Accord de traitement des données

MODÈLE (DPA, ARTICLE 28 DU RGPD) · VERSION 1.3 · 15 NOVEMBRE 2026 · VERSION PDF

Ce document est le modèle d'accord conclu entre MENDI HORIZON, sous-traitant, et chacun de ses clients, responsable de traitement, dès lors que Mendi traite des données personnelles pour son compte. Les mentions « [CHAMP À REMPLIR] » sont complétées à la signature. Pour le recevoir prêt à signer : contact@mendi.tech.

Entre les soussignés

Le Responsable de Traitement :

- Raison sociale : **[CHAMP À REMPLIR — Nom client]**
- Adresse : **[CHAMP À REMPLIR]**
- Représentée par : **[CHAMP À REMPLIR — Nom, fonction]**
- Ci-après dénommée « **le Client** »

Le Sous-traitant :

- Raison sociale : **MENDI HORIZON** (SASU au capital de 500 €)
- SIREN : 101 661 429 — RCS Pontoise 101 661 429
- Siège : 14 avenue Paul Thoureau, 95290 L'Isle-Adam, France
- Représentée par : Thomas Barracho, Président
- Ci-après dénommée « **Mendi** »

Ensemble « les Parties ».

Préambule

Le Client et Mendi ont signé un contrat de service (ci-après « le Contrat principal ») portant sur la fourniture du service Mendi. Dans le cadre de l'exécution du Contrat principal, Mendi sera amenée à traiter des données à caractère personnel pour le compte du Client.

Le présent Data Processing Agreement (ci-après « DPA ») encadre ce traitement conformément à l'Article 28 du Règlement (UE) 2016/679 (ci-après « RGPD »).

1 Objet

Le DPA a pour objet de définir les conditions dans lesquelles Mendi s'engage à traiter les données personnelles du Client dans le cadre du Contrat principal.

2 Description du traitement

2.1 Finalité

Traitement de données dans le cadre de la fourniture d'un copilote IA pour la Maîtrise d'Œuvre d'Exécution BTP, permettant notamment :

- L'assistance à la rédaction de livrables métier (CR, fiches visa, courriers, etc.)
- L'analyse de documents contractuels (CCTP, CCAP, DPGF, etc.)
- La tenue de CR de réunion de chantier
- La mémorisation du contexte projet entre sessions
- Le dashboard opérationnel cross-projets

2.2 Catégories de personnes concernées

- Utilisateurs de Mendi (collaborateurs du Client) : MOE, BET, AMO, conducteurs de travaux, chefs de projet
- Personnes mentionnées dans les documents BTP traités : représentants d'entreprises, architectes, maîtres d'ouvrage, coordonnateurs SPS, administrations

2.3 Catégories de données

- **Données d'identification** : nom, prénom, fonction, entreprise, email professionnel, téléphone professionnel
- **Données de connexion** : identifiant compte, horodatage connexions, IP
- **Données contenues dans les documents BTP uploadés** : données professionnelles diverses (techniques, financières, contractuelles)
- **Conversations avec l'IA** : messages échangés, contexte conversation
- **Données techniques** : logs applicatifs (anonymisés), métriques d'usage

2.4 Données sensibles

Aucune donnée sensible au sens de l'Article 9 RGPD n'est collectée intentionnellement. Si de telles données apparaissent incidemment dans un document BTP uploadé, elles sont traitées comme le reste du document sans extraction spécifique.

2.5 Durée

Durée du Contrat principal + durées de conservation (cf. Article 8).

