faciale.

Deux principes non négociables : (1) Le web public n'est pas une zone de non-droit : la publication d'un contenu sur un réseau social ne vaut pas consentement à sa réutilisation pour un modèle commercial. (2) Réutiliser des données en dehors de l'attente raisonnable des personnes constitue un traitement déloyal au sens de l'article 5-1 a du RGPD.

Sur le terrain du RGPD (art. 5-1 a) : la licéité du scraping de données personnelles ne dépend pas du robots.txt mais de l'existence d'une base légale valide et du respect du principe de loyauté — comme l'illustre la sanction Clearview AI. Ces deux conditions sont indépendantes l'une de l'autre et doivent chacune être vérifiées.

Sur le terrain du droit d'auteur (directive 2019/790) : vérifiez si les sites sources ont activé une clause d'opposition (opt-out / robots.txt) à l'exception TDM. Si tel est le cas, l'utilisation de ces contenus pour l'entraînement n'est pas couverte par l'exception et engage la responsabilité du fournisseur pour contrefaçon.

II. La qualité des données : le rempart contre les biais discriminatoires

Des données d'entraînement biaisées produisent des algorithmes discriminatoires, exposant leurs concepteurs à des sanctions sur le fondement du RGPD et à une interdiction de mise sur le marché au titre de l'AI Act.

A. Le cadre légal de la qualité des données

- **Principe de loyauté (art. 5-1 a RGPD) :** un algorithme qui discrimine de manière opaque ou reproduit des inégalités systémiques viole ce principe fondamental.
- **AI Act, articles 10 et 15 :** pour les systèmes à Haut Risque, les jeux de données d'entraînement, de validation et de test doivent être pertinents, représentatifs, exempts d'erreurs et complets (dispositions s'appliquant pleinement à partir d'août 2026).

B. La feuille de route pour auditer vos datasets

1. **Auditer la représentativité statistique :** le biais de représentativité survient lorsque la population cible est mal cartographiée dans l'échantillon. Il convient d'équilibrer les classes par suréchantillonnage ou diversification des sources.
2. **Traquer les « variables proxies » :** supprimer une variable sensible (sexe, âge) ne suffit pas. L'IA peut reconstruire ces variables via des critères corrélés (code postal, centres d'intérêt, établissement de formation). Des tests de robustesse algorithmique s'imposent.
3. **Exploiter la dérogation de l'AI Act (art. 10-5) :** pour vérifier l'absence de discrimination, il est parfois nécessaire de traiter des données sensibles. L'AI Act crée une dérogation expresse à l'article 9 du RGPD, à la condition stricte que ce traitement soit exclusivement destiné à détecter et corriger les biais, sous réserve de mesures de sécurité renforcées.

III. L'Analyse d'Impact (AIPD) : l'outil maître de cartographie des risques

L'Analyse d'Impact relative à la Protection des Données (AIPD ou DPIA) est obligatoire en vertu de l'**article 35 du RGPD** dès lors que le traitement présente un risque élevé (profilage à grande échelle, décision automatisée, surveillance). La CNIL a publié des listes spécifiques de traitements soumis à l'AIPD obligatoire.

Qui doit réaliser l'AIPD ?

L'obligation légale pèse exclusivement sur le **Responsable du Traitement** — c'est-à-dire le déployeur. Toutefois, le RGPD organise une collaboration structurée :

Répartition des rôles dans l'AIPD

DÉPLOYEUR (Responsable de traitement)

- Pilote et signe l'AIPD
- Analyse les risques in concreto (contexte métier, impact sur salariés/clients)
- Sollicite obligatoirement l'avis de son DPO
- Consulte la CNIL si risques résiduels élevés

FOURNISSEUR (Sous-traitant)

- Obligation légale d'assistance (art. 28-3 f RGPD)
- Fournit un « Kit de conformité » détaillant la logique de l'algorithme
- Documente les mesures de cybersécurité et la gestion des logs

