

Hidden Tokens face à la grille de lecture IA du CNB

Le Conseil national des barreaux résume chaque outil d'IA qu'il a audité par une fiche de dix champs. Voici ces dix champs remplis pour Hidden Tokens. Chaque réponse renvoie à ce qui permet de la vérifier ; quand un champ ne s'applique pas, nous le disons et nous disons pourquoi.

Tardigrade SARL · mis à jour le 24 octobre 2026 · versions décrites : appli de bureau 0.8.0, connecteur 2.22.0, extension navigateur 0.3.0

EN BREF

- **Hidden Tokens n'est pas un outil d'IA juridique de plus.** C'est la couche qui code le dossier sur le poste de l'avocat avant qu'il n'atteigne l'outil d'IA choisi par le cabinet, puis remet les vraies valeurs dans le résultat, sur le même poste. Il ne remplace pas ces outils : il rend leur usage défendable.
- **« Où sont hébergées les données ? » Elles ne quittent pas le poste.** Hidden Tokens n'a pas de serveur ; l'éditeur ne reçoit ni fichier, ni clé, ni journal.
- **Deux champs portent sur le LLM et un sur la RAG** (champs 1, 3 et 7). Hidden Tokens n'est ni un LLM ni une RAG : ces champs sont sans objet pour lui, et nous disons ce que le LLM reçoit à la place — des codes.
- **Chaque affirmation pointe vers une preuve** : un contrôle que vous faites vous-même sur le poste, un fichier du code source (ouvert à l'audit), ou un engagement du contrat.

Pourquoi ce dossier

La grille de lecture du CNB (1^{re} édition, juin 2025, v1.2) classe quatre critères de souveraineté ; le deuxième est la nationalité de l'entreprise qui héberge les données des clients (le quatrième applique la même règle au LLM). Elle écarte les entreprises dont le droit national permet des réquisitions extraterritoriales, « comme les entreprises américaines en l'état actuel de leur législation ». Pour éliminer ces risques, elle ne retient que deux voies : l'anonymisation totale préalable des données, ou l'installation du LLM sur les systèmes du cabinet. Le guide du CNB sur la déontologie et l'IA (avril 2026) élargit la première : il recommande de pseudonymiser ou d'anonymiser systématiquement les données avant tout outil d'IA générative.

Sur les quinze fiches de synthèse de la grille, d'après notre décompte, quatorze citent une société américaine parmi celles qui hébergent le LLM (la quinzième porte « N/A »), et neuf ne déclarent rien sur la pseudonymisation ou l'anonymisation (« N/C » ou « N/A »). Ce n'est pas un reproche fait à ces outils : les grands modèles sont, pour l'essentiel, hébergés par des sociétés américaines. C'est la place de Hidden Tokens. Placé en amont de l'outil d'IA, il fait que le LLM, où qu'il soit hébergé, ne reçoit que des codes, et que la clé qui permet de les relire reste au cabinet.

Où se place Hidden Tokens

LE POSTE DU CABINET

Le dossier en clair.
Hidden Tokens code les
noms, sociétés,
identifiants et montants
sensibles. La clé reste ici.



L'OUTIL D'IA CHOISI

Claude, ChatGPT, Gemini,
Copilot ou un outil d'IA
juridique. Il reçoit NOM-
001 , SOCIETE-003 , jamais
les valeurs.



RETOUR SUR LE POSTE

Hidden Tokens remet les
vraies valeurs dans le
Word ou l'Excel produit.
Rien ne repart.

La fiche du CNB décrit donc ici deux choses distinctes : l'outil d'IA, son LLM et ses serveurs, qui gardent leur propre fiche ; et ce que cet outil reçoit, que Hidden Tokens réduit à des codes. Les réponses ci-dessous concernent Hidden Tokens. Pour l'outil d'IA lui-même, sa fiche reste la référence.

Deux chemins mènent à l'outil d'IA. **Les fichiers** (Word, Excel, PDF, texte, scans) sont codés en une copie déposée dans le sous-dossier `Hidden-Tokens/` ; c'est elle qu'on donne à l'IA, par Claude Desktop ou par dépôt dans n'importe quel outil. **La saisie en ligne** est codée par l'extension navigateur sur ChatGPT, claude.ai, Gemini et Copilot, à ce jour seulement.

La fiche de synthèse

1 LIEU D'HÉBERGEMENT DU LLM

Sans objet : Hidden Tokens n'est pas un LLM et n'en héberge aucun. Le LLM de l'outil choisi ne reçoit que des codes.