3 Obligations de Mendi (Sous-traitant)

Conformément à l'Article 28 RGPD, Mendi s'engage à :

1. **Traiter les données uniquement sur instructions documentées** du Client (l'usage du produit via l'interface utilisateur vaut instruction).
2. **Garantir la confidentialité** des personnes autorisées à traiter les données.
3. **Mettre en œuvre les mesures techniques et organisationnelles** détaillées à l'Article 5.
4. **Respecter les conditions** du recours à un autre sous-traitant (cf. Article 6).
5. **Assister le Client** pour répondre aux demandes d'exercice des droits des personnes concernées (cf. Article 7).
6. **Notifier toute violation** de données personnelles (cf. Article 9).
7. **Aider le Client** dans la réalisation des analyses d'impact (DPIA) et les consultations préalables avec la CNIL.
8. **Supprimer ou restituer** les données à la fin du Contrat (cf. Article 10).
9. **Mettre à disposition** toutes les informations nécessaires pour démontrer le respect des obligations.

4 Obligations du Client (Responsable de Traitement)

Le Client s'engage à :

1. Fournir à Mendi **les données nécessaires** à la prestation.
2. **Documenter les instructions** particulières relatives au traitement.
3. **Veiller au respect** des obligations RGPD par ses propres utilisateurs.
4. **Superviser le traitement** y compris en réalisant les audits prévus à l'Article 11.
5. **Informer les personnes concernées** des traitements effectués via Mendi (mention d'information dans les politiques de confidentialité du Client).

5 Mesures techniques et organisationnelles

5.1 Mesures techniques (référentiel détaillé)

Mendi met en œuvre les mesures techniques décrites dans son dossier de sécurité, communiqué au Client sur demande :

- **Cloisonnement par cabinet** : chaque requête est filtrée sur le cabinet de l'utilisateur ; des essais automatisés vérifient ce cloisonnement
- **Chiffrement en transit** : TLS 1.3, HSTS avec pré-loading
- **Chiffrement au repos** : AES-256 (BDD selon hébergeur), safeStorage natif OS (secrets locaux)
- **Authentification** : jetons signés (ES256) vérifiés par le serveur ; second facteur exigé pour la console de l'opérateur
- **Prompt injection defense** : défense 3 couches sur toutes les surfaces user-controlled
- **Path traversal guard** : blocklist dotfiles sensibles
- **Audit log immuable** : append-only hash-chained vérifiable
- **Protection web** : CSP nonce per-request, CSRF guard, rate limiting
- **Sandbox code** : Docker `--network=none --cap-drop=ALL --read-only` pour exécution générée

5.2 Mesures organisationnelles

Décrites dans le dossier de sécurité :

- Accès production restreint (liste nominative, MFA)
- Rotation secrets (30-90 jours selon type)
- Revue de code à deux yeux dès équipe > 1
- Onboarding/offboarding employés tracé
- Formation sécurité annuelle
- Gestion incidents documentée

5.3 Tests de sécurité

- **Essais automatisés** exécutés à chaque modification du logiciel
- **Test d'intrusion externe** : non réalisé à la date du présent document ; ses conclusions seront communiquées au Client lorsqu'il aura eu lieu
- **Audit log monitoring** continu
- **Dependabot + npm audit** + Gitleaks en CI

6 Sous-traitants ultérieurs

6.1 Autorisation générale

Le Client autorise Mendi à recourir aux sous-traitants ultérieurs suivants :

SOUS-TRAITANT	LOCALISATION	SERVICE	GARANTIES
Amazon Web Services EMEA SARL	Luxembourg ; données hébergées en région UE (eu-west-3, Paris)	Hébergement : serveur, base de données, stockage des fichiers, sauvegardes, exécution de code à la demande	Hébergement dans l'UE ; SCC UE 2021/914 incluses dans les conditions de service d'AWS
Anthropic, PBC	USA (Californie)	Fourniture modèle Claude (LLM)	SCC UE 2021/914 + SOC 2 Type II
Mistral AI SAS	France (Paris) ; infrastructure UE	Transcription de la voix — dictée du planning, facultative (modèle Voxtral)	Société de droit français, traitement dans l'UE ; aucun entraînement sur les données de l'API ; conservation 30 jours au plus (surveillance des abus)
Supabase Pte. Ltd.	Singapour ; projet configuré en région UE	Authentification ; conservation des fichiers déposés avant octobre 2026	SCC UE 2021/914 (accord de traitement des données de Supabase) ; données stockées dans la région choisie
Stripe Payments Europe Ltd	Irlande ; UE / USA	Paiements et facturation des abonnements	SCC UE 2021/914 ; Data Privacy Framework le cas échéant
Youtrust SAS (service Yousign)	France (Caen) ; hébergement UE	Signature électronique : document à signer, nom, prénom et adresse e-mail des signataires	Société de droit français, hébergement dans l'UE
Plus Five Five, Inc. (service Resend)	USA	Envoi des courriels du Service : adresses des destinataires, objet et contenu	SCC UE 2021/914 ; Data Privacy Framework
Google Ireland Ltd / Google LLC (optionnel)	UE / USA	Authentification (SSO) et connexion à la boîte Gmail de l'utilisateur	SCC UE 2021/914 ; Data Privacy Framework le cas échéant
Microsoft Ireland Operations Ltd (optionnel)	UE / USA	Authentification (SSO) et connexion à la boîte Outlook de l'utilisateur	SCC UE 2021/914 ; Data Privacy Framework le cas échéant

SOUS-TRAITANT	LOCALISATION	SERVICE	GARANTIES
650 Industries, Inc. (service Expo)	USA	Notifications de l'application mobile : jeton de l'appareil, titre et texte de la notification	SCC UE 2021/914 (à confirmer avant signature)
Sentry (optionnel)	USA	Tracking erreurs	SCC UE 2021/914 (activable / désactivable par tenant)
Langfuse (optionnel)	USA ou self-hosted UE	Tracing LLM	SCC si cloud US

Voyage AI (embeddings), cité dans la version 1.1, n'est pas activé : son activation suivrait la procédure de l'article 6.3.

Le détail des transferts et des garanties figure dans le dossier de sécurité, communiqué au Client sur demande.

6.2 Engagement contractuel

Mendi s'engage à imposer aux sous-traitants ultérieurs des obligations de protection des données équivalentes à celles du présent DPA.

6.3 Modification de la liste

Tout nouveau sous-traitant ou changement de sous-traitant fait l'objet d'une notification au Client au moins **30 jours avant** sa mise en œuvre effective. Le Client dispose d'un droit d'opposition motivé pour des raisons tenant à la protection des données.

7 Droits des personnes concernées

Mendi assiste le Client dans la réponse aux demandes suivantes via les endpoints API documentés :

DROIT	ENDPOINT API MENDI	DÉLAI
Accès / portabilité (Art. 15 + 20)	`GET /api/moex/user-data/export`	Réponse immédiate
Effacement (Art. 17)	`DELETE /api/moex/user-data/delete`	Cascade sous 24 h
Rectification (Art. 16)	`PATCH /api/moex/user-data/rectify`	Immédiat
Limitation (Art. 18)	Via désactivation compte	Sur demande

Le Client reste responsable de traiter les demandes sous **30 jours** (Art. 12 RGPD).

Mendi transmet au Client toute demande reçue directement des personnes concernées sous **5 jours ouvrés**.

8 Durée de conservation

8.1 Principe

Les données sont conservées **pendant la durée du Contrat principal** et **jusqu'à suppression explicite par le Client** ou l'utilisateur final.

8.2 Justification durée longue

Les projets BTP se déroulent sur plusieurs années (phases conception → exécution → réception → garanties décennales — Art. 1792 Code civil). Une purge automatique serait préjudiciable au Client.

8.3 Suppression à la fin du Contrat

Cf. Article 10 — Modalités de fin de contrat.

9 Notification de violation

9.1 Engagement de Mendi

Mendi notifie au Client **sans délai et au plus tard dans les 48 heures** suivant la découverte de toute violation de données susceptible d'affecter les droits et libertés des personnes concernées.

9.2 Contenu de la notification

- Nature de la violation
- Catégories et nombre approximatif de personnes concernées
- Catégories et nombre approximatif d'enregistrements concernés
- Conséquences probables
- Mesures prises ou proposées pour remédier à la violation

9.3 Support à la notification CNIL

Mendi assiste le Client dans la notification à la CNIL (Art. 33) dans les 72 heures suivant la découverte, et le cas échéant dans l'information aux personnes concernées (Art. 34).

10 Modalités de fin de contrat

10.1 À la fin du Contrat principal

Au choix du Client, notifié par écrit à Mendi dans les 30 jours suivant la fin du contrat :

Option A — Restitution : Mendi remet au Client un export JSON complet de toutes les données (format documenté, réutilisable), dans les 30 jours suivant la demande.

Option B — Destruction : Mendi supprime définitivement toutes les données du Client (base de données + stockage fichiers + backups) dans les 30 jours, et fournit une **attestation de destruction**.

Par défaut si pas d'instruction : destruction à l'expiration du délai de trente (30) jours suivant la fin du contrat, comme le prévoient les conditions générales de vente.

10.2 Exceptions

Mendi peut conserver certaines données au-delà en cas d'obligation légale (audit log immuable, logs de sécurité selon Art. 32). La liste exhaustive est transmise au Client.

11 Audits et contrôles

11.1 Droit d'audit

Le Client peut effectuer un audit de conformité du traitement, soit :

- Sur pièces : revue de la documentation (DPA, DPIA, registre, SBOM, rapports de tests de sécurité disponibles, etc.)
- Sur place : visite des locaux ou systèmes (préavis 30 jours, pendant les heures ouvrables, à la charge du Client)

Fréquence maximale : **1 audit par an** (sauf incident majeur).

11.2 Documents mis à disposition

Mendi met à disposition du Client sur simple demande :

- Ce DPA signé
- DPIA à jour
- Registre des traitements
- Rapports de tests de sécurité disponibles
- SBOM à jour

- Attestations sous-traitants

11.3 Confidentialité

Les informations obtenues lors d'un audit sont couvertes par les obligations de confidentialité du Contrat principal.

12 Responsabilité et indemnisation

La responsabilité de chaque Partie est régie par les dispositions du Contrat principal et par les Articles 82 et suivants du RGPD.

En cas de sanction administrative (CNIL) ou de dommages causés à une personne concernée, la répartition entre les Parties se fait au prorata de leur part de responsabilité conformément à l'Article 82 RGPD.

13 Durée et résiliation

Le présent DPA prend effet à la signature et court pendant toute la durée du Contrat principal + les durées de conservation post-contrat.

La résiliation du Contrat principal entraîne la fin du DPA, sous réserve de l'exécution des obligations de fin de contrat (Article 10).

14 Modification

Toute modification du présent DPA fait l'objet d'un avenant signé par les deux Parties.

Mendi notifie au Client toute évolution substantielle de ses mesures de sécurité ou de sa liste de sous-traitants avec un préavis minimum de 30 jours.

15 Droit applicable et juridiction

Le présent DPA est soumis au **droit français**.

Tout litige relevant de l'interprétation ou de l'exécution du DPA sera soumis à la juridiction compétente du lieu du siège social du Client (sauf disposition contraire du Contrat principal).

16 Contacts

16.1 Pour MENDI HORIZON (SASU)

- **Protection des données et sécurité** : Thomas Barracho, Président — contact@mendi.tech
- Mendi n'a pas désigné de délégué à la protection des données.

16.2 Pour le Client

- **DPO** : **[CHAMP À REMPLIR — Nom, contact]**
- **Référent sécurité** : **[CHAMP À REMPLIR]**
- **Contact contractuel** : **[CHAMP À REMPLIR]**

Signatures

Fait à [CHAMP À REMPLIR], **le [CHAMP À REMPLIR]**, en deux exemplaires originaux.

Pour le Client

Nom : **[CHAMP À REMPLIR]** Fonction : **[CHAMP À REMPLIR]** Date : Signature :

Pour MENDI HORIZON

Nom : Thomas Barracho Fonction : Président Date : Signature :

Annexes

Communiquées au Client sur demande, à la signature :

- **Annexe 1** — Mesures techniques détaillées
- **Annexe 2** — Mesures organisationnