

GUIDE ANACOFI L'INTELLIGENCE ARTIFICIELLE POUR LES CGP

Principes, un cadre réglementaire et une boîte à outils pour un usage professionnel, responsable et conforme de l'IA en gestion de patrimoine.



ANACOFI | COMMISSION TECH & INNOVATION | Édition 2026

SOMMAIRE

Sommaire	1
----------------	---

Préambule — Ce qui change durablement pour le métier de CGP	4
Chapitre 1 — Comprendre l'IA en dix minutes.....	5
L'intelligence artificielle générative.....	5
Le modèle de langage, ou LLM	5
Le prompt et la fenêtre de contexte	5
L'hallucination	5
Le RAG, une IA qui cite ses sources	5
L'agent IA	5
Chapitre 2 — Les cinq principes ANACOFI.....	6
1. Responsabilité	6
2. Confidentialité	6
3. Supervision humaine	6
4. Transparence	6
5. Traçabilité	6
Chapitre 3 — Les usages, en un tableau.....	8
Chapitre 4 — RGPD, protéger et anonymiser les dossiers clients.....	9
Le cadre en quatre points.....	9
Base légale.....	9
Minimisation.....	9
Contrat de sous-traitance (DPA).....	9
Conservation.....	9
Anonymiser et pseudonymiser un dossier client	9
Exemple, avant et après	10
Checklist, avant d'envoyer un prompt	10
Chapitre 5 — AI Act, ce qui concerne un cabinet de CGP	11
Deux rôles distincts : fournisseur et déployeur.....	11
Un calendrier progressif, mis à jour mi-2026	11
Le conseil en gestion de patrimoine est-il « à haut risque » ?	11
Chapitre 6 — Guide pratique du cabinet.....	13
Gouvernance : qui fait quoi	13
Les collaborateurs et la formation	13
Les licences	13
Les prompts	13
Les contrôles et la continuité	14
Mise en œuvre progressive	14
Chapitre 7 — Boîte à outils.....	15
Arbre de décision, avant tout usage de l'IA sur un dossier client	15
Checklist, avant d'utiliser une IA sur un dossier client	15
Guide du prompt	15
Trois cas pratiques.....	16

Glossaire — Quinze définitions à connaître	17
Conclusion — L'humain au cœur	18
Note de sources.....	18

PREAMBULE — CE QUI CHANGE DURABLEMENT POUR LES METIERS DU CONSEIL (CGP, CFE, COURTIER, ...)

Une évolution technologique majeure, comparable par son ampleur à l'arrivée d'internet dans les cabinets, et qui appelle la même exigence méthodique que toute nouveauté touchant au conseil.

L'intelligence artificielle générative permet de produire, en quelques secondes, un premier jet de note, une synthèse de texte réglementaire ou une piste d'analyse patrimoniale. Pour un cabinet de conseil en gestion de patrimoine, ce gain de temps est réel et déjà mesurable sur les tâches rédactionnelles et documentaires. Il ne change en revanche rien à la nature du métier : le devoir de conseil, le secret professionnel et la responsabilité personnelle du conseiller restent entiers, que le premier jet ait été écrit par un collaborateur ou suggéré par une IA.

Ce guide s'adresse aux CGP, CIF et courtiers adhérents, à leurs dirigeants et à l'ensemble des collaborateurs de cabinet. Il a un objectif pratique : poser un cadre commun, simple à retenir et à appliquer au quotidien, plutôt que de multiplier les mises en garde générales.

Il s'organise autour de cinq principes, d'un tableau des usages, d'un cadre réglementaire à jour au 4 août 2026, et d'une boîte à outils directement utilisable en cabinet.

CHAPITRE 1 — COMPRENDRE L'IA EN DIX MINUTES

Chaque cabinet réunit des niveaux de connaissance très différents sur l'IA. Ce chapitre pose un socle commun avant d'aborder les règles et les usages.

L'intelligence artificielle générative

L'IA générative désigne des technologies capables de créer du contenu original, texte, image ou donnée, à partir d'instructions formulées en langage naturel. ChatGPT (OpenAI), Claude (Anthropic), Perplexity et Mistral AI en sont les outils textuels les plus courants, Canva ou Genspark pour la mise en forme visuelle. Elle se distingue de l'IA dite classique, déjà présente depuis longtemps dans les outils financiers pour la détection de fraude ou le score de crédit : cette IA plus ancienne classe ou évalue, l'IA générative produit du contenu nouveau et peut converser.