- Réalise sa propre AIPD pour la phase R&D

Conseil pratique — L'AIPD en 4 étapes clés

1. **Décrire le traitement :** finalités, données traitées, acteurs, flux, durées de conservation.
2. **Évaluer la nécessité et la proportionnalité :** base légale, minimisation, respect des droits des personnes.
3. **Identifier et qualifier les risques :** accès non autorisé, modification illicite, disparition des données. Pour chaque risque, évaluer la vraisemblance et la gravité.
4. **Définir les mesures et valider les risques résiduels :** si les risques résiduels demeurent élevés malgré les mesures, consultation préalable de la CNIL obligatoire (art. 36 RGPD). Un risque est dit « résiduel » lorsqu'il subsiste après application de toutes les mesures techniques et organisationnelles raisonnablement disponibles : ni la pseudonymisation, ni le chiffrement, ni la supervision humaine ne permettent de le ramener à un niveau acceptable. C'est précisément ce seuil qui déclenche l'obligation de consultation préalable.

Exemples de risques résiduels typiques dans un projet IA

Les quatre exemples ci-dessous sont construits selon une grille constante : situation factuelle, qualification juridique du manquement résiduel, niveau de gravité au sens de l'article 35 du RGPD, et obligations correctives qui s'imposent au responsable de traitement.

1. Discrimination résiduelle dans un système de présélection algorithmique (recrutement)

Un déployeur utilise un algorithme de présélection de candidatures. Malgré la suppression formelle des variables sensibles (origine, sexe, âge), des critères de substitution conservés dans le modèle — code postal de résidence, intitulé de l'établissement scolaire — reproduisent des inégalités systémiques sans que les mesures d'audit conduites aient permis de les éliminer.

Ce risque est qualifié sur le terrain du **principe de loyauté (art. 5-1 a RGPD)** : un traitement produisant des effets discriminatoires indirects viole ce principe, indépendamment de l'intention du responsable de traitement. Ce raisonnement rejoint le test de la discrimination indirecte au sens de la directive 2000/78/CE, qui s'apprécie sur les effets concrets du critère utilisé, non sur sa forme. Le responsable de traitement ne peut se prévaloir de l'absence de discrimination directe pour s'exonérer.

La gravité est **élevée** au sens de l'article 35 RGPD : une décision de rejet en matière d'embauche produit des effets durables sur la situation économique et sociale de la personne. La vraisemblance est **modérée**. L'obligation corrective est double : garantir un droit de recours effectif devant un être humain (art. 22 RGPD) et consigner dans le registre des traitements les limites non réduites du modèle. Si le risque demeure élevé après ces mesures, la consultation préalable de la CNIL est obligatoire (art. 36 RGPD).

2. Réidentification résiduelle de données de santé pseudonymisées

Un fournisseur d'IA médicale entraîne son modèle sur des données de patients pseudonymisées selon les standards en vigueur. Malgré cette mesure, la combinaison de variables conservées — tranche d'âge, pathologie rare, établissement de soin — permet, pour certains profils au sein d'une population réduite, une réidentification

potentielle par croisement avec des bases tierces accessibles.

La qualification juridique repose sur deux fondements cumulatifs. D'une part, la **pseudonymisation ne vaut pas anonymisation** au sens du RGPD : les données demeurent des données personnelles dès lors que la réidentification est « raisonnablement possible » (considérant 26 RGPD). D'autre part, les données de santé relèvent de la **catégorie spéciale de l'article 9** : toute atteinte à leur protection est présumée causer un préjudice grave (risque de discrimination, atteinte à la vie privée, stigmatisation). Ces deux fondements se cumulent pour déterminer une exposition accrue du responsable de traitement.

La gravité est **très élevée**. La vraisemblance est **faible mais juridiquement non nulle**, ce qui suffit à maintenir l'obligation d'AIPD et, compte tenu du niveau de gravité, à déclencher la consultation préalable obligatoire de la CNIL (art. 36 RGPD) si aucune mesure complémentaire ne réduit ce risque à un niveau acceptable. L'AIPD doit explicitement mentionner ce risque subsistant, justifier pourquoi il ne peut être éliminé et décrire les protections renforcées retenues.

3. Inexplicabilité résiduelle d'une décision automatisée produisant des effets juridiques (scoring crédit)

Un établissement financier déploie un algorithme de scoring crédit et intègre des outils d'explicabilité. Les explications fournies identifient les principales variables d'influence sans permettre à la personne concernée de comprendre la logique complète de la décision individuelle qui la vise, ni d'en contester les fondements de manière éclairée.