2 LIEU D'HÉBERGEMENT DES DONNÉES

Le poste de l'utilisateur ; le registre commun, chiffré, sur le partage de fichiers du cabinet. Aucun serveur Hidden Tokens.

3 SOCIÉTÉ HÉBERGEANT LE LLM (NATIONALITÉ)

Sans objet : c'est le fournisseur d'IA choisi par le cabinet (Anthropic, OpenAI, Google, Microsoft : américaines).

4 SOCIÉTÉ HÉBERGEANT LES DONNÉES (NATIONALITÉ)

Aucune société tierce : le cabinet lui-même. L'éditeur, Tardigrade SARL, marocaine, ne reçoit aucune donnée.

5 RÉUTILISATION DES DONNÉES DES CLIENTS PAR LE LLM

Ce que le LLM pourrait réutiliser se réduit à des codes. Preuve locale : le journal « Ce que Claude a vu ».

6 CHIFFREMENT DES DONNÉES

Registre commun en AES-256-GCM, clés de poste dans le trousseau du système, clé détenue par le cabinet seul. Clé d'un poste seul : droits du compte, sans chiffrement propre.

7 RAG SÉCURISÉE

Sans objet : Hidden Tokens ne construit aucun index. Un outil qui indexe la copie codée n'indexe que des codes.

8 PSEUDONYMISATION / ANONYMISATION

Pseudonymisation réversible, sur le poste, avant l'IA : c'est la fonction du produit. Banc d'essai : 201 valeurs sensibles codées sur 201.

9 DONNÉES DES CLIENTS ACCESSIBLES AUX SALARIÉS

Aucun accès possible des salariés de l'éditeur : rien ne lui parvient. Le support travaille sur les codes.

10 MESURES DIVERSES SUPPLÉMENTAIRES

Journal de ce que l'IA a reçu, pages de preuve signées, sceau vérifiable par le client, rapport de couverture, politique signée, appli notarisée, aucune télémétrie.

Cases en pointillé : champ sans objet pour Hidden Tokens, expliqué ci-dessous.

Champ par champ, avec la preuve

SUR VOTRE POSTE un contrôle que vous, votre DPO ou votre informaticien faites vous-même, sans nous croire sur parole ;

DANS LE CODE un fichier du code source ou de la documentation technique, consultable lors d'un audit (contrat cadre, article 11) ;

AU CONTRAT un engagement écrit de l'éditeur dans le contrat cadre Organisation.

1 Lieu d'hébergement du LLM

Sans objet. Hidden Tokens n'est pas un modèle de langage et n'en héberge aucun, ni sur le poste ni ailleurs.

Le LLM est celui de l'outil d'IA que le cabinet choisit ; il reste hébergé là où le dit la fiche de cet outil. Hidden Tokens ne déplace pas ce LLM : il change ce qu'il reçoit. Le texte qui lui parvient

porte des codes (`NOM-001` , `SOCIETE-003`) à la place des noms, sociétés et identifiants.

PREUVE

SUR VOTRE POSTE Coupez Internet : le codage et le décodage fonctionnent. Aucun modèle n'est appelé par Hidden Tokens.

DANS LE CODE `test/reseau.test.js` (connecteur) : tout le parcours — tableur, PDF, OCR d'un scan, lot, journal, tableau de bord — tourne avec le réseau interdit par le modèle de permissions de Node ; toute connexion échouerait.

LIMITE Hidden Tokens ne dispense pas de vérifier où est hébergé le LLM de l'outil choisi : il réduit ce que ce LLM voit.

2 Lieu d'hébergement des données

Les données ne quittent pas le poste. Les fichiers en clair, la clé de correspondance, les fichiers décodés et le journal restent sur le disque de l'utilisateur ; le registre commun d'un cabinet vit sur son propre partage de fichiers (NAS, serveur, SharePoint), chiffré.

Hidden Tokens n'a pas de serveur : ni compte, ni stockage en ligne, ni appel de licence. La licence est un jeton signé, vérifié sur le poste.

PREUVE

SUR VOTRE POSTE Avec un pare-feu applicatif (LuLu, Little Snitch), le connecteur ne tente aucune connexion sortante.

SUR VOTRE POSTE La seule connexion sortante de l'appli de bureau est la recherche de mise à jour sur GitHub (en version 0.8.0 : au lancement, puis toutes les six heures). Elle transmet l'adresse IP et la version installée ; aucun fichier, code ni clé.

DANS LE CODE `extension/manifest.json` : la seule autorisation réseau de l'extension est `http://127.0.0.1` , l'appli du même poste. Ses scripts s'exécutent dans les pages de ChatGPT, claude.ai, Gemini et Copilot pour coder le message avant l'envoi (politique de confidentialité de l'extension).

DANS LE CODE `server/licence.js` : licence vérifiée par signature Ed25519, hors ligne.
`server/registre.js` : le registre commun est un dossier du partage du cabinet ; aucun serveur.

AU CONTRAT Article 8 : le logiciel fonctionne sans connexion vers l'éditeur, sans compte, sans télémétrie.
Article 9 : il ne transmet rien à l'éditeur.

LIMITE Un dossier de travail synchronisé dans un cloud (iCloud, Google Drive, Dropbox, OneDrive) emporte les fichiers et la clé hors du poste. Hidden Tokens le détecte et le signale (audit de confinement, outil `verifier_confinement`) ; il ne l'empêche pas.

3 Société hébergeant le LLM (nationalité)

Sans objet pour Hidden Tokens : c'est la société du fournisseur d'IA choisi par le cabinet.

Pour les assistants les plus utilisés — Claude (Anthropic), ChatGPT (OpenAI), Gemini (Google), Copilot (Microsoft) — ce sont des sociétés américaines, celles que visent les deuxième et quatrième critères de souveraineté de la grille. Hidden Tokens ne change pas leur nationalité. Il fait qu'aucune d'elles ne reçoit le nom d'un client, et qu'aucune ne détient la clé qui permettrait de le retrouver.

PREUVE

SUR VOTRE POSTE Le journal « Ce que Claude a vu » (champ 5) montre le texte exact remis à l'IA et le revérifie contre la clé.

DANS LE CODE `server/sortie.js` : sur le texte final de chaque réponse d'outil, toute valeur connue de la clé redevient son code, et toute forme sensible (e-mail, téléphone, IBAN, identifiant long) est masquée.

LIMITE Le statut, au regard du RGPD et des règles de transfert, de données pseudonymisées confiées à un destinataire qui n'a pas la clé reste à apprécier par le cabinet et son conseil (lignes directrices 01/2025 du CEPD ; CJUE, 4 septembre 2025, C-413/23 P).

4 Société hébergeant les données (nationalité)

Aucune société tierce : les données sont chez le cabinet. L'éditeur, Tardigrade SARL (Casablanca, Maroc, RC 620437), n'en reçoit, n'en stocke et n'en traite aucune.

L'éditeur n'a donc ni fichier, ni clé, ni journal à remettre, à qui que ce soit. Pour la même raison, il n'est pas sous-traitant du cabinet au sens de l'article 28 du RGPD pour les données traitées par le logiciel : le cabinet en reste le seul responsable de traitement.

Le logiciel lui-même est distribué par GitHub (Microsoft, États-Unis) et ce site est hébergé par Netlify (États-Unis). Ces canaux transportent le logiciel signé et des pages publiques, jamais les données d'un dossier.

PREUVE

AU CONTRAT Article 9 : l'éditeur ne reçoit, ne stocke et ne traite aucune donnée du client, ni registre, ni clé de correspondance, ni journal ; il n'agit pas comme sous-traitant (RGPD, art. 28 ; loi n° 09-08).

SUR VOTRE POSTE Les contrôles réseau du champ 2.

LIMITE L'éditeur traite les données de la relation commerciale (contacts, facturation), décrites par sa politique de confidentialité.

5 Réutilisation des données des clients par le LLM

Hidden Tokens ne peut pas engager le fournisseur du LLM sur l'usage qu'il fait de ce qu'il reçoit. Il fait que ce qu'il reçoit, et pourrait donc réutiliser, se réduit à des codes — et il le prouve sur le poste.

Le guide du CNB observe qu'une promesse de non-réutilisation n'est en général ni prouvable ni vérifiable. Hidden Tokens ne demande pas de croire une promesse : le journal local montre ce qui est parti.

PREUVE

SUR VOTRE POSTE Demandez à Claude « montre-moi ce que tu as vu » (outil `journal_ia`) : la page locale `CE-QUE-CLAUDE-A-VU.html` liste chaque texte remis à l'IA par Hidden Tokens et le nombre de valeurs réelles qu'on y retrouve. Résultat attendu : 0.

DANS LE CODE `server/journal.js` : chaque réponse est notée après le verrou de sortie, c'est-à-dire exactement ce que le modèle reçoit. À chaque consultation, tout le journal est repassé contre la clé actuelle : une valeur sortie avant que la clé la connaisse est retrouvée après coup. Une fuite y est montrée par son code, jamais par sa valeur.

DANS LE CODE Messages écrits dans ChatGPT, claude.ai, Gemini ou Copilot : le texte codé envoyé est journalisé de la même façon ; du texte en clair, seule la longueur est notée (`SPEC-VERROU-UNIVERSEL.md`).

LIMITE Le LLM reçoit les codes et la structure du dossier — dates, intitulés, raisonnement, montants non sensibles — et peut en faire l'usage que permettent ses conditions.

6 Chiffrement des données

Hidden Tokens remplace plutôt qu'il ne chiffre : ce qui part vers l'IA ne contient pas les valeurs. Ce qu'il partage et ce qu'il garde est protégé ainsi, et la clé est détenue et gérée par le cabinet seul.

PREUVE

DANS LE CODE **Registre commun**, sur le partage du cabinet : chaque entrée chiffrée en AES-256-GCM ; les secrets scellés pour chaque poste certifié (X25519, HKDF-SHA256, AES-256-GCM) ; le registre signé Ed25519 par l'administrateur. Le partage n'a pas à être de confiance (`server/registre.js`, `server/enveloppe.js`).

DANS LE CODE **Clé privée de chaque poste** : trousseau de session sous macOS, DPAPI sous Windows ; jamais de repli silencieux sur un fichier en clair (`sentinelle/lib/trousseau.js`).

AU CONTRAT **Détention de la clé** : par le cabinet. Le séquestre s'ouvre par un quorum de gardiens nommés par le cabinet ; une feuille de secours s'imprime. L'éditeur ne détient aucune clé et ne peut rien restituer (article 8).

DANS LE CODE **Signatures Ed25519** : politique du cabinet, licence, sceau, pages de preuve.

SUR VOTRE POSTE **Transit** : vers l'IA, le chiffrement HTTPS/TLS est celui du fournisseur d'IA. Entre l'extension et l'appli, l'échange passe par `127.0.0.1` et ne quitte pas le poste.

LIMITE La clé de correspondance d'un poste (`cle-de-session.json`) est protégée par les droits du compte (lisible par le seul utilisateur), pas chiffrée par Hidden Tokens dans cette version (`server/index.js`). Activez le chiffrement du disque (FileVault sous macOS, BitLocker sous Windows) : c'est lui qui la protège au repos.

7 RAG sécurisée

Sans objet. Hidden Tokens ne construit ni index, ni base vectorielle, ni moteur de recherche sur les documents, sur le poste ou ailleurs.

Si l'outil d'IA du cabinet indexe des documents, il peut recevoir la copie codée produite par Hidden Tokens : son index ne contiendra alors que des codes, et un document Word qu'il produit à partir d'elle se décode sur le poste (outil `decoder_word`). La sécurité de la RAG elle-même reste celle de l'outil.

PREUVE

DANS LE CODE Les seize outils du connecteur codent, décodent, vérifient ou rendent compte ; aucun n'indexe. Le connecteur n'écrit que la clé, le journal et les copies codées, dans `Hidden-Tokens/` .

8 Pseudonymisation / anonymisation

Pseudonymisation réversible, faite sur le poste, avant l'IA. C'est la fonction de Hidden Tokens.

Les noms, sociétés, adresses, identifiants (pièce d'identité, passeport, SIREN et SIRET, IBAN, n° RG, de parquet, de pourvoi...), références et, dans un tableur, les montants qui disent la finance d'une personne (paie, soldes, honoraires, réglable colonne par colonne) deviennent des codes. La clé est cumulative : la même personne porte le même code dans toutes les pièces du dossier, et avec le registre commun dans tout le cabinet, ce qui permet à l'IA de raisonner sur l'ensemble. La pseudonymisation est voulue : elle seule permet de rendre au client un travail qui porte les vrais noms. Le guide du CNB l'admet expressément, à côté de l'anonymisation.

PREUVE

SUR VOTRE POSTE Le codage se fait en deux temps : le plan s'affiche (ce qui sera codé, ce qui restera lisible), l'utilisateur le valide, puis la copie est écrite. Ouvrez-la : aucun nom de client.

DANS LE CODE Trois verrous empilés. Le verrou (`server/verrou.js`) ne laisse lisible que ce qui est prouvé inoffensif — mots d'un dictionnaire de 336 000 formes, nombres non identifiants, liste blanche (juridictions, codes, intitulés d'actes) — et code tout le reste. Le contrôle d'aperçu repasse chaque cellule montrée à l'IA. Le verrou de sortie (`server/sortie.js`) repasse chaque réponse.

DANS LE CODE Test de réidentification (`server/reidentification.js`) : sur le texte codé, il compte les indices indirects réunis dans un même passage (lieu, âge, fonction rare, date de naissance) ; la date de naissance est codée d'office ; l'option `generaliser` code les villes et ramène un âge à sa tranche.

DANS LE CODE Banc d'essai (connecteur 2.10.0, 21 octobre 2026) : 201 valeurs sensibles codées sur 201, dans 15 documents fictifs (droit, finance, monétique), 0 fuite (`bench/resultats.json` , `npm run bench`). Chasse aux fuites sur tous les outils : `test/fuite.test.js` .

LIMITE Pseudonymiser n'est pas anonymiser : pour le cabinet, qui a la clé, les données restent des données personnelles (RGPD, art. 4(5)). Un mot qui est d'abord une ville, un jour ou un rôle, employé seul comme nom de famille (« Paris »), peut rester lisible ; les indices indirects sont signalés, pas tous réécrits. D'où la relecture du plan.

9 Données des clients accessibles aux salariés

Aucun accès possible des salariés de l'éditeur : aucune donnée de client ne lui parvient.

Le support travaille sur les codes : pour signaler un problème, l'utilisateur cite `NOM-012` , jamais la valeur, et l'éditeur ne demande jamais une donnée du client. Le logiciel ne comporte ni accès à distance, ni console de l'éditeur sur les postes.

Au sein du cabinet, l'ajout et le retrait d'un poste, l'ouverture du séquestre et toute restauration sont journalisés et signés dans le registre ; le rapport de couverture ne donne que des comptes.

PREUVE

AU CONTRAT Article 7 : le client cite les codes, jamais les valeurs ; l'éditeur ne demandera jamais de donnée du client. Article 9 : aucune donnée chez l'éditeur.

SUR VOTRE POSTE Les contrôles réseau du champ 2 : rien ne part vers l'éditeur.

DANS LE CODE `SPEC-REGISTRE-ORGANISATION.md` , invariant 5 : ajout, retrait de poste, ouverture de séquestre et restauration journalisés dans `registre/journal.jsonl` , signés.

LIMITE Dans cette version, tout poste certifié du registre commun peut décoder tous les codes du cabinet : le cloisonnement par équipe ou par dossier n'est pas encore livré.

10 Mesures diverses supplémentaires

SUR VOTRE POSTE **Pages de preuve signées.** Le journal et le rapport de couverture portent un jeton signé (Ed25519) sur leurs comptes et l'empreinte SHA-256 de la page : un chiffre retouché à la main invalide la signature. Vérification hors ligne dans l'appli (« Vérifier une preuve... »).

SUR VOTRE POSTE **Le sceau pour le client** (outil `sceau_dossier`) : une preuve signée que son dossier est passé par Hidden Tokens sans fuite, que le connecteur refuse d'émettre s'il en trouve une. Le client la vérifie lui-même sur hiddentokens.com/fr/verifier-sceau, hors ligne : le sceau voyage dans la partie de l'adresse que le navigateur n'envoie pas au serveur.

DANS LE CODE **Le rapport de couverture** (`rapport_couverture` , `server/couverture.js`) : poste par poste, ce qui a été protégé avant l'IA et les postes qui ne passent plus par Hidden Tokens. Des comptes, jamais une valeur, un code ou un nom de fichier.

SUR VOTRE POSTE **L'audit de confinement** (`verifier_confinement`) nomme les autres portes vers le dossier : autre extension ou serveur MCP qui y a accès, mode Cowork, pilotage du navigateur ou de l'écran, dossier synchronisé dans un cloud.

DANS LE CODE **La politique du cabinet est signée** (Ed25519) et revérifiée à chaque codage : absente, altérée ou rétrogradée, le codage s'arrête (fail closed). Le décodage n'est jamais bloqué (`server/politique.js`).

DANS LE CODE **L'extension retient le message** dès qu'elle a été jumelée : appli absente, texte non remplacé dans la zone de saisie, règle bloquante — rien ne part (`extension/README.md`). Une organisation l'impose dès l'installation par stratégie Chrome.

SUR VOTRE POSTE **Appli signée et notarisée par Apple** (Developer ID, équipe 2CTJY8T842) : `spctl -a -vv "/Applications/Hidden Tokens.app"` répond « source=Notarized Developer ID ». Chaque version publiée porte ses sommes de contrôle SHA-512 ([page des versions](#)).

AU CONTRAT **Aucune télémétrie**, aucune statistique d'usage (article 8). **Le code est ouvert à l'audit** du client ou d'un prestataire indépendant qu'il mandate, avec le vérificateur de preuve et le banc d'essai (article 11).

DANS LE CODE **Les scans sont lus sur le poste** : la reconnaissance de caractères est embarquée (`server/ocr.js`), sans service en ligne.

DANS LE CODE **Documents fournis** : modèle d'analyse d'impact pré-rempli, modèle de charte IA, fiche sécurité, tableau de correspondance RGPD, loi 09-08 et guide du CNB (dossier `confiance/` du connecteur).

LIMITE Hidden Tokens n'a, à ce jour, ni certification, ni label, ni audit de sécurité indépendant publié. L'installateur Windows n'est pas encore signé : Windows affiche « éditeur inconnu » à la première installation. Avant tout premier jumelage, l'extension laisse partir les messages en le signalant par un bandeau rouge.

Vérifier vous-même, en dix minutes

1. Installez l'appli (essai de 14 jours, sans compte) et vérifiez sa signature : `spctl -a -vv "/Applications/Hidden Tokens.app"` .
2. Coupez Internet. Codez un dossier fictif, faites travailler Claude dessus, décodez le Word produit : tout fonctionne.
3. Rétablissez Internet derrière un pare-feu applicatif (LuLu est gratuit) : le connecteur ne tente aucune connexion ; l'appli ne contacte que GitHub, pour les mises à jour.

4. Ouvrez la copie codée dans **Hidden-Tokens/** : aucun nom de client.
5. Demandez à Claude « montre-moi ce que tu as vu » : la page locale affiche 0 valeur réelle.
6. Demandez « vérifie le confinement » : vous obtenez la liste des autres portes ouvertes vers le dossier, et le geste qui ferme chacune.
7. Produisez un sceau et vérifiez-le sur hiddentokens.com/fr/verifier-sceau, onglet réseau des outils de développement ouvert : le sceau n'apparaît dans aucune requête.

Ce que Hidden Tokens ne couvre pas

- Un texte tapé ou collé directement dans une conversation sans l'extension, un fichier joint à la main : ils ne passent par aucun verrou. La charte IA du cabinet fait de Hidden Tokens la seule voie autorisée ; le rapport de couverture permet de vérifier qu'elle est suivie.
- La saisie en ligne ailleurs que sur ChatGPT, claude.ai, Gemini et Copilot, y compris dans l'interface d'un outil d'IA juridique : on y dépose la copie codée, mais ce qu'on y tape n'est pas codé.
- Les indices indirects (fonction, âge, contexte) : ils sont signalés, pas tous réécrits.
- Les tâches où la pseudonymisation ne s'applique pas, comme le compte rendu en direct d'un rendez-vous client, que cite le guide du CNB.
- Les obligations du cabinet : analyse d'impact, choix et contrat du fournisseur d'IA, information du client. Hidden Tokens outille la conformité ; il ne la certifie pas.

Sources

- CNB, Grille de lecture — synthèse des consultations effectuées par le groupe de travail sur l'intelligence artificielle – <https://cnb.avocat.fr/medias/cnb-grille-lecture-intelligence-aartificielle-2025-68f775b81ba5b2.65545272.pdf>, 1^{re} édition, juin 2025, v1.2.
- CNB, commission des règles et usages, *La déontologie et l'intelligence artificielle*, 1^{re} édition, avril 2026.
- RGPD, articles 4(5), 25, 28 et 32 ; CEPD, lignes directrices 01/2025 sur la pseudonymisation ; CJUE, 4 septembre 2025, CEPD c. CRU, C-413/23 P.
- Hidden Tokens, contrat cadre Organisation Hidden Tokens – [/fr/contrat-cadre/](https://hiddentokens.com/fr/contrat-cadre/), articles 7, 8, 9 et 11.
- Hidden Tokens, politique de confidentialité de l'extension – <https://hiddentokens.com/fr/extension/confidentialite/> ; versions publiées et sommes de contrôle – <https://github.com/ai4xedu/hidden-tokens-releases/releases> ; vérifier un sceau – [/fr/verifier-sceau/](https://hiddentokens.com/fr/verifier-sceau/).