Le modèle de langage, ou LLM

Un LLM, grand modèle de langage, est entraîné sur d'immenses volumes de texte pour prédire, mot après mot, la suite la plus probable d'un texte. Ce mécanisme statistique (probabiliste) explique à la fois sa puissance, une capacité de rédaction et de synthèse très large, et ses limites : le modèle ne vérifie rien, il prolonge un texte de façon plausible, y compris quand il n'a pas l'information demandée.

Le prompt et la fenêtre de contexte

Le prompt est l'instruction adressée au modèle. La qualité du résultat dépend largement de sa précision, un guide pratique du prompt est proposé au chapitre 7. La fenêtre de contexte est la quantité de texte que le modèle peut prendre en compte à un instant donné, l'échange en cours et les documents joints. Au-delà de cette limite, les éléments les plus anciens de la conversation sortent progressivement de son champ.

L'hallucination

Une hallucination est une réponse plausible mais factuellement fausse, affirmée par le modèle avec la même assurance qu'une réponse exacte. Elle découle directement du fonctionnement du LLM décrit plus haut : rien, dans le mécanisme de prédiction, ne garantit l'exactitude. À cela s'ajoutent des connaissances arrêtées à une date d'entraînement donnée, qui imposent une vigilance particulière sur l'actualité réglementaire récente. C'est la raison pour laquelle la supervision humaine, principe détaillé au chapitre 2, est non négociable pour tout livrable client.

Le RAG, une IA qui cite ses sources

Le RAG, ou génération augmentée par récupération, est une technique qui force le modèle à s'appuyer sur une base documentaire déterminée plutôt que sur sa seule mémoire d'entraînement. Elle réduit, sans le supprimer, le risque d'hallucination, et permet la citation de sources vérifiables. Perplexity par exemple, fonctionne largement sur ce principe, ce qui en fait un outil adapté à la veille réglementaire.

L'agent IA

Un agent est un système capable d'exécuter seul plusieurs actions successives, rechercher, rédiger, envoyer, sans validation humaine à chaque étape. C'est l'usage le plus risqué pour un cabinet, précisément parce qu'il retire le contrôle humain à chaque étape intermédiaire. Le chapitre 3 y revient dans le tableau des usages proscrits.

CHAPITRE 2 — LES CINQ PRINCIPES ANACOFI

Cinq principes auxquels les chapitres suivants se réfèrent.

Ces cinq principes sont des recommandations professionnelles de l'ANACOFI, destinées à guider la pratique quotidienne des adhérents.

Ils se distinguent des obligations légales strictes, détaillées aux chapitres 4 (RGPD) et 5 (AI Act), qu'ils permettent en pratique de couvrir dans leur quasi-totalité, sans s'y substituer.

1. Responsabilité

Le conseiller reste seul responsable légal et déontologique de toute recommandation, qu'elle ait été assistée par l'IA ou non. L'intelligence artificielle demeure un outil d'aide à la décision, jamais un décideur.

Le devoir de conseil impose de pouvoir expliquer et justifier chaque recommandation devant un client ou un contrôleur, ce qui suppose de comprendre ce que l'IA a produit, pas seulement de le transmettre.

Recourir à l'IA constitue un outil de diligence supplémentaire, il ne se substitue en aucun cas à l'expertise humaine, ni ne l'allège.

2. Confidentialité

Les données clients sont protégées par une minimisation et, le plus souvent, une anonymisation systématiques avant tout envoi à un outil d'IA, selon la méthode détaillée au chapitre 4.

Seuls des outils sous licence professionnelle, couverts par un contrat de sous-traitance des données signé, sont utilisés.

Aucune donnée identifiante n'est saisie dans un outil grand public.

3. Supervision humaine

Tout livrable généré ou assisté par l'IA fait l'objet d'une relecture et d'une validation humaine avant toute diffusion.

C'est le principe le plus souvent invoqué du guide, il n'est développé qu'ici : aucune recommandation, aucun courrier, aucun chiffre ne part sans un regard humain compétent, quel que soit le niveau de risque de l'usage concerné.

Le conseiller signe, pas l'IA.