Ce risque résiduel engage directement le **droit à l'information sur la logique sous-jacente (art. 13-2 f et 14-2 g RGPD)** et le **droit à obtenir une explication de la décision (art. 22-3 RGPD)**. La CNIL a précisé dans ses lignes directrices que l'explication doit être « intelligible et spécifique à la situation » de la personne concernée : une mention générique de la logique générale du modèle ne satisfait pas cette exigence. Le manquement est caractérisé même si l'établissement a cru s'en acquitter par la mise en place d'outils d'explicabilité partiels.

La gravité est **élevée** (refus de crédit aux effets patrimoniaux directs et immédiats). La vraisemblance est **élevée**, ce risque étant structurellement lié à l'architecture de certains modèles. L'obligation corrective est la mise en place d'une procédure de contestation humaine effectivement accessible — non fictive — et la documentation dans l'AIPD de l'inexplicabilité résiduelle comme risque non réduit, avec justification.

4. Violation potentielle de données par exposition d'un modèle génératif via API

Un fournisseur met à disposition un modèle de génération de texte via une interface de programmation ouverte. Les mesures de sécurité standard ont été appliquées. Cependant, la nature même de certains modèles entraînés sur des corpus denses peut conduire à la restitution de fragments proches des données d'apprentissage lorsque des requêtes spécialement conçues lui sont adressées.

Ce scénario constitue une **violation potentielle de données personnelles au sens de l'article 4-12 du RGPD** : la divulgation ou l'accès non autorisé, même partiel et involontaire, répond à la définition légale. L'absence de procédure de détection et de notification prédéfinie constitue elle-même un manquement à l'**obligation de sécurité (art. 32 RGPD)**, indépendamment de la survenance effective d'une violation. Dès qu'il a connaissance d'un tel événement, le fournisseur est soumis à l'obligation de notification dans les 72 heures (art. 33 RGPD), délai courant également pour le déployeur.

La gravité est **très élevée** si les données potentiellement restituées relèvent des catégories spéciales. La vraisemblance est **modérée à élevée** selon la densité du corpus. L'AIPD doit documenter ce risque résiduel ; le DPA doit prévoir contractuellement les procédures que le fournisseur s'engage à activer et les délais dans lesquels il en informera le déployeur, afin que celui-ci puisse respecter l'obligation de 72 heures vis-à-vis de la CNIL.

IV. Déterminer sa classe de risque au titre de l'AI Act

L'AI Act fonde son système d'obligations sur une **approche proportionnée aux risques**, classés en quatre catégories. Le fournisseur et le déployeur doivent co-évaluer la classification de la solution.

Niveau de risque	Exemples	Obligations
Inacceptable	Notation sociale, surveillance de masse biométrique en temps réel	**Interdit — mise sur le marché prohibée**
Haut Risque	Recrutement, scoring crédit, systèmes de santé, infrastructures critiques (art. 6 et annexe III)	Système de gestion des risques, documentation technique, marquage CE, logs automatiques (en vigueur août 2026)
Risque limité	Chatbots, générateurs de deepfakes, outils de synthèse vocale	Obligations de transparence : information que le contenu est généré par une IA
Minimal	Filtres anti-spam, systèmes de recommandation, jeux vidéo	Aucune obligation spécifique. Code de conduite volontaire recommandé

V. Le choc des qualifications : RGPD vs AI Act

Le RGPD et l'AI Act régulent l'écosystème selon deux prismes distincts et non superposables : le premier protège les dronnées personnelles, le second encadre le produit et son niveau de risque. Les rôles ne se recoupent pas automatiquement.

L'asymétrie juridique illustrée — Exemple du SaaS RH

Un éditeur logiciel fournit une solution d'IA en mode SaaS à une direction des ressources humaines pour analyser des candidatures :

- **Éditeur (fournisseur) :** sous-traitant au sens du RGPD (traitement pour le compte de la DRH via un DPA) ; fournisseur au sens de l'AI Act (responsable de la robustesse technique et de l'absence de biais dans le produit).
- **DRH cliente (déployeur) :** responsable du traitement au sens du RGPD (définit la finalité recrutement) ; déployeur au sens de l'AI Act (doit respecter la notice d'utilisation et garantir la supervision humaine).

