



NODE PULSE

Guide complet

GUIDE COMPLET

IA en cabinet : travailler sans exposer les données clients

Guide pratique à destination des experts-comptables

Édition · 24 août 2026

node-pulse.com/ressources/ia-cabinet-donnees-clients

Informations vérifiées au 24 août 2026. Les conditions des fournisseurs évoluent régulièrement. Ce guide présente un état du droit et des conditions des fournisseurs à la date indiquée ci-dessus. Il ne constitue pas une consultation juridique et ne dispense pas d'un avis sur une situation particulière.

REPÈRES

Pourquoi ce guide

I.

Les outils d'intelligence artificielle sont entrés dans les cabinets plus vite que les règles pour les utiliser. Les démonstrations sont partout — rédaction de courriers, préparation d'entretiens, analyse de balances — et la question des données clients y est presque toujours expédiée en une ligne, quand elle est posée.

Or l'expert-comptable est dépositaire d'un secret protégé par la loi pénale, responsable ou sous-traitant au sens du RGPD selon les traitements, et tenu par un code de déontologie qui encadre jusqu'à la manière de formuler une proposition. Utiliser l'IA au cabinet est parfaitement possible ; le faire sans exposer les données clients suppose de comprendre ce que le droit impose déjà, où vont réellement les données, et ce qu'il faut exiger d'un fournisseur avant de signer. Ce guide a été écrit pour cela. Il ne recommande aucun éditeur et reste utilisable quel que soit l'outil que votre cabinet retiendra.

SOMMAIRE

- | | |
|--|---|
| 01 Le cadre qui s'applique déjà quand des données clients sortent du cabinet | 02 Où vont réellement les données une fois le message envoyé |
| 03 Six situations à risque, et pourquoi elles posent problème | 04 La checklist : dix questions à poser au fournisseur avant de signer |
| 05 Travailler proprement dès aujourd'hui : cinq mesures à la portée de tout cabinet | 06 Comment Node Pulse a tranché |

Le cadre qui s'applique déjà quand des données clients sortent du cabinet

— Le secret professionnel : une infraction pénale, pas une clause de confidentialité

La base textuelle tient en deux articles qui se lisent ensemble : l'article 21 de l'ordonnance n° 45-2138 du 19 septembre 1945 soumet les experts-comptables, leurs salariés autorisés et les stagiaires au secret professionnel « dans les conditions et sous les peines fixées par l'article 226-13 du code pénal », lequel punit d'un an d'emprisonnement et de 15 000 euros d'amende la révélation d'une information à caractère secret par une personne qui en est dépositaire par état ou par profession (article 226-13 du code pénal dans sa version en vigueur depuis le 1er janvier 2002 ; article 21 de l'ordonnance de 1945 dans sa version en vigueur depuis le 24 décembre 2016 — Légifrance, consulté le 24 août 2026).

Deux décisions de la Cour de cassation en fixent la portée, plus large qu'on ne le croit souvent. La première : « quel que soit l'objet de la mission dont il est chargé par contrat, l'expert-comptable est tenu à un secret professionnel relativement aux faits qu'il n'a pu connaître qu'en raison de la profession qu'il exerce » (Cass. civ. 1re, 10 septembre 2015, n° 14-22.699, publié au Bulletin, cassation) : le périmètre du secret n'est pas celui de la lettre de mission. La seconde : la révélation « n'en suppose pas la divulgation ; qu'elle peut exister légalement, lors même qu'elle en est donnée à une personne unique et lors même que cette personne est elle-même tenue au secret » (Cass. crim., 16 mai 2000, n° 99-85.304, publié au Bulletin, rejet). Cet arrêt concerne un avocat, mais il définit la notion de « révélation » au sens de l'article 226-13, qui est commune à tous les dépositaires d'un secret professionnel — et c'est à ce titre qu'il vaut ici. Il ferme deux raisonnements courants : « ce n'est pas public, donc ce n'est pas une divulgation », et « le prestataire s'est engagé à la confidentialité, donc c'est couvert ».

Les trois cas de levée prévus par l'alinéa 4 de l'article 21 sont tous défensifs (le professionnel poursuivi ou mis en cause) : aucun ne couvre une transmission choisie pour travailler plus vite. L'alinéa 1 réserve par ailleurs les autres dispositions législatives qui peuvent, dans des cas particuliers, imposer une communication.

Et le cas précis d'un service d'IA ? À la date de ce guide, aucune décision publiée, aucun texte et aucune position officielle vérifiable ne tranche expressément cette situation. Ce qui suit est donc un raisonnement, à prendre comme tel. Dans le cas type d'une balance nominative collée dans un assistant grand public, la configuration de fait est celle que visent les textes cités : un dépositaire par profession, une information connue en raison de cette profession, et une transmission hors du cabinet — dont la Cour de cassation a jugé, dans l'arrêt de 2000, qu'elle peut constituer une révélation même faite à une personne unique et elle-même tenue au secret. Deux questions restent entières, et aucune source ne permet aujourd'hui de les trancher : celle de l'élément intentionnel de l'infraction, et celle de savoir si un prestataire purement technique, sans accès humain aux contenus, est un « tiers » au sens de la révélation pénale ou le prolongement matériel du cabinet. La formulation honnête est donc : le risque pénal ne peut pas être écarté, et personne ne peut affirmer aujourd'hui que ce serait un délit ou que ce n'en serait pas un.

Une précision pratique : recueillir l'accord écrit du client est une précaution utile, mais sa portée sur le terrain pénal n'est pas tranchée — le consentement du client ne figure pas parmi les cas de levée du secret énumérés par l'alinéa 4 de l'article 21.

— Le RGPD : la question préalable est « qui décide de quoi »

Le RGPD ne parle pas d'IA en particulier ; il parle de traitements, et il commence par une question de rôle : le responsable du traitement « détermine les finalités et les moyens du traitement », le sous-traitant traite « pour le compte du responsable du traitement » (article 4 du RGPD, texte consulté sur cnil.fr le 24 août 2026).

Appliquée au cabinet, cette grille donne deux situations nettes et une zone discutée. Pour ses propres traitements — dossiers clients, facturation, ressources humaines — le cabinet est responsable du traitement. Quand il traite pour le compte du client des données dont celui-ci détermine finalités et moyens (la paie du personnel du client, typiquement), il est sous-traitant : brancher une IA sur ces données ajoute un sous-traitant ultérieur, ce qui suppose une autorisation écrite préalable du client, « spécifique ou générale » (article 28.2 du RGPD) : une autorisation générale est possible, à condition que le client soit informé de tout ajout de sous-traitant et puisse s'y opposer. Pour les traitements comptables et fiscaux eux-mêmes, la qualification du cabinet est discutée en doctrine ; la question à se poser, traitement par traitement, reste la même : qui détermine les finalités et les moyens ?

Quand le cabinet fait appel à un fournisseur d'IA, l'article 28 impose un contrat de sous-traitance comportant des mentions précises : traitement sur instruction documentée, confidentialité des personnes autorisées, mesures de sécurité (article 32), encadrement de la sous-traitance ultérieure, restitution ou suppression en fin de contrat, contribution aux audits. Ce ne sont pas des bonnes pratiques mais des mentions obligatoires, et elles forment l'ossature de la checklist de la section 4.

Un point commande tout le reste, et la CNIL l'a explicité dans sa fiche « Déterminer la qualification juridique des fournisseurs de systèmes d'IA » du 8 avril 2024 : un fournisseur qui constitue sa base d'entraînement pour son propre compte agit en responsable de traitement. Quand un fournisseur réutilise vos messages pour entraîner ses modèles, il ne traite plus seulement pour votre compte mais pour le sien, et le cabinet ne peut plus s'abriter derrière son contrat de sous-traitance. Voilà pourquoi la question « mes contenus servent-ils à l'entraînement, par défaut ? » passe avant toutes les autres.

Dernier étage : les transferts hors de l'Union européenne. Ils sont encadrés, pas interdits : ils supposent une base valable au titre du chapitre V du RGPD — décision d'adéquation (article 45) ou garanties appropriées, dont les clauses contractuelles types de la Commission (article 46). Pour les États-Unis, la décision d'adéquation du 10 juillet 2023 (décision d'exécution (UE) 2023/1795, dite Data Privacy Framework) a été confirmée par le Tribunal de l'Union européenne le 3 septembre 2025 (aff. T-553/23, Latombe / Commission), qui a jugé que les États-Unis assuraient un niveau de protection adéquat à la date d'adoption de cette décision, et a rappelé que la Commission doit surveiller en continu l'évolution du cadre américain et peut suspendre, modifier ou abroger sa décision. Cet arrêt pouvait faire l'objet d'un pourvoi, limité aux questions de droit, devant la Cour de justice (communiqué de presse CJUE n° 106/25 du 3 septembre 2025). Les deux versions antérieures du cadre, Safe Harbor et Privacy Shield, ont chacune été invalidées. C'est donc une base valable mais réversible ; à service équivalent, une architecture qui n'en dépend pas — hébergement dans l'Union, ou clauses contractuelles types doublées de mesures techniques — vieillira mieux.

— Le code de déontologie : les articles que presque personne ne cite

Le code de déontologie des professionnels de l'expertise comptable (chapitre des articles 141 à 169 du décret n° 2012-432 du 30 mars 2012, trente-trois articles au total) ne comporte aucune disposition consacrée au recours à un prestataire technique, à l'externalisation informatique ou à l'hébergement des données. Il encadre le recours à des collaborateurs (article 148) et la collaboration rémunérée avec d'autres professionnels sur une affaire déterminée (article 162), mais aucun de ces deux textes n'a été écrit pour un fournisseur de logiciel. Ce sont donc les devoirs généraux qui s'appliquent — et ils suffisent largement. Précision utile : ces obligations pèsent sur les professionnels et, pour celles qui ne concernent pas les seules personnes physiques, sur les sociétés d'expertise comptable elles-mêmes (article 141, alinéa 2). Trois dispositions s'appliquent directement à la manière d'utiliser ces outils.

L'article 147 institue, « sans préjudice de l'obligation au secret professionnel », un devoir de discrétion « dans l'utilisation de toutes les informations » dont le professionnel a connaissance dans le cadre de son activité. Ce devoir s'ajoute au secret et vise l'utilisation des informations, pas seulement leur révélation : il couvre l'hypothèse même qui nous occupe.

L'article 145, 2° impose de « donner à chaque question examinée tout le soin et le temps qu'elle nécessite, de manière à acquérir une certitude suffisante avant de faire toute proposition » : reprendre telle quelle une réponse d'IA sans la contrôler, c'est ne pas acquérir cette certitude. Le 1° du même article impose de tenir à jour sa culture professionnelle, ce qui fonde une obligation de comprendre ces outils plutôt que de les ignorer. Enfin, la lettre de mission (article 151) est le véhicule naturel pour informer le client de l'usage d'outils d'IA, même si le texte n'impose pas cette mention.

Et une fois l'outil adopté ? L'article 150 impose d'apprécier, avant d'accepter une mission, la possibilité de l'exécuter conformément aux textes, puis d'examiner périodiquement, pour les missions récurrentes, « si des circonstances nouvelles ne remettent pas en cause la poursuite de celles-ci ». Un changement de conditions contractuelles, l'ajout d'un sous-traitant ou un déplacement de l'hébergement sont des circonstances nouvelles. Le réexamen n'est pas une précaution de confort.

Où vont réellement les données une fois le message envoyé

Mécaniquement, un « prompt » est une transmission : le texte que vous collez, pièce jointe comprise, quitte le cabinet et est traité sur les serveurs du fournisseur, parfois chez ses propres sous-traitants. La revue des conditions de trois fournisseurs parmi les plus utilisés, faite sur leurs pages officielles le 24 août 2026, en tire trois enseignements.

À RETENIR

La ligne de partage ne passe pas entre fournisseurs, elle passe entre offres.

Chez les trois éditeurs examinés, l'offre commerciale n'entraîne pas les modèles sur les contenus clients par défaut, tandis que l'offre grand public le fait ou peut le faire. Au 24 août 2026 :

● **OpenAI.**

Grand public (ChatGPT) : les conversations servent par défaut à l'amélioration des modèles, sauf désactivation dans les réglages ; les conversations temporaires ne sont ni historisées ni utilisées pour l'entraînement ; en revanche, l'envoi d'un retour (pouce levé ou baissé) peut transmettre la conversation entière à l'entraînement, même après désactivation ; les conversations sont conservées tant qu'elles ne sont pas supprimées, une conversation supprimée étant purgée sous trente jours, sauf dé-identification préalable ou obligations légales (help.openai.com, pages consultées le 24/08/2026). Offres professionnelles (ChatGPT Business, Enterprise) : pas d'entraînement par défaut, partage sur choix explicite (même source). API : les données envoyées ne servent pas à entraîner les modèles sauf partage explicite, engagement qu'OpenAI date du 1er mars 2023 (developers.openai.com, guide « Your data », consulté le 24/08/2026) ; journaux de surveillance des abus conservés 30 jours par défaut, option de non-conservation soumise à l'approbation préalable d'OpenAI, résidence des données en Europe proposée sous conditions contractuelles supplémentaires (même source).

● **Anthropic.**

Grand public (Claude Free, Pro, Max) : l'utilisation des conversations pour l'entraînement relève d'un choix explicite de l'utilisateur (annonce officielle du 28 août 2025) ; conservation de cinq ans si ce choix est activé, de 30 jours sinon. Offres commerciales et API : les conditions commerciales du 17 juin 2025 excluent l'entraînement sur les contenus clients ; sur l'API, les contenus ne sont pas conservés par défaut, avec des exceptions documentées fonctionnalité par fonctionnalité. Point peu connu : au 24 août 2026, l'API d'Anthropic en direct ne propose pas de résidence des données dans l'Union européenne — les seules zones d'inférence disponibles sont « global » et « us ». Le constat ne vaut pas pour les mêmes modèles distribués via un fournisseur de cloud, où la région dépend de ce dernier (platform.claude.com, documentation data residency, consultée le 24/08/2026).

● Mistral AI.

Grand public (Le Chat) : les entrées et sorties servent à l'entraînement, sauf opposition de l'utilisateur depuis son compte (politique de confidentialité en vigueur au 27 juillet 2026) ; conversations conservées jusqu'à leur suppression. Offre commerciale et API : les conditions commerciales du 5 août 2026 excluent l'entraînement sauf choix explicite ; sur les API, surveillance des abus sur 30 jours glissants (hors offre Agents, au régime documenté séparément). Hébergement dans l'Union européenne par défaut, avec deux réserves documentées : le point d'entrée API américain entraîne un hébergement aux États-Unis, et certaines fonctionnalités peuvent occasionner des transferts temporaires hors de l'Union, encadrés par des clauses contractuelles types (help.mistral.ai, consulté le 24/08/2026).

“ Un cabinet dont un collaborateur utilise un compte personnel gratuit et un cabinet sous contrat entreprise chez le même éditeur ne sont donc pas dans la même situation juridique. C'est le message central de ce guide.

À RETENIR

« Pas d'entraînement » ne veut pas dire « pas de conservation ».

Chez OpenAI comme chez Mistral, des journaux de surveillance des abus sont conservés trente jours par défaut sur les API. Chez Anthropic, les contenus de l'API ne sont pas conservés par défaut, mais plusieurs fonctionnalités et certains modèles imposent une conservation documentée, de l'ordre de trente jours. Autrement dit, « combien de temps ? » et « pour quoi faire ? » sont deux questions distinctes, et les deux se posent — y compris chez un éditeur qui annonce ne rien conserver.

À RETENIR

L'hébergement dans l'Union européenne n'est pas acquis, y compris chez ceux qui l'annoncent.

Au 24 août 2026, aucun des trois éditeurs examinés ne permet d'écrire « données hébergées en Europe » sans réserve : l'un ne propose pas de résidence européenne sur son API, l'autre la propose sous conditions supplémentaires, le troisième héberge dans l'Union par défaut avec des exceptions documentées. La vérification se fait ligne à ligne, offre par offre.

Un mot enfin sur les transferts vers les États-Unis. La décision d'adéquation ne bénéficie qu'aux organisations effectivement inscrites sur la liste publique du Data Privacy Framework : au 24 août 2026, ni OpenAI ni Anthropic n'y figurent sous ces dénominations (dataprivacyframework.gov/list, consultée le 24/08/2026). Leurs transferts depuis l'Espace économique européen reposent donc sur les garanties de l'article 46 du RGPD, et c'est ce que disent leurs contrats : celui d'Anthropic (date d'effet du 24 février 2025) s'appuie sur les clauses contractuelles types de la Commission ; celui d'OpenAI (version mise à jour au 1er décembre 2025, entrée en vigueur le 1er janvier 2026) prévoit que les transferts hors de l'EEE se font « sur la base d'accords contenant des clauses contractuelles types (CCT) [...] ou d'une décision d'adéquation émise par la Commission européenne en vertu de l'article 45 du RGPD », et précise que les clients de l'EEE contractent avec OpenAI Ireland Ltd, OpenAI agissant en sous-traitant (documents consultés le 24/08/2026). Cela ne rend ces transferts ni illégaux ni suspects : la base juridique à vérifier est simplement contractuelle, et non l'adéquation. Première vérification à faire de votre côté : rechercher sur la liste le nom exact de l'entité juridique avec laquelle vous contractez, qui n'est pas toujours celui de la marque.

03

SECTION

Six situations à risque, et pourquoi elles posent problème

01

La balance nominative collée dans un assistant grand public. C'est le cas type de tout ce qui précède : une information couverte par le secret professionnel, transmise à un tiers, sur une offre où le contenu peut par défaut servir à l'entraînement — c'est-à-dire à un traitement que le fournisseur opère pour son propre compte. Une seule manipulation concerne chaque étage du cadre de la section 1.

02

Le compte personnel d'un collaborateur. Un compte gratuit personnel place le cabinet dans la situation la plus défavorable : conditions grand public, aucun contrat de sous-traitance avec le fournisseur, aucune visibilité sur les réglages — l'opposition à l'entraînement, quand elle existe, se fait compte par compte. Le cabinet supporte les obligations sans avoir aucun des leviers.

03

« J'ai enlevé les noms, donc c'est bon. » Retirer les noms réduit le risque sans le supprimer. Des données pseudonymisées restent des données personnelles au sens du RGPD, car une personne identifiable indirectement reste identifiable (article 4, 1) et 5)) : « le gérant de la SELARL d'ophtalmologie de quatre associés à Bayonne » n'a plus de nom et reste parfaitement reconnaissable. Et le secret professionnel couvre les faits, pas seulement les identités. Seule une anonymisation réellement irréversible fait sortir du champ du RGPD, et elle est difficile à atteindre sur des données comptables détaillées.

04

« Le fournisseur a signé un DPA, donc c'est réglé. » Le contrat de sous-traitance est nécessaire ; il ne règle pas à lui seul la question du secret professionnel, qui est de nature pénale. La Cour de cassation a jugé qu'une révélation peut exister même faite à une personne elle-même tenue au secret : un engagement contractuel de confidentialité ne répond pas à cette question-là.

05

L'extension ou le connecteur branché sur le dossier sans examen. Une extension qui lit le dossier client pour « assister » le collaborateur est un sous-traitant comme un autre, souvent adossé à un fournisseur d'IA qui en est un second. L'article 28 du RGPD impose de ne faire appel qu'à des sous-traitants présentant des garanties suffisantes et d'encadrer la chaîne de sous-traitance ultérieure : un outil qu'on ne peut rattacher ni à un contrat, ni à une localisation, ni à une politique d'entraînement identifiée ne devrait pas voir passer de données clients. Le cas particulier des outils de prospection alimentés avec des données issues des dossiers mérite d'être nommé : les moyens employés pour la promotion et le démarchage sont expressément soumis au respect du secret professionnel (article 152, alinéa 2 du code de déontologie).

06

Une sixième situation ne concerne pas les données mais les livrables : reprendre la réponse de l'outil sans la contrôler. L'article 145, 2° du code de déontologie impose d'acquiescer une certitude suffisante avant toute proposition ; la sortie d'une IA est une matière première à vérifier, pas un avis.

04

SECTION

La checklist : dix questions à poser au fournisseur avant de signer

Une question précède les dix autres, et elle s'adresse au cabinet, pas au fournisseur.

QUESTION 0

Question 0 — Quelles informations vais-je réellement soumettre, et lesquelles puis-je ne pas soumettre ?

Si le contenu transmis ne permet ni d'identifier un client ni de lui rattacher un fait, aucune des dix questions suivantes ne se pose. C'est la seule mesure qui supprime le risque au lieu de l'encadrer — et ce n'est pas que du bon sens : c'est le principe de minimisation des données (article 5.1 c) du RGPD).

Puis, au fournisseur :

1. Les contenus que je vous transmets servent-ils à entraîner vos modèles ? Par défaut, ou seulement si je l'active ? La réponse est-elle la même pour l'offre que je souscris et pour votre offre grand public ?

Fondement : article 28.3 a) du RGPD — traitement sur instruction documentée uniquement ; un réemploi pour entraînement fait basculer le fournisseur vers la qualité de responsable de traitement (fiche CNIL du 8 avril 2024).

2. Combien de temps conservez-vous mes contenus, et pour quelle finalité ? Existe-t-il une option de non-conservation, et à quelles conditions ?

Fondement : articles 5.1 e) et 28.3 g) du RGPD ; la non-conservation est parfois soumise à l'approbation préalable de l'éditeur.

3. Où mes données sont-elles traitées et stockées ? Puis-je imposer une région, et couvre-t-elle à la fois l'inférence et le stockage ?

Fondement : article 44 du RGPD ; la distinction entre lieu de calcul et lieu de stockage est documentée chez au moins un éditeur majeur.

4. Si des données sortent de l'Union européenne, sur quelle base juridique — décision d'adéquation, clauses contractuelles types, les deux ? Pouvez-vous me communiquer les clauses signées ?

Fondement : articles 45 et 46 du RGPD ; décision d'exécution (UE) 2023/1795 du 10 juillet 2023, confirmée par le Tribunal de l'UE le 3 septembre 2025 (aff. T-553/23).

5. Me faites-vous signer un contrat de sous-traitance comportant les huit engagements de l'article 28.3 ? Puis-je le lire avant de souscrire ?

Fondement : article 28.3 a) à h) du RGPD ; un DPA accessible seulement après signature du contrat commercial est déjà une réponse.

6. Quelle est la liste de vos sous-traitants ultérieurs, où sont-ils situés, et comment suis-je informé d'un ajout ? Quel délai ai-je pour m'y opposer ?

Fondement : articles 28.2 et 28.4 du RGPD, et article 150, alinéa 2 du code de déontologie (réexamen périodique des missions récurrentes en cas de circonstances nouvelles) ; les délais d'objection observés vont de 10 à 15 jours — il faut une procédure interne pour les tenir.

7. Dans quels cas un humain peut-il lire mes contenus, et vos personnels sont-ils soumis à un engagement de confidentialité ?

Fondement : articles 28.3 b) et 32.4 du RGPD ; c'est aussi la question la plus directement reliée au secret professionnel (Cass. crim., 16 mai 2000, n° 99-85.304 : une révélation peut exister même envers une personne elle-même tenue au secret).

8. Quelles mesures techniques protègent mes contenus — chiffrement en transit et au repos, cloisonnement entre clients, journalisation des accès — et sur quelles preuves puis-je m'appuyer (rapport SOC 2, certification ISO 27001) ?

Fondement : article 32.1 a) à d) du RGPD.

9. Quel droit d'audit m'accordez-vous — sur pièces, sur site, à quelle fréquence, à quels frais ?

Fondement : article 28.3 h) du RGPD ; en pratique, la vraie valeur de la question est de savoir quelles certifications l'éditeur produit à la place d'un audit sur site.

10. À la fin du contrat, que deviennent mes données — restitution, suppression, dans quel délai, avec quelle preuve, et sous quel format puis-je récupérer ce que j'ai produit ?

Fondement : article 28.3 g) du RGPD, et article L. 123-22 du code de commerce (conservation des documents comptables et pièces justificatives pendant dix ans) — un outil qui ne restitue pas dans un format exploitable crée un problème de conservation, pas seulement de confort.

La plupart de ces questions correspondent à des mentions que l'article 28 rend obligatoires dans le contrat ; un fournisseur sérieux y répond vite et par écrit.

Travailler proprement dès aujourd'hui : cinq mesures à la portée de tout cabinet



Trier avant d'envoyer.

C'est la question 0 : dans la grande majorité des usages — reformuler un courrier, structurer une note, préparer une trame d'entretien — rien n'impose de transmettre des données identifiantes. Pseudonymisez le reste, en gardant à l'esprit les limites vues en section 3.



Passer sur les offres professionnelles, et fermer la porte aux comptes personnels.

La différence entre offre grand public et offre commerciale est le premier déterminant de votre situation juridique : entraînement par défaut ou exclu, contrat de sous-traitance ou pas, réglages centralisés ou individuels. Un cabinet qui tolère les comptes personnels a, de fait, une politique IA qu'il ne connaît pas.



Écrire une règle d'usage interne courte.

Quels outils sont autorisés, sous quels comptes, pour quelles tâches, avec quelles données — et qui répond aux notifications du fournisseur, les délais d'objection à un nouveau sous-traitant se comptant en jours. Une page suffit, à condition que chacun l'ait lue. Ce n'est pas qu'une bonne pratique : les sociétés d'expertise comptable veillent à ce que les professionnels qu'elles emploient adoptent le comportement qu'exige le code (article 145, dernier alinéa), et l'article 150 impose de réexaminer périodiquement les missions récurrentes quand les circonstances changent — les conditions d'un fournisseur d'IA en font partie.



Informez le client.

La lettre de mission (article 151 du code de déontologie) est le véhicule naturel d'une mention sur l'usage d'outils d'IA, même si aucun texte ne l'impose. Recueillir l'accord écrit du client est une précaution utile, dont la portée sur le terrain pénal n'est pas tranchée.



Contrôler les sorties comme on contrôle un travail de collaborateur.

L'exigence de certitude suffisante de l'article 145, 2° du code de déontologie s'applique à toute proposition, quelle qu'en soit la source. Cela vaut aussi pour la communication du cabinet : un contenu de promotion doit être exact, non trompeur et « exempt de tout élément comparatif » (article 152, alinéa 4) — une page web rédigée par une IA et publiée sans contrôle s'expose sur ce terrain-là aussi ; et le 1° du même article fait de la compréhension de ces outils une composante de la mise à jour de votre culture professionnelle. La formation des équipes fait partie de la conformité, au même titre que les contrats.

Comment Node Pulse a tranché

Node Pulse développe des outils de conseil pour les cabinets d'expertise comptable. La question traitée dans ce guide s'est posée à nous en tant qu'éditeur ; voici ce que nous avons retenu.

Les fonctions d'IA de Node Pulse reposent exclusivement sur Mistral AI, éditeur français, sous offre commerciale et avec un contrat de sous-traitance signé : dans ce cadre, les données ne servent pas à l'entraînement des modèles sauf choix explicite du client — choix que nous n'avons pas activé, et que nous vérifions dans la console de l'éditeur — et l'hébergement est dans l'Union européenne par défaut, avec les réserves documentées par l'éditeur, rappelées en section 2 — réserves que nous avons vérifiées pour les fonctionnalités que nous utilisons.

L'architecture est fermée par conception : aucun mécanisme de bascule vers un autre fournisseur n'existe dans le produit. Si le service d'IA est indisponible, la fonctionnalité l'est aussi ; les données ne partent jamais vers un fournisseur qui n'aurait pas été examiné selon les mêmes critères que ceux de la section 4.

Nous ne revendiquons ni label ni certification de conformité — il n'existe d'ailleurs pas de certification RGPD générale. Les cabinets qui veulent vérifier ces choix peuvent nous poser les dix questions de la section 4 ; c'est exactement ce à quoi elles servent.

Guide établi le 24 août 2026 à partir de textes consultés en source primaire (Légifrance, cnil.fr, curia.europa.eu) et des pages officielles des fournisseurs cités, aux dates de consultation indiquées dans le corps du texte. Ce document ne constitue pas une consultation juridique.