4. Transparence

L'usage de l'IA est notifié au client, par une mention intégrée au document d'entrée en relation et, le cas échéant, sur les livrables assistés par l'IA.

Cette transparence sert la relation de confiance autant que la conformité, RGPD comme AI Act, développée aux chapitres 4 et 5.

5. Traçabilité

Les prompts utilisés, les résultats bruts obtenus et les sources consultées sont conservés pour chaque dossier.

En cas de contrôle, cette trace prouve la diligence professionnelle.

Elle rejoint un principe constant de la responsabilité civile professionnelle du conseiller, où les sanctions visent traditionnellement un défaut de diligence et de vérification, et non l'outil utilisé pour produire un document. Aucune décision de justice spécifique à l'usage de l'IA générative en gestion de patrimoine n'est à ce jour connue, la prudence recommande de raisonner par analogie avec ce principe établi plutôt que d'anticiper une jurisprudence qui n'existe pas encore.

À RETENIR

Responsabilité, confidentialité, supervision humaine, transparence, traçabilité. Un cabinet qui applique sérieusement ces cinq principes couvre, dans le même mouvement, l'essentiel de ses obligations RGPD et AI Act en tant qu'utilisateur d'outils d'IA, développées aux chapitres 4 et 5.

CHAPITRE 3 — LES USAGES EN UN TABLEAU

Pour chaque ligne de ce tableau détaillant un usage, sont indiqués le statut (autorisé/prudence/interdiction), une évaluation du risque RGPD et les garde-fous spécifiques, en plus de ces principes.

La colonne « Risque RGPD » évalue le seul risque lié aux données personnelles, à garde-fou appliqué.

Usage	Statut	Risque RGPD	Garde-fou spécifique
Compte rendu, note de synthèse, courrier type	Autorisé	Faible	Validation humaine avant diffusion
Veille et synthèse réglementaire	Autorisé	Faible	Exiger des sources citées et vérifiables
Formation interne, quiz et cas pratiques	Autorisé	Faible	Relecture par le référent DPO du cabinet et/ou l'expert
Analyse préliminaire patrimoniale, pistes complémentaires	Autorisé	Modéré	Utilisation en second avis uniquement, pour vérification de l'exhaustivité de la première proposition
Communication client, adaptation du ton	Prudence	Modéré	Double relecture humaine avant envoi
Modélisation de scénarios d'investissement	Prudence	Modéré	Validation experte avant toute recommandation
Rapport d'adéquation, préconisations	Prudence	Élevé	Revue intégrale par le conseiller, qui signe
Analyse fiscale complexe	Prudence	Élevé	Revue par un expert qualifié, recoupement des chiffres
Recommandation envoyée au client sans relecture	Interdit	Élevé	Contraire au principe de supervision humaine
Délégation totale de la relation client à un agent IA	Interdit	Élevé	Aucune supervision possible action par action
Saisie de données identifiantes dans un outil grand public	Interdit	Élevé	Contraire au principe de confidentialité, chapitre 4

CHAPITRE 4 — RGPD, PROTÉGER ET ANONYMISER LES DOSSIERS CLIENTS

Ce chapitre fixe le cadre légal, puis détaille, pas à pas, comment préparer un dossier client avant de le transmettre à une IA.

Le cadre en quatre points

Base légale

Pour un usage professionnel courant de l'IA, l'intérêt légitime, documenté au registre des traitements, est l'approche la plus pragmatique.

Le consentement, révocable à tout moment, est souvent trop fragile pour fonder un traitement récurrent.

Pour tout usage à risque élevé, profilage automatisé ou décision individuelle automatisée notamment, une analyse d'impact relative à la protection des données (AIPD) est obligatoire au sens de l'article 35 du RGPD.

Minimisation

Seules les données strictement nécessaires à la tâche demandée sont transmises à l'outil d'IA, conformément au principe de minimisation de l'article 5 du RGPD.

C'est le point de départ du guide d'anonymisation ci-dessous.

Contrat de sous-traitance (DPA)

Tout outil d'IA utilisé sur des données clients doit faire l'objet d'un contrat de sous-traitance conforme à l'article 28 du RGPD, un DPA (Data Processing Agreement).

Il garantit notamment que les données transmises ne servent pas à réentraîner le modèle du fournisseur.