Conséquence pratique immédiate : un contrat ne peut pas se contenter d'un DPA standard. Il doit intégrer une dimension « conformité AI Act » spécifique pour chaque partie (voir partie VIII).

VI. Les obligations spécifiques du déployeur : surveillance et espace public

Le déployeur ne peut se décharger de sa responsabilité sur son fournisseur. En tant que responsable du traitement, il porte des devoirs stricts lors de la mise en production.

La gouvernance humaine (Human-in-the-loop)

En vertu de l'**article 22 du RGPD**, le déployeur doit garantir le droit des personnes à ne pas faire l'objet d'une décision exclusivement automatisée (ex. : tri automatique de CV sans relecture humaine). Une supervision humaine effective doit être implémentée et documentée.

Jurisprudence actualisée — Caméras augmentées et espace public

CE, 30 janvier 2026, n° 506370 (Commune de Nice / CNIL) : le Conseil d'État confirme l'illégalité du traitement algorithmique automatisé des images de vidéoprotection en l'absence de base légale spécifique. L'article L. 251-2 du Code de la sécurité intérieure autorise la vidéoprotection, non l'adjonction d'une analyse algorithmique systématique. Le principe de proportionnalité ne suffit pas : même un dispositif limité et expérimental est illégal sans texte l'y autorisant expressemént.

CAA Marseille, 2020 (« Lycées de la Région Sud ») : la reconnaissance faciale biométrique ne peut se fonder sur le consentement dans un contexte de relation d'autorité entre usagers et administration.

Leçon pour l'écosystème : fournisseurs, n'allez pas commercialiser des solutions de « Smart City » algorithmiques sans vérifier la présence d'un décret ou d'une loi sectorielle d'autorisation. Déployeurs, vous portez l'entière responsabilité de l'illégalité du traitement si vous activez ces modules sans base légale adéquate.

VII. Flux internationaux, cycle de vie et souveraineté des modèles

L'encadrement des transferts hors EEE (art. 44 à 49 RGPD)

Le recours à des puissances de calcul étrangères (cloud d'infrastructure, API tierces) impose une vigilance accrue depuis l'arrêt **Schrems II** (CJUE, C-311/18). Si des données personnelles transitent vers les États-Unis, les sous-traitants doivent être certifiés au titre du **Data Privacy Framework (DPF)**. À défaut, le recours aux Clauses Contractuelles Types (SCC) associé à une analyse de risque pays tiers (Transfer Impact Assessment — TIA) est obligatoire.

Souveraineté et cycle de vie

- **Risque extraterritorial :** pour les secteurs sensibles (santé, banque, secteur public), l'usage d'API soumises au Cloud Act américain présente un risque de fuite de données souveraines. Privilégier les modèles open source hébergés sur des infrastructures SecNumCloud est devenu un argument commercial différenciant.
- **Purge post-entraînement (art. 5-1 e RGPD) :** une fois les poids mathématiques du modèle fixés, les données d'apprentissage doivent être purgées ou anonymisées de manière irréversible.
- **Machine Unlearning et droit à l'effacement (art. 17 RGPD) :** les fournisseurs doivent concevoir des architectures permettant d'effacer l'influence d'une donnée spécifique sans détruire le modèle.

VIII. Transparence et gouvernance interne : lutter contre le Shadow AI

Le « Shadow AI » est le risque opérationnel numéro un pour les déployeurs. Des collaborateurs utilisent des outils d'IA générative grand public non sécurisés pour y injecter des données clients ou des secrets d'affaires, en dehors de tout contrôle de la DSI et du DPO.

Obligations légales du déployeur en matière de gouvernance IA

- **Transparence (art. 13, 14 et 22 RGPD) :** mentionner explicitement dans la politique de confidentialité l'usage d'un système d'IA, la logique sous-jacente de l'algorithme, et garantir le droit de ne pas faire l'objet d'une décision exclusivement automatisée.
- **Sécurité des traitements (art. 32 RGPD) :** mettre en place une Charte d'usage de l'IA, former les équipes, et n'autoriser que les solutions validées par la DSI et le DPO.
- **Registre des traitements (art. 30 RGPD) :** intégrer chaque système d'IA déployé dans le registre, avec description de la logique algorithmique et durées de conservation des logs.

IX. Propriété intellectuelle et IA : entrée et sortie

Le droit d'auteur à l'entrée (données d'entraînement)

L'aspiration de contenus protégés pour l'entraînement est encadrée par l'exception de fouille de textes et de données (Text and Data Mining — TDM) de la **directive européenne 2019/790**. Si un auteur ou un éditeur exerce son droit d'opposition (opt-out), le fournisseur d'IA a l'obligation légale de retirer ces contenus de son dataset. L'AI Act impose par ailleurs la publication d'un résumé détaillé des contenus utilisés pour l'entraînement.

La titularité à la sortie (outputs générés)

En droit français et européen, une création purement générée par une IA, sans intervention humaine directe et créative, ne bénéficie pas de la protection par le droit d'auteur. Les CGS du fournisseur doivent clarifier contractuellement la répartition et la cession des droits sur les résultats générés, pour sécuriser l'exploitation commerciale du déployeur.

X. L'encadrement contractuel : au-delà du DPA classique

La répartition des risques entre fournisseur et déployeur doit être gravée dans le marbre contractuel. Face aux spécificités des LLM et de l'IA prédictive, les clauses traditionnelles de l'article 28 du RGPD doivent être profondément refondues.

A. Le DPA « Spécial IA » — deux clauses critiques

- **Clause de non-réutilisation pour l'entraînement global :** le DPA doit stipuler explicitement si le fournisseur a le droit — ou l'interdiction absolue — d'utiliser les données métiers et les requêtes (prompts) injectées par le déployeur pour améliorer ou reentraîner son modèle général.
- **Sort des données en fin de contrat :** au-delà de la restitution/suppression des bases (art. 28-3 g RGPD), le contrat doit préciser le sort des modèles personnalisés ou affinés (fine-tuned) au cours de la relation. Qui conserve la propriété des poids mathématiques ajustés grâce aux données du client ?

B. Les clauses de responsabilité produit et AI Act

- **Garantie de conformité AI Act :** le fournisseur certifie que le système a fait l'objet d'une évaluation de conformité appropriée (marquage CE si haut risque) et respecte les standards techniques européens de robustesse et de cybersécurité.
- **Clause de déchéance de qualification (art. 25 AI Act) :** toute modification substantielle de l'IA ou tout changement de finalité par le déployeur entraîne la rupture des garanties du fournisseur. La responsabilité bascule intégralement sur le déployeur, qui devient légalement le « nouveau fournisseur » du système.

XI. Matrice de gouvernance croisée (RACI de conformité)

Le tableau ci-dessous synthétise la répartition opérationnelle des responsabilités entre fournisseur et déployeur sur les principales thématiques de conformité.

Thématique	Fournisseur	Déployeur	Référence
Sourcing des données	Audite la légalité des bases externes, respecte les opt-out	Exige une garantie contractuelle d'éviction sur l'origine licite des données	CNIL, Clearview AI / art. 5 & 9 RGPD
Biais & qualité des données	Garantit la représentativité du dataset, élimine les proxies	S'assure que les données métiers injectées ne créent pas de dérive	Art. 10 AI Act / art. 5 RGPD
Analyse d'Impact (AIPD)	Fournit le kit de conformité (algorithme, sécurité, logs)	Réalise, pilote et signe l'AIPD liée au contexte métier	Art. 35 RGPD
Gouvernance contractuelle	Fournit un DPA conforme, garantit l'étanchéité des données	Valide le périmètre, interdit l'usage des prompts sensibles si non sécurisés	Art. 28 RGPD / art. 25 AI Act
Vidéoprotection / espace public	Conçoit des outils sans traitement biométrique non autorisé	Vérifie la base légale sectorielle, mène une AIPD d'infrastructure	CE, Nice (2026) / art. 5 AI Act
Droits des personnes	Intègre les fonctionnalités de Machine Unlearning	Reçoit, valide et répond aux demandes d'exercice de droits	Art. 15 à 22 RGPD
Violation de données (72h)	Alerte le déployeur sans délai indu en cas de faille SaaS	Notifie la CNIL dans les 72h et informe les personnes concernées	Art. 33 & 34 RGPD

XII. Questions fréquentes (FAQ)

Mon entreprise utilise ChatGPT ou Copilot. Est-elle concernée par ces obligations ?

