

SÉCURITÉ DES LLMs POUR L'USAGE JURIDIQUE

Livre blanc comparatif sur la confidentialité, la rétention des données et la conformité des modèles de langage pour les cabinets d'avocats.
Analyse approfondie d'OpenAI, Anthropic, Google et Mistral AI.



Confidentiel
Juillet 2025

CABINET D'AVOCATS
Intelligence artificielle & conformité juridique

Sommaire exécutif

Ce livre blanc compare les garanties de sécurité et confidentialité offertes par les principaux fournisseurs de modèles de langage (LLMs) pour un usage en cabinet d'avocats, où les données manipulées sont hautement sensibles et protégées par le secret professionnel.

Les cabinets d'avocats doivent porter une attention particulière à la confidentialité des données, la politique de rétention, et la conformité réglementaire lors du choix d'un LLM.

Points clés de l'analyse

- La **Zero Data Retention (ZDR)** est un critère essentiel pour garantir qu'aucune donnée client n'est conservée par le fournisseur du LLM
- Tous les fournisseurs étudiés (OpenAI, Anthropic, Google, Mistral) proposent des options de sécurité avancée, mais avec des différences significatives
- Les offres **Enterprise** sont systématiquement recommandées par rapport aux versions grand public
- La **souveraineté des données** et le respect du RGPD sont des avantages compétitifs pour certains fournisseurs (Mistral)

Recommandations principales

L'activation d'un accord Zero Data Retention, la minimisation des données envoyées et le déploiement d'une politique de gouvernance interne sont les trois piliers d'une utilisation sécurisée des LLMs en cabinet d'avocats.

Table des matières

1	Introduction	p.4	5	Google (Gemini)	p.9
	Contexte et enjeux de l'IA générative dans le secteur juridique			Sécurité sur Vertex AI et options de configuration	
2	Enjeux de sécurité	p.5-6	6	Mistral AI	p.10
	Confidentialité, rétention des données, conformité RGPD et auditabilité			Focus sur la souveraineté européenne des données	
3	OpenAI (GPT-4)	p.7	7	Tableau comparatif	p.11-12
	Analyse des garanties de confidentialité et conformité			Synthèse des garanties de sécurité par fournisseur	
4	Anthropic (Claude)	p.8	8	Recommandations	p.13-15
	Sécurité et politique de rétention des données			Bonnes pratiques et conclusion pour un usage juridique sécurisé	

1 Introduction

L'IA générative dans le secteur juridique

Les cabinets d'avocats manipulent quotidiennement des données hautement confidentielles : contrats, analyses juridiques, informations client, stratégies contentieuses. Avec l'essor de l'intelligence artificielle générative, les modèles de langage (LLMs) offrent des opportunités sans précédent pour automatiser et optimiser certaines tâches juridiques.

Cependant, l'utilisation de ces modèles soulève des questions fondamentales en matière de confidentialité, de secret professionnel et de conformité réglementaire. Comment s'assurer que les données sensibles envoyées à ces systèmes ne seront ni conservées, ni réutilisées, ni exposées à des tiers non autorisés ?

Objectif de cette étude comparative

Analyser et comparer les garanties de sécurité et de confidentialité offertes par les principaux fournisseurs de LLMs (OpenAI, Anthropic, Google et Mistral AI) afin d'identifier les solutions les plus adaptées aux exigences strictes du secteur juridique français et européen.



Confidentialité



Rétention des
données



Conformité RGPD



Sécurité

Enjeux de sécurité pour les LLMs juridiques

Les cabinets d'avocats manipulent quotidiennement des données hautement confidentielles (contrats, analyses juridiques, données clients). L'utilisation des modèles de langage (LLMs) dans ce contexte soulève des enjeux critiques de sécurité et de confidentialité.

Le secret professionnel des avocats exige des garanties techniques et juridiques particulièrement robustes pour l'usage de l'IA générative.

Confidentialité absolue des données

Les prompts et réponses peuvent contenir des informations couvertes par le secret professionnel. Ces données ne doivent être ni accessibles à des tiers non autorisés, ni réutilisées sans consentement explicite pour l'entraînement des modèles.

Rétention des données

De nombreux services conservent par défaut les journaux de requêtes pendant plusieurs jours ou semaines. Pour un cabinet d'avocats, il est crucial de minimiser cette durée, voire d'obtenir une garantie de non-rétention (ZDR).

Conformité réglementaire

Le traitement doit respecter le RGPD (principes de finalité, minimisation et durée de conservation). Les certifications (SOC 2, ISO 27001) et la localisation de l'hébergement (UE vs. hors UE) sont cruciales pour la conformité.

Cas d'usage sensibles

L'analyse de contrats ou la génération d'actes juridiques requièrent une traçabilité (audit logs) et une maîtrise totale sur l'accès aux données, leur stockage et leur éventuel déploiement dédié (cloud privé ou on-premise).

Conséquences d'une défaillance de sécurité

Une fuite de données confidentielles pourrait entraîner des violations du secret professionnel, des sanctions disciplinaires, des poursuites judiciaires pour violation du RGPD, et une perte irrémédiable de confiance des clients.

Confidentialité des données et Zero Data Retention (ZDR)

Le Zero Data Retention (ZDR) est un principe de sécurité selon lequel aucune donnée client n'est conservée par le fournisseur de service au-delà du traitement immédiat de la requête. Pour les cabinets d'avocats manipulant des informations confidentielles, c'est une garantie essentielle.

En l'absence de ZDR, les prompts et réponses peuvent être conservés pendant 24h à 30 jours sur les serveurs du fournisseur, créant un risque pour le secret professionnel.

Pourquoi la ZDR est critique

- **Secret professionnel** : obligation déontologique des avocats de protéger les informations des clients
- **Risques juridiques** : responsabilité en cas de divulgation de données confidentielles
- **Conformité RGPD** : principe de minimisation et de limitation de la conservation
- **Exposition aux lois extraterritoriales** : Cloud Act, FISA pour les fournisseurs américains

Rétention standard des LLMs

- **OpenAI** : conservation jusqu'à 30 jours par défaut
- **Anthropic** : conservation jusqu'à 30 jours par défaut
- **Google Gemini** : cache de 24h par défaut + métadonnées 30 jours
- **Mistral AI** : varie selon l'offre (conservation pour les offres gratuites, option ZDR pour les offres pro)

Impact concret du ZDR

Le ZDR garantit qu'après traitement, **aucune trace des documents confidentiels** (contrats, analyses juridiques, correspondances client) ne subsiste sur les serveurs du fournisseur, éliminant ainsi le risque de fuites ultérieures, d'accès non autorisé ou de réquisitions légales.

Comment obtenir des garanties ZDR

- Souscrire aux **offres professionnelles** (Enterprise/Business) des fournisseurs
- Demander **explicitement l'activation du ZDR** (option non automatique)
- Formaliser cette garantie dans un **avenant contractuel** au DPA RGPD
- Envisager les **solutions autohébergées** pour un contrôle total

OpenAI (GPT-4) – Confidentialité & conformité

OpenAI propose GPT-4 via son API et ChatGPT Enterprise avec plusieurs mesures de sécurité adaptées aux besoins des cabinets d'avocats.

Sécurité des données

- Chiffrement systématique en transit (TLS 1.2+)
- Chiffrement au repos (AES-256)
- Accès interne limité et contrôlé
- Programme bug bounty actif

Rétention des données

- Par défaut: conservation 30 jours
- Mode Zero Data Retention (ZDR) disponible
- ZDR uniquement pour clients Enterprise/Business
- Pas de réutilisation pour entraînement (par défaut)

Certifications et conformité

- Certification SOC 2 Type II (contrôles internes)
- Data Processing Addendum (DPA) RGPD disponible
- Accord BAA pour secteur santé (HIPAA)
- Option de résidence des données dans l'UE pour clients Enterprise

Évaluation pour l'usage juridique

OpenAI offre un cadre de sécurité adapté aux cabinets d'avocats, à condition de:

- Passer par l'API en mode ZDR (via contrat Enterprise)
- Obtenir des garanties contractuelles (DPA + ZDR)
- Considérer Azure OpenAI pour une conformité renforcée

Sans accord ZDR, la conservation 30 jours représente un risque en cas de faille ou réquisition légale aux États-Unis.

Pour respecter pleinement le secret professionnel et le RGPD, un cabinet d'avocats devrait utiliser GPT-4 uniquement via l'offre Enterprise avec garanties contractuelles appropriées.

Anthropic (Claude) – Sécurité & politique de données

Anthropic, avec son modèle Claude, a mis l'accent sur la confidentialité pour répondre aux exigences des entreprises manipulant des données sensibles, notamment dans le secteur juridique.

🕒 Rétention des données

- Par défaut, stockage des données clients API pendant 30 jours maximum
- Claude Enterprise permet une durée de rétention personnalisable
- Option **Zero Data Retention (ZDR)** disponible pour l'API sous accord spécifique avec approbation préalable

🛡️ Utilisation des données

- Engagement à ne pas utiliser les entrées/sorties pour entraîner Claude sans consentement
- Données issues des produits commerciaux (Claude Enterprise, API) non utilisées pour l'amélioration du modèle

Les clients Enterprise d'Anthropic peuvent définir leur propre politique de rétention des données, voire obtenir une garantie de non-rétention (ZDR) pour les cas d'usage les plus sensibles.

Certifications et conformité

- ISO/IEC 27001:2022 (système de management de la sécurité de l'information)
- ISO/IEC 42001:2023 (nouvelle norme relative aux systèmes de management de l'IA)
- Audit SOC 2 Type I puis Type II complété avec succès
- Addendum RGPD (DPA) disponible pour les clients européens
- Business Associate Agreement pour les clients santé soumis à HIPAA

Point d'attention pour cabinets d'avocats

Claude est accessible via la plateforme AWS Bedrock, qui offre nativement une non-rétention des prompts. Cette approche peut constituer une isolation supplémentaire, l'exécution se faisant au sein du cloud AWS avec logs seulement en mémoire.

Google (Gemini) – Sécurité sur Vertex AI

Google propose Gemini via sa plateforme cloud Vertex AI avec un engagement fort pour la confidentialité des données. Sa politique "AI/ML Privacy Commitment" stipule que les clients gardent le contrôle total sur leurs données.

Politique de rétention des données

Cache de 24 heures

Par défaut, les modèles mettent en cache les requêtes et réponses pendant 24h pour accélérer les interactions ultérieures, isolées par projet client.

Option Zero Data Retention

Possibilité de désactiver complètement le cache au niveau du projet pour obtenir une rétention zéro des prompts et sorties.

Métadonnées techniques

Logs techniques conservés 30 jours sans contenir le texte intégral des prompts si le cache est désactivé.

Non-utilisation des données

Aucune utilisation des données client pour entraîner les modèles sans consentement explicite (Section 17 des conditions de service).

Infrastructure et conformité

- Certifications multiples : ISO/IEC 27001 (sécurité), ISO/IEC 27701 (vie privée), SOC 2 Type II, SOC 3
- Choix de la région d'hébergement des données : configuration possible pour n'utiliser que des ressources UE
- Addendum RGPD (CDPA) intégré aux contrats Google Cloud
- Options de clé de chiffrement gérée par le client et Private Link pour isoler le trafic

Pour atteindre un véritable ZDR avec Gemini, les cabinets d'avocats doivent désactiver le cache 24h et s'assurer d'avoir un contrat entreprise Google Cloud.

Avantages pour les cabinets d'avocats

Avec les bonnes configurations (cache désactivé, pas de grounding search), Vertex AI offre un niveau de sécurité très élevé. Attention toutefois : même si les données restent en Europe, Google reste soumis au Cloud Act américain.

Mistral AI – Souveraineté des données

Mistral AI est une startup française qui développe des LLMs en mettant l'accent sur la confidentialité et la souveraineté européenne des données. Contrairement à ses concurrents américains, Mistral propose des déploiements hybrides ou entièrement on-premise en plus des options cloud.

La souveraineté numérique européenne est au cœur de l'offre de Mistral AI, avec la possibilité d'héberger intégralement les modèles dans l'environnement du client.

Politique de rétention et usage des données

- Pour les clients **Le Chat Enterprise** et **Plateforme API** (offres professionnelles), Mistral n'utilise pas les données pour entraîner ses modèles (désactivé par défaut)
- Mode **Zero Data Retention** disponible sur demande pour l'API (aucune donnée conservée après traitement)
- Mistral OCR fonctionne en ZDR par défaut (aucune image scannée n'est conservée)
- Options de déploiement on-premise permettant un contrôle total des données sans exposition externe



Certifications & conformité

Conformité SOC 2 Type II, ISO/IEC 27001/27701, entreprise 100% européenne (hors Cloud Act/FISA)



Hébergement & localisation

Serveurs en France/UE, architecture privacy-by-design avec contrôles d'accès stricts

Avantage pour cabinets d'avocats

Mistral offre le plus haut niveau de contrôle sur les données juridiques sensibles grâce à son modèle d'hébergement flexible (cloud sécurisé ou on-premise), sa politique ZDR et sa conformité RGPD native. Pour des workflows juridiques très confidentiels, c'est une option de choix pour éviter toute exposition des données.

Tableau comparatif des garanties de sécurité

Le tableau ci-dessous compare les principales caractéristiques de sécurité et confidentialité des quatre fournisseurs de LLMs étudiés, avec une attention particulière aux éléments critiques pour les cabinets d'avocats.

Fournisseur	Rétention des données (par défaut)	Zero Data Retention (ZDR)	Non-utilisation des données client	Certifications & conformité	Hébergement / Localisation
OpenAI (GPT-4)	API : 30 jours max. ChatGPT Enterprise : configurable	✓ Disponible via contrat Enterprise (sur demande)	✓ Par défaut pour clients API	SOC 2 Type II DPA RGPD CSA STAR	USA par défaut Option résidence UE (Enterprise)
Anthropic (Claude)	API : 30 jours (suppression auto) Claude Enterprise : configurable	✓ Clients Enterprise sur approbation Via AWS Bedrock également	✓ Pour clients Enterprise/API ⚠ Possible pour Free/Pro (opt-out)	ISO 27001/27701 ISO 42001 (IA) SOC 2 Type II DPA RGPD	Infrastructure US (AWS/GCP) Pas encore d'option EU-only
Google (Gemini)	Cache 24h (désactivable) Métadonnées 30 jours	✓ Par configuration technique : désactiver cache + compte Enterprise	✓ Engagement contractuel ferme	ISO 27001/27701 SOC 2/3 Nombreuses certifications Google Cloud DPA RGPD	Datacenters mondiaux Option région UE ⚠ Soumis Cloud Act (USA)
Mistral AI	API : durée minimale Le Chat Enterprise : configurable	✓ Pour API (demande motivée) ✓ Déploiement on-premise	✓ Pour clients Enterprise/API ⚠ Possible pour Free/Pro (opt-out)	ISO 27001/27701 SOC 2 Type II DPA RGPD Conformité européenne native	✓ EU-only : France/UE Option on-premise Hors champ Cloud Act

Points clés de la comparaison

Tous les fournisseurs proposent des options ZDR mais avec des modalités différentes. Mistral offre l'avantage de la souveraineté européenne et du déploiement on-premise, tandis que les autres fournisseurs compensent par des certifications et des contrôles plus matures. Pour un cabinet d'avocats français, le choix dépendra de la sensibilité des données et de l'importance accordée à la juridiction applicable.

Cas pratiques & cas d'usages sensibles

Les cabinets d'avocats exploitent les LLMs pour diverses tâches impliquant des données confidentielles. L'adéquation des garanties de sécurité doit être évaluée en fonction du niveau de sensibilité de chaque usage.



Analyse de contrats sensibles

Risque élevé

- Extraction de clauses contractuelles confidentielles
- Analyse de risques sur accords stratégiques
- **Précaution** : ZDR obligatoire, contrat Enterprise, pseudonymisation des parties



Due diligence & M&A

Risque élevé

- Traitement de données financières confidentielles
- Analyse de documents stratégiques sensibles
- **Précaution** : Instance privée/isolée recommandée (ex: Mistral on-premise)



Recherche jurisprudentielle

Risque modéré

- Requêtes incluant des éléments de fait spécifiques
- Résumé de décisions pour analyse
- **Précaution** : Offres Business, anonymisation des données client



Génération de documents types

Risque modéré

- Création de contrats modèles, mises en demeure
- Personnalisation de templates juridiques
- **Précaution** : Vérification manuelle, pas de données identifiantes

Précautions opérationnelles par fournisseur

Fournisseur	Usage très sensible (M&A, contentieux)	Usage moyennement sensible (recherche, rédaction)
OpenAI	API Enterprise + ZDR activé + DPA	ChatGPT Enterprise avec minimisation des données
Anthropic	Claude API Enterprise + ZDR + AWS Bedrock	Claude Enterprise avec historique contrôlé
Google	Vertex AI + cache désactivé + contrat Enterprise	Vertex AI avec minimisation des données
Mistral	Déploiement on-premise ou API avec ZDR	Le Chat Enterprise avec historique limité

Bonnes pratiques pour cabinets d'avocats

Les cabinets d'avocats peuvent tirer parti des LLMs tout en préservant la confidentialité des données en appliquant ces bonnes pratiques de gouvernance et de sécurité.

✓ Choisir les offres Enterprise

Privilégier exclusivement les versions professionnelles des LLMs (ChatGPT Enterprise, Claude Enterprise, Vertex AI, Mistral Le Chat Enterprise) qui offrent des garanties contractuelles et des contrôles d'accès renforcés.

🛡️ Exiger la Zero Data Retention

Négocier un accord ZDR avec le fournisseur ou configurer l'API pour supprimer immédiatement les données après traitement (désactivation du cache sur Vertex AI, mode ZDR sur OpenAI API).

🏠 Minimiser et pseudonymiser

N'envoyer que les informations strictement nécessaires.
Remplacer les données identifiantes (noms, adresses) par des pseudonymes avant transmission au LLM.

🔒 Utiliser réseaux privés

Privilégier les connexions sécurisées via VPN ou Private Link (Azure Private Link, AWS PrivateLink) pour éviter que les données transitent sur Internet public.

🌐 Vérifier la localisation

Configurer l'hébergement en Europe quand c'est disponible (région EU sur Google Vertex AI, option EU-only sur ChatGPT Enterprise, serveurs français pour Mistral).

📋 Auditer les interactions

Mettre en place un journal interne des requêtes (date, utilisateur, empreinte du document). Utiliser les outils d'audit des offres Enterprise pour tracer l'usage.

👤 Former les utilisateurs

Sensibiliser les collaborateurs aux risques et aux bonnes pratiques. Désigner un référent IA qui valide les cas d'usage sensibles et suit les évolutions techniques.

🖥️ Évaluer l'autohébergement

Pour les cabinets très stricts, étudier l'option de déployer un modèle open-source (Mistral, Llama) sur vos propres serveurs, éliminant tout risque de fuite externe.

Point clé à retenir

L'application de ces bonnes pratiques permet aux cabinets d'avocats d'exploiter les avantages des LLMs (efficacité accrue, assistance à la recherche juridique) tout en respectant strictement leurs obligations de confidentialité et de secret professionnel.

Conclusion : ZDR et sécurité, conditions d'un usage responsable

L'analyse comparative des quatre principaux fournisseurs de LLMs montre que la technologie peut être utilisée par les cabinets d'avocats en respectant les exigences de confidentialité, à condition de mettre en place les garanties nécessaires.

L'accord Zero Data Retention constitue aujourd'hui une protection essentielle pour garantir que les données confidentielles ne persistent pas au-delà de leur traitement immédiat.

Sécurité selon le fournisseur

- **OpenAI et Anthropic** : ZDR via contrat Enterprise spécifique, conservation 30j par défaut
- **Google** : ZDR via configuration technique (cache off), options de résidence des données
- **Mistral** : Avantage souveraineté, ZDR API sur demande, déploiement on-premise possible

En l'absence de ZDR

- Minimiser drastiquement les données envoyées (pseudonymisation)
- Envisager une solution autohébergée (modèles open source)
- Limiter l'usage aux contenus les moins sensibles
- Établir des clauses contractuelles spécifiques (DPA renforcé)

Responsabilité du cabinet

Quelle que soit la solution choisie, le cabinet d'avocats reste responsable de la protection des données qu'il traite. Formation des collaborateurs, traçabilité des usages et évaluation régulière des risques sont indispensables pour une utilisation éthique et sécurisée des LLMs.

Points de vigilance pour l'avenir

- Surveiller l'évolution des modèles et des conditions d'utilisation (OpenAI, Anthropic, etc.)
- Rester informé des évolutions réglementaires (AI Act européen et ses impacts)
- Anticiper les besoins d'audit et de traçabilité croissants dans le cadre juridique



Contact & Remerciements

Pour approfondir la discussion sur la sécurité des LLMs

Contact

AI Tomorrow Solutions

✉ contact@tomorrowsolutions.fr

☎ +33 (0)7 84 26 19 44

🌐 www.tomorrowsolutions.fr

Équipe

Antoine Billotte

Robin Pellaton

Remerciements

Nous tenons à remercier l'ensemble des professionnels et organisations qui ont contribué à cette étude, notamment les équipes techniques d'OpenAI, Anthropic, Google et Mistral AI pour les précisions apportées sur leurs infrastructures respectives. Nous remercions également la CNIL pour ses éclairages sur l'application du RGPD aux technologies d'IA, ainsi que l'Ordre des Avocats de Paris pour son soutien dans la diffusion de ces bonnes pratiques.

Ressources complémentaires

 [Guide complet \(PDF\)](#)

 [Boîte à outils techniques](#)

 [Modèles de clauses contractuelles](#)

 [Webinaire : LLMs & secret professionnel](#)

 [Formations et événements](#)