C'est la différence essentielle entre une licence professionnelle (ChatGPT Team ou Enterprise, Claude Team ou Enterprise) et un compte grand public gratuit.

Conservation

Une politique de rétention est définie pour chaque outil, avec une suppression automatique des échanges au terme d'un délai fixé par le cabinet, par exemple trente jours, plutôt que de laisser des informations sensibles accessibles indéfiniment.

Anonymiser et pseudonymiser un dossier client

Deux techniques, à ne pas confondre, permettent de préparer un dossier avant de le transmettre à une IA.

ANONYMISATION

Selon la définition retenue par la CNIL, l'anonymisation est un traitement qui rend impossible, en pratique et de manière irréversible, toute identification de la personne, par quelque moyen que ce soit.

Une donnée réellement anonymisée sort du champ d'application du RGPD.

Trois critères permettent de vérifier qu'une anonymisation est réelle : il doit être impossible d'isoler un individu dans l'ensemble de données, de corréler deux ensembles de données entre eux, et d'inférer une information nouvelle sur la personne.

PSEUDONYMISATION

La pseudonymisation remplace les identifiants directs d'une personne, nom, prénom, par un identifiant indirect, un alias ou un numéro.

Le lien avec la personne reste traçable via une table de correspondance conservée séparément, de façon sécurisée, par le cabinet.

Une donnée pseudonymisée reste donc une donnée personnelle : le RGPD continue de s'appliquer intégralement.

Critère	Anonymisation	Pseudonymisation
Identification de la personne	Impossible	Possible, indirectement
Soumis au RGPD	Non	Oui
Réversible	Non	Oui, via la table de correspondance
Usage recommandé	Prompt envoyé à un outil d'IA tiers	Usage interne tracé au cabinet

Exemple, avant et après

AVANT, DONNÉE BRUTE

Claire Dupont, 42 avenue Foch, 75116 Paris. Patrimoine financier 4 237 845 euros. Cliente depuis 2019, contrat d'assurance vie luxembourgeois n° LU-88214.

APRÈS ANONYMISATION, POUR UN PROMPT ENVOYÉ À UNE IA TIERCE

Cliente A. Patrimoine financier proche de 4,2 millions d'euros. Région parisienne. Contrat d'assurance vie luxembourgeois.

APRÈS PSEUDONYMISATION, POUR UN USAGE INTERNE TRACÉ

Client 2026-014. Patrimoine financier 4 237 845 euros. Contrat d'assurance vie luxembourgeois n° LU-88214. Table de correspondance conservée séparément, accès restreint au cabinet.

Checklist, avant d'envoyer un prompt

Supprimer ou transformer systématiquement : nom, prénom, adresse postale, adresse électronique, numéro de téléphone, IBAN, numéro de contrat, date de naissance exacte, employeur, raison sociale d'une société, numéro fiscal, numéro ORIAS.

Puis, selon le besoin : arrondir les montants, remplacer une date précise par une tranche d'âge ou une année, remplacer une ville par une région.

CHAPITRE 5 — AI ACT, CE QUI CONCERNE UN CABINET DE CGP

Ce chapitre se concentre sur ce qui s'applique réellement à un cabinet utilisateur d'outils d'IA, en écartant les obligations techniques qui concernent les seuls éditeurs de modèles.

Deux rôles distincts : fournisseur et déployeur

Le règlement européen sur l'IA (règlement (UE) 2024/1689) distingue le fournisseur, qui développe un système d'IA et le met sur le marché sous son nom (OpenAI, Anthropic, Mistral AI), et le déployeur, qui utilise ce système sous sa propre autorité professionnelle.

Une entreprise qui utilise ChatGPT Team ou Claude Enterprise est un déployeur, jamais un fournisseur.

Ses obligations, sensiblement plus légères que celles d'un fournisseur, portent sur un usage responsable, l'information des personnes concernées et, pour les seuls systèmes à haut risque, la supervision humaine et la tenue de registres.

Un calendrier progressif, mis à jour mi-2026

Le règlement est entré en vigueur en août 2024, mais ses obligations s'appliquent par étapes.

Un paquet dit « omnibus numérique » (règlement (UE) 2026/1744), adopté au premier semestre 2026, a reporté l'échéance des systèmes à haut risque : la date de la règle et sa date d'application réelle doivent donc être distinguées.

Échéance	Ce qui s'applique
2 février 2025	Interdiction des pratiques inacceptables (manipulation, notation sociale) et obligation de culture IA (article 4) pour toute organisation utilisatrice, y compris les cabinets déployeurs.
2 août 2025	Obligations applicables aux modèles d'IA à usage général (GPAI). Elles concernent les éditeurs de modèles, non les cabinets qui les utilisent.
2 août 2026	Obligations de transparence de l'article 50 : informer les personnes qu'elles interagissent avec une IA, étiqueter les contenus générés ou manipulés destinés à être diffusés. Délai de grâce jusqu'au 2 décembre 2026 pour les systèmes déjà en service.
2 décembre 2027	Obligations applicables aux systèmes d'IA à haut risque de l'annexe III. L'échéance initiale du 2 août 2026 a été reportée par le paquet omnibus numérique.

Le conseil en gestion de patrimoine ou courtage est-il « à haut risque » ?

L'annexe III du règlement ne classe en haut risque que des cas d'usage précis et limités dans les services financiers : l'évaluation de la solvabilité et le score de crédit des particuliers, ainsi que la tarification et l'évaluation du risque en assurance vie et santé.

La rédaction assistée, la synthèse réglementaire, l'analyse préliminaire patrimoniale ou la communication client n'entrent pas dans cette catégorie.

Un cabinet qui ne pratique pas de score de crédit automatisé ni de tarification algorithmique d'assurance n'a, en l'état de ses usages, aucun système d'IA à haut risque au sens strict du texte.

Cette qualification s'apprécie cas par cas et se réévalue à chaque évolution de l'usage de l'IA du cabinet.

CE QU'IL FAUT RETENIR

En tant que déployeur, appliquer sérieusement les cinq principes du chapitre 2 couvre l'essentiel des obligations de l'AI Act qui concernent un cabinet de CGP.

Documenter, dans le registre RGPD déjà tenu, les outils d'IA utilisés, leur fournisseur et la base légale retenue.

Suivre l'échéance du 2 août 2026 sur la transparence, qui reste d'application malgré le report des règles sur le haut risque.

CHAPITRE 6 — GUIDE PRATIQUE DU CABINET

Une gouvernance claire détaille les responsabilités du cabinet, de ses collaborateurs pour le choix et l'utilisation des licences, des prompts et les contrôles. Si votre entreprise utilise des I.A vous avez des obligations.

Gouvernance : qui fait quoi

Question	Rôle responsable
Qui valide les outils autorisés ?	Le référent DPO du cabinet, souvent le dirigeant ou un associé désigné
Qui choisit les licences et signe les DPA ?	Le dirigeant ou l'associé gérant
Qui met à jour la bibliothèque de prompts ?	Le référent DPO, avec les conseillers qui l'utilisent
Qui réalise les audits périodiques ?	Le référent conformité, interne ou externe au cabinet
Qui gère un incident (fuite, résultat suspect) ?	Le référent DPO, à alerter sans délai par tout collaborateur
Qui suit les évolutions réglementaires ?	Le référent DPO, qui met à jour la charte au moins une fois par an

Les collaborateurs et la formation

Un parcours à trois niveaux, qui s'appuie sur les chapitres précédents plutôt que de les répéter.

Niveau	Public	Contenu
1. fondamentaux	Tous les collaborateurs, dès l'arrivée	Chapitres 1 à 3 : comprendre l'IA, les cinq principes, le tableau des usages
2. intermédiaire	Conseillers, rappel semestriel	Prompts avancés (chapitre 7), procédures internes, checklist de validation
3. expert	Référent DPO, gouvernance	Pilotage des risques, audits de biais, veille réglementaire (chapitre 5)

Rythme recommandé : onboarding obligatoire à l'arrivée, rappel annuel, atelier pratique annuel.

Les licences

Toujours une licence professionnelle avec DPA signé, jamais un compte grand public gratuit pour des données clients. Vérifier, avant de retenir un outil, ses certifications de sécurité, ISO 27001, ISO 42001, SOC 2.

Configurer, quand l'outil le permet, une politique de rétention courte et la désactivation de l'entraînement des modèles du fournisseur sur les données du cabinet.