Oui. Dès lors que vos collaborateurs injectent des données personnelles de clients ou de salariés dans un outil IA grand public, votre entreprise est qualifiée de déployeur. Elle doit disposer d'un DPA avec l'éditeur de l'outil, intégrer le traitement dans son registre, et mettre en place une politique interne encadrant cet usage.

L'AIPD est-elle obligatoire pour tout projet IA ?

Non. L'AIPD est obligatoire lorsque le traitement présente un risque élevé pour les droits et libertés des personnes : notamment le profilage à grande échelle, les décisions automatisées produisant des effets juridiques, et la surveillance systématique. La CNIL publie une liste des traitements soumis à AIPD obligatoire (délib. n° 2018-326 du 11 octobre 2018).

Quand les obligations « haut risque » de l'AI Act s'appliquent-elles ?

Les dispositions substantielles applicables aux systèmes à haut risque (articles 8 à 15 du règlement) entrent pleinement en vigueur en août 2026. Les interdictions relatives aux pratiques inacceptables (art. 5) sont, elles, applicables depuis février 2025. Il est conseillé d'anticiper la mise en conformité dès à présent.

Notre fournisseur IA affirme que son système est conforme RGPD. Est-ce suffisant ?

Non. La conformité RGPD du fournisseur couvre ses propres traitements en tant que sous-traitant. Elle ne dispense pas le déployeur de ses propres obligations en tant que responsable du traitement : AIPD, information des personnes, gestion des droits, et garantie de supervision humaine. La conformité se co-gère, elle ne se délègue pas.

Que risque concrètement une entreprise qui ne respecte pas ces obligations ?

Sur le terrain du RGPD : jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial annuel. Sur le terrain de l'AI Act : jusqu'à 35 millions d'euros ou 7 % du CA mondial pour les violations les plus graves (art. 99). S'y ajoutent les risques réputationnels, les procédures en responsabilité civile, et pour les systèmes haut risque, l'interdiction de mise sur le marché.

Conclusion — La conformité comme levier de croissance

Anticiper les risques éthiques et juridiques liés à l'IA exige une vision systémique. L'AI Act responsabilise fortement le concepteur en tant que fournisseur, tandis que le RGPD maintient une exigence de vigilance élevée sur le déployeur en tant que responsable du traitement.

La clé du succès réside dans la transparence contractuelle et technique : des architectures documentées, des droits clarifiés, des responsabilités assumées dès la conception. Une démarche qui transforme la contrainte réglementaire en avantage concurrentiel et en gage de pérennité.

Accompagnement du Cabinet Ghilassene

Le cabinet vous accompagne sur l'ensemble des problématiques décrites dans ce guide :

- Audit de conformité RGPD et AI Act de vos solutions IA
- Rédaction et négociation de DPA « Spécial IA » et de CGS adaptées aux LLM
- Pilotage ou assistance à la réalisation d'Analyses d'Impact (AIPD)
- Veille réglementaire et formation des équipes (DSI, DPO, direction juridique)

- Contentieux et relations avec la CNIL

Contact : contact@cabinet-ghilassene.fr

Sources et références

- Règlement (UE) 2016/679 du 27 avril 2016 (RGPD)
- Règlement (UE) 2024/1689 du 13 juin 2024 (« AI Act »)
- Directive (UE) 2019/790 du 17 avril 2019 (droit d'auteur marché unique numérique)
- CJUE, C-311/18, 16 juillet 2020 (Schrems II)
- CNIL, décision Clearview AI, 17 octobre 2022
- CNIL, délib. n° 2018-326 du 11 octobre 2018 (liste AIPD obligatoires)
- CAA Marseille, 27 novembre 2020 (« Lycées de la Région Sud »)
- CE, 30 janvier 2026, n° 506370 (Commune de Nice / CNIL)
- CEPD, lignes directrices sur l'intérêt légitime (02/2019 et actualisations)