

Politique de confidentialité

Mendi — Copilote IA pour la maîtrise d'œuvre du BTP

Version 1.0 — Dernière mise à jour : 3 juillet 2026

1. Introduction

La présente politique de confidentialité décrit la manière dont **MENDI HORIZON** (SASU) (ci-après « **Mendi** », « **nous** ») collecte, utilise, partage et protège les données à caractère personnel dans le cadre de l'utilisation de son service de copilote IA pour la maîtrise d'œuvre du BTP (ci-après le « **Service** »).

Nous nous engageons à traiter les données personnelles conformément au Règlement (UE) 2016/679 (« **RGPD** ») et à la loi n° 78-17 du 6 janvier 1978 modifiée (« **Informatique et Libertés** »).

2. Responsable de traitement

Le responsable du traitement des données est :

- **MENDI HORIZON**, SASU au capital de 500 €
- **Siège social** : 14 avenue Paul Thoureau, 95290 L'Isle-Adam, France
- **SIREN** : 101 661 429 — **RCS** : Pontoise 101 661 429
- **Contact (données personnelles)** : contact@mendi.tech
- **Délégué à la protection des données (DPO)** : [le cas échéant, à désigner] — contact@mendi.tech

Répartition des rôles. Mendi agit en qualité de **responsable de traitement** pour les données liées à la gestion des comptes, à la facturation, à la sécurité et au bon fonctionnement du Service. Pour les données contenues dans le Contenu Utilisateur (contenu des projets, documents, courriels) traitées pour le compte de ses clients professionnels, Mendi agit en qualité de **sous-traitant** au sens de l'article 28 du RGPD, le client professionnel étant responsable de traitement ; un **accord de traitement des données (DPA)** encadre alors ces traitements.

3. Données que nous traitons

Selon l'utilisation du Service, nous sommes amenés à traiter les catégories de données suivantes :

3.1 Données de compte et d'identification

- Adresse e-mail, nom, prénom (si fournis), identifiant de compte.
- Données d'authentification (mot de passe **haché**, jetons de session), y compris via connexion Google ou Microsoft/Outlook.
- Organisation / entité de rattachement (identifiant d'organisation, dit « tenant »).

3.2 Contenu Utilisateur (données de projet)

- Contenu des conversations avec l'assistant, instructions et requêtes.
- Documents et fichiers soumis ou rendus accessibles au Service (par exemple : pièces de marché, CCTP, DPGF, comptes rendus, plans, devis, offres).
- Informations de projet, « mémoire de projet » (faits, décisions, acteurs, jalons).
- Livrables générés à votre demande.

Données de tiers (article 14 du RGPD). Ces contenus peuvent contenir des données personnelles de tiers (par exemple, noms et coordonnées d'intervenants d'un chantier) que ces personnes ne nous ont pas communiquées directement. Ces données proviennent de l'Utilisateur ou du Client qui les soumet. Pour

ces traitements, **Mendi agit en tant que sous-traitant** : l'information des personnes concernées incombe au Client, responsable de traitement, qui garantit disposer d'une base légale pour la transmission de ces données au Service.

3.3 Données de messagerie (fonctionnalité optionnelle)

Si vous connectez une boîte Gmail ou Outlook, nous traitons, dans la limite des autorisations que vous accordez : les jetons d'accès OAuth, ainsi que le contenu des courriels (objet, corps, expéditeur, destinataires, pièces jointes) que vous demandez à lire, rechercher, rédiger ou envoyer. **L'envoi d'un courriel n'a jamais lieu sans votre confirmation explicite.**

3.4 Données de facturation

Pour les abonnements payants, les données nécessaires à la facturation et au paiement, traitées via notre prestataire **Stripe** (Mendi ne stocke pas les numéros de carte bancaire).

3.5 Données techniques et d'usage

- Journaux techniques, adresses IP, identifiants d'appareil, données de connexion.
- Données d'usage du Service (fonctionnalités utilisées, métriques de coût et de performance des traitements IA).
- Données de supervision des erreurs (via **Sentry**) et de traçabilité des traitements IA (via **Langfuse**). Ces données peuvent inclure des extraits de Contenu Utilisateur ; des mesures de **minimisation et de masquage des données personnelles** sont appliquées, et la traçabilité IA (Langfuse) n'est activée que sur une instance maîtrisée par l'Éditeur (voir sections 6 et 9).

3.6 Cookies et traceurs

Voir la section 11. Cookies et traceurs.

Nous ne cherchons pas à collecter de **données sensibles** (article 9 du RGPD). Merci de ne pas soumettre de telles données au Service, sauf strict besoin et base légale appropriée.

4. Finalités et bases légales

Finalité	Base légale (RGPD)
Création et gestion du compte, authentification	Exécution du contrat (art. 6.1.b)
Fourniture des fonctionnalités du Service (analyse de documents, génération de Livrables, mémoire de projet, assistance IA)	Exécution du contrat (art. 6.1.b)
Connexion et traitement des courriels (Gmail/Outlook)	Consentement (art. 6.1.a), révocable à tout moment
Facturation et gestion des paiements	Exécution du contrat (art. 6.1.b) et obligation légale comptable (art. 6.1.c)
Sécurité, prévention de la fraude, supervision des erreurs	Intérêt légitime (art. 6.1.f)
Amélioration et bon fonctionnement du Service	Intérêt légitime (art. 6.1.f) — sur la base de données d'usage et de mesures agrégées , à l'exclusion de toute utilisation du Contenu Utilisateur pour l'entraînement de modèles (voir section 5)
Réponse aux demandes de support et communications de service	Exécution du contrat / intérêt légitime

Finalité	Base légale (RGPD)
Communications commerciales (le cas échéant)	Consentement (art. 6.1.a)
Respect des obligations légales et réponse aux autorités	Obligation légale (art. 6.1.c)

5. Traitement par l'intelligence artificielle

Pour répondre à vos requêtes et produire des Livrables, le Contenu Utilisateur pertinent est transmis à notre fournisseur de modèles d'IA, **Anthropic** (Claude), via une passerelle (proxy) opérée par Mendi.

- Les données transmises sont utilisées **uniquement pour générer la réponse ou le Livrable demandé**.
- Le Contenu Utilisateur **n'est pas utilisé pour entraîner les modèles d'IA** d'Anthropic, conformément aux conditions commerciales applicables à l'usage professionnel de son API.
- Le transfert vers Anthropic (États-Unis) est encadré par des garanties appropriées (voir section 7).

Absence de décision automatisée à effet juridique (article 22 du RGPD). Le Service est un **outil d'assistance sous contrôle humain**. Il ne prend aucune décision produisant des effets juridiques à votre égard, ou vous affectant de manière significative, sur le seul fondement d'un traitement automatisé. Les réponses et Livrables générés par l'IA sont, par nature probabiliste, destinés à être vérifiés et validés par l'Utilisateur avant tout usage.

6. Destinataires et sous-traitants

Nous ne vendons pas vos données. Nous les partageons uniquement avec des sous-traitants agissant sur nos instructions, dans la limite nécessaire à la fourniture du Service, et sous contrat conforme à l'article 28 du RGPD :

Sous-traitant	Rôle	Localisation / entité	Transfert hors UE
Amazon Web Services (AWS)	Hébergement de l'infrastructure, des serveurs et de la base de données applicative (auto-hébergée, PostgreSQL)	Région eu-west-3 (Paris, UE). Entité : AWS EMEA SARL (Luxembourg)	Non (UE)
Supabase	Authentification et stockage de fichiers (documents, Livrables)	Projet en UE ; éditeur Supabase, Inc. (États-Unis)	Possible (voir §7)
Anthropic	Moteur d'intelligence artificielle générative (Claude)	États-Unis — Anthropic PBC	Oui
Stripe	Traitement des paiements et facturation	UE / États-Unis — Stripe Payments Europe Ltd (Irlande)	Possible
Sentry	Supervision des erreurs et stabilité applicative	États-Unis — Functional Software, Inc.	Oui
Langfuse	Observabilité et traçabilité des traitements IA	Instance maîtrisée par l'Éditeur (auto-hébergée ou UE) ; aucun envoi vers le cloud public US par défaut ; désactivée à défaut	Non par défaut