Les prompts

Une bibliothèque de prompts validés par le cabinet pour les tâches récurrentes, méthode détaillée au chapitre 7. Exiger, pour toute recherche ou synthèse réglementaire, que l'outil cite ses sources.

Les contrôles et la continuité

La checklist de validation du chapitre 7 s'applique avant toute diffusion.

Un journal des vérifications documente qui a validé quoi, et quand.

Le cabinet conserve un mode de fonctionnement sans IA pour ses tâches essentielles, testé au moins une fois par an, pour absorber une interruption de service ou un changement tarifaire brutal d'un fournisseur.

En cas d'erreur visible d'un client ou d'un tiers, un protocole simple prévoit qui contacte le client, qui documente l'incident et qui communique si nécessaire.

Mise en œuvre progressive

Phase	Durée	Priorités
1. pilote	Mois 1 à 3	Usages à faible risque uniquement, checklist et bibliothèque de prompts, formation initiale de tous les collaborateurs
2. déploiement encadré	Mois 4 à 9	Licences professionnelles et DPA signés, référent DPO désigné, DER et registre RGPD mis à jour, formation avancée par métier
3. optimisation	Mois 10 à 18	Audit des biais et de la qualité, mesure du temps gagné et du taux d'erreur, test grandeur nature du mode sans IA

CHAPITRE 7 — BOITE A OUTILS

Un arbre de décision, une checklist, un guide du prompt et trois cas pratiques, prêts à être utilisés en cabinet.

Arbre de décision, avant tout usage de l'IA sur un dossier client

1. Le résultat sera-t-il diffusé au client, sous quelque forme que ce soit (document, message, recommandation) ?

Non Usage interne uniquement. La checklist ci-dessous suffit.

Oui Passer à la question 2.



2. Les données transmises à l'IA contiennent-elles des données personnelles d'un client, anonymisées ou pseudonymisées au préalable (chapitre 4) ?

Non Interdit tant que les données n'ont pas été anonymisées ou pseudonymisées.

Oui Aucune donnée identifiante en jeu, ou anonymisation faite. Passer à la question 3.



3. L'outil utilisé est-il couvert par une licence professionnelle avec DPA signé (chapitre 4) ?

Non Interdit. Changer d'outil ou repasser en usage strictement interne.

Oui Passer à la question 4.



4. Le résultat a-t-il été relu et validé par un collaborateur compétent avant diffusion ?

Non Interdit tant que la validation humaine n'a pas eu lieu.

Oui Autorisé. Diffusion possible, mention de l'usage de l'IA si nécessaire (chapitre 2).

Checklist, avant d'utiliser une IA sur un dossier client

- ☐ Licence professionnelle avec DPA signé
- ☐ Données minimisées, puis anonymisées ou pseudonymisées (chapitre 4)
- ☐ Prompt enregistré dans la bibliothèque du cabinet ou noté dans le dossier
- ☐ Résultat relu et vérifié par un collaborateur compétent
- ☐ Sources citées et contrôlées
- ☐ Validation humaine actée avant toute diffusion au client
- ☐ Mention de l'usage de l'IA ajoutée si le livrable en porte la trace

Guide du prompt

À ÉVITER

« Fais un rapport d'adéquation. » Aucune donnée fournie, aucune limite posée : le modèle comble les vides de sa propre initiative, c'est-à-dire qu'il hallucine.

À PRIVILÉGIER

« Tu es un assistant rédactionnel pour un conseiller en gestion de patrimoine français.

Tu te réfères aux Guide pratique I.A., Livret et Kits Réglementaires de l'Adhérent de l'ANACOFI pour t'assurer de respecter exigences réglementaires et bonnes pratiques.

Tu rédiges un premier projet de rapport d'adéquation à partir des éléments suivants [coller les données anonymisées].

Tu ne crées aucune donnée manquante, tu écris « information manquante » si nécessaire.

Tu cites les textes que tu connais avec leur référence exacte. Ce projet sera relu et validé par le conseiller avant tout envoi. »

Trois règles suffisent.

- Donner le contexte, qui rédige, pour qui, dans quel cadre
- Fournir des données déjà anonymisées
- Poser des limites explicites, ne rien inventer, signaler les manques, citer les sources

Trois cas pratiques

- **Veille réglementaire.**

Un conseiller utilise Perplexity pour résumer une nouvelle réglementation.

Il vérifie chaque source citée avant de mettre à jour sa note interne. Principes mobilisés : supervision humaine et traçabilité.

- **Rapport d'adéquation.**

Un premier projet est généré à partir de données anonymisées.

Un expert du cabinet vérifie chiffres et références, corrige, puis le conseiller signe avant l'envoi au client.

Principes mobilisés : responsabilité et statut « Prudence » du chapitre 3.

- **Ce qu'il ne faut pas faire.**

Un collaborateur copie le nom complet, l'adresse et le montant du patrimoine d'un client dans un compte ChatGPT gratuit pour rédiger un courrier personnalisé.

Cet usage est interdit au sens du chapitre 3 : les données identifiantes ne doivent jamais être saisies dans un outil grand public, chapitre 4.

GLOSSAIRE - QUINZE DEFINITIONS A CONNAITRE

Agent IA. Intelligence artificielle capable d'exécuter seule plusieurs actions successives, sans validation à chaque étape.

AIPD. Analyse d'impact relative à la protection des données, étude obligatoire avant tout traitement RGPD à risque élevé, article 35.

Anonymisation. Suppression irréversible de toute possibilité d'identifier une personne. Une donnée anonymisée sort du champ du RGPD.

DPA. Contrat de sous-traitance des données (Data Processing Agreement), obligatoire avec tout fournisseur d'IA traitant des données clients, article 28 du RGPD.

Déployeur. Personne ou organisation qui utilise un système d'IA sous sa propre autorité professionnelle, sans l'avoir développé.

Fenêtre de contexte. Quantité de texte qu'un modèle d'IA peut prendre en compte à un instant donné.

Fournisseur, au sens AI Act. Personne ou organisation qui développe un système d'IA et le met sur le marché sous son nom.

GPAI. Modèle d'IA à usage général, catégorie visée par l'AI Act, qui concerne les éditeurs de modèles plus que leurs utilisateurs professionnels.

Hallucination. Réponse plausible mais factuellement fausse, produite avec assurance par un modèle d'IA.

IA générative. Technologie capable de créer du contenu original, texte, image ou donnée, à partir d'instructions en langage naturel.

LLM. Grand modèle de langage, entraîné sur d'immenses volumes de texte pour prédire la suite la plus probable d'un texte.

Minimisation. Principe posé par l'article 5 du RGPD, qui impose de ne collecter et de ne transmettre que les données strictement nécessaires à la tâche en cours, jamais un dossier complet par commodité.

Prompt. Instruction adressée à un système d'IA.

Pseudonymisation. Remplacement des identifiants directs d'une personne par un identifiant indirect, réversible via une table de correspondance. Reste soumise au RGPD.

RAG. Technique consistant à faire travailler une IA à partir d'une base documentaire déterminée plutôt que de sa seule mémoire, pour réduire le risque d'hallucination et permettre la citation de sources.

Système à haut risque. Catégorie de l'AI Act soumise aux obligations les plus strictes, limitée à une liste précise de cas d'usage, annexe III, qui ne couvre pas, en l'état, le conseil en gestion de patrimoine dans son ensemble.

CONCLUSION — L'HUMAIN AU CŒUR

« L'IA doit être considérée comme un stagiaire ou un assistant, jamais comme un décideur autonome. »

Les cinq principes du guide présentés en Chapitre 2, responsabilité, confidentialité, supervision humaine, transparence, traçabilité, suffisent à couvrir l'essentiel.

Un cabinet qui les applique sérieusement satisfait, dans le même mouvement, à ses obligations de déployeur au sens du RGPD et de l'AI Act.

La valeur ajoutée du CGP reste l'alliance de la puissance technologique et du jugement humain, pas leur substitution.

Note de sources

Règlement (UE) 2024/1689 établissant des règles harmonisées concernant l'intelligence artificielle (AI Act) et règlement (UE) 2026/1744 portant paquet dit « omnibus numérique ».

Règlement (UE) 2016/679 relatif à la protection des données à caractère personnel (RGPD), articles 4, 5, 28 et 35. CNIL, définitions et critères de l'anonymisation et de la pseudonymisation des données personnelles.

Commission européenne, direction générale des réseaux de communication, du contenu et des technologies, lignes directrices sur les obligations de transparence de l'article 50.

Rédaction achevée le 4 Août 2026 avec l'assistance de Claude.