Sous-traitant	Rôle	Localisation / entité	Transfert hors UE
Google	Authentification (SSO) et intégration Gmail (optionnelle)	États-Unis — Google Ireland Ltd / Google LLC	Oui
Microsoft	Authentification (SSO) et intégration Outlook (optionnelle)	UE / États-Unis — Microsoft Ireland Operations Ltd	Possible

Précision sur l'architecture. La base de données relationnelle contenant les projets, conversations, mémoire et métadonnées est **auto-hébergée par Mendi sur l'infrastructure AWS en région UE** ; Supabase intervient pour l'authentification et le stockage de fichiers.

Nous pouvons également communiquer des données lorsque la loi l'exige, à la demande d'une autorité compétente, ou pour faire valoir nos droits. La liste des sous-traitants est susceptible d'évoluer ; nous informerons les utilisateurs de tout changement substantiel.

7. Transferts hors Union européenne

L'hébergement principal des données (infrastructure et base de données applicative sur AWS) est situé dans l'**Union européenne** (région eu-west-3, Paris).

Certains sous-traitants (notamment **Anthropic, Sentry, Google**, et selon la configuration **Supabase, Stripe et Microsoft**) peuvent traiter des données en dehors de l'Union européenne, en particulier aux **États-Unis**. Ces transferts sont encadrés par des **garanties appropriées** au sens du chapitre V du RGPD, notamment :

- les **Clauses Contractuelles Types (CCT)** de la Commission européenne ;
- le cas échéant, l'adhésion du destinataire au **Data Privacy Framework (DPF)** UE–États-Unis ;
- des mesures techniques et organisationnelles complémentaires (chiffrement en transit, minimisation, masquage des données personnelles).

Une copie des garanties applicables peut être demandée à contact@mendi.tech.

8. Durées de conservation

Nous conservons les données uniquement le temps nécessaire aux finalités poursuivies :

Données	Durée de conservation
Données de compte	Pendant la durée de la relation contractuelle, puis suppression ou anonymisation
Contenu Utilisateur (projets, documents, conversations, mémoire, Livrables)	Pendant la durée d'utilisation du Service ; à la clôture du compte, une fenêtre d'export de 30 jours est offerte, puis les données sont supprimées ou anonymisées (sous réserve des délais techniques de purge)
Jetons de messagerie (Gmail/Outlook)	Jusqu'à révocation de la connexion par l'Utilisateur
Données de facturation	Durée légale de conservation comptable (10 ans)
Journaux techniques et de sécurité	Durée proportionnée à la finalité de sécurité (généralement 6 à 12 mois)

Données	Durée de conservation
Données de prospection (le cas échéant)	3 ans à compter du dernier contact

À l'issue de ces durées, les données sont supprimées ou anonymisées.

9. Sécurité

Nous mettons en œuvre des mesures techniques et organisationnelles appropriées pour protéger les données, notamment :

- **Cloisonnement multi-organisations (isolation par tenant)** au niveau de la base de données (politiques de sécurité au niveau des lignes / *Row Level Security*), garantissant qu'une organisation n'accède qu'à ses propres données ;
- **Chiffrement des données en transit** (TLS/HTTPS) ;
- authentification par jetons signés et contrôle d'accès ;
- **minimisation des secrets côté poste utilisateur** : la clé du fournisseur d'IA et les identifiants de base de données ne sont jamais exposés au poste de l'utilisateur, les appels transitant par des passerelles serveur ;
- exécution du code de génération des Livrables dans un **environnement isolé et éphémère** (bac à sable) ;
- **minimisation et masquage des données personnelles** dans les journaux de supervision et de traçabilité IA ;
- journalisation, supervision et sauvegardes.

Notification des violations de données. En cas de violation de données à caractère personnel, nous mettons en œuvre les procédures requises et, lorsque les conditions légales sont réunies, notifions la **CNIL** dans les 72 heures (article 33 du RGPD) et informons les personnes concernées et/ou les clients responsables de traitement dans les meilleurs délais (article 34 du RGPD).

Aucun système n'étant infallible, nous ne pouvons garantir une sécurité absolue, mais nous nous efforçons de maintenir un niveau de protection adapté au risque.

10. Vos droits

Conformément au RGPD, vous disposez des droits suivants sur vos données personnelles :

- **Droit d'accès** : obtenir la confirmation que des données vous concernant sont traitées et en obtenir une copie ;
- **Droit de rectification** : corriger des données inexacts ou incomplètes ;
- **Droit à l'effacement** (« droit à l'oubli ») : demander la suppression de vos données ;
- **Droit à la limitation** du traitement ;
- **Droit à la portabilité** : recevoir les données que vous avez fournies dans un format structuré et lisible par machine, pour les traitements fondés sur le consentement ou l'exécution du contrat ;
- **Droit d'opposition** au traitement fondé sur l'intérêt légitime, et à la prospection ;
- **Droit de retirer votre consentement** à tout moment, pour les traitements qui en dépendent (par exemple la connexion à votre messagerie) ;
- **Droit de définir des directives** relatives au sort de vos données après votre décès.

Le Service intègre par ailleurs des fonctionnalités permettant la suppression de votre compte et l'effacement des données associées.

Comment exercer vos droits : en écrivant à **contact@mendi.tech**. Nous pourrions vous demander de justifier de votre identité. Nous répondons dans un délai d'un (1) mois, prolongeable de deux (2) mois en cas de complexité.

Lorsque Mendi agit en tant que sous-traitant (Contenu Utilisateur), les demandes des personnes concernées sont, le cas échéant, transmises au Client responsable de traitement, que nous assistons dans le respect de ses obligations.

Si vous estimez que vos droits ne sont pas respectés, vous pouvez introduire une réclamation auprès de la **CNIL** (Commission Nationale de l'Informatique et des Libertés — www.cnil.fr, 3 Place de Fontenoy, TSA 80715, 75334 Paris Cedex 07).

11. Cookies et traceurs

Le Service utilise des cookies et technologies similaires strictement nécessaires à son fonctionnement (authentification, session, sécurité), qui ne requièrent pas de consentement.

Le cas échéant, des cookies de mesure d'audience ou de préférence peuvent être déposés ; ceux qui ne sont pas strictement nécessaires ne sont déposés qu'avec votre **consentement**, recueilli via un bandeau ou un panneau de gestion, et révocable à tout moment. [Section à préciser selon les traceurs effectivement déployés.]

12. Protection des mineurs

Le Service est destiné à un usage professionnel et ne s'adresse pas aux mineurs. Nous ne collectons pas sciemment de données concernant des personnes mineures.

13. Modification de la politique

Nous pouvons mettre à jour la présente politique pour tenir compte des évolutions du Service, de nos sous-traitants ou de la réglementation. La version applicable est celle publiée à la date de votre utilisation du Service. En cas de modification substantielle, nous en informons les utilisateurs par un moyen approprié. La date de dernière mise à jour figure en tête du document.

14. Contact

Pour toute question relative à la présente politique ou à l'exercice de vos droits :

contact@mendi.tech

MENDI HORIZON (SASU) — 14 avenue Paul Thoureau, 95290 L'Isle-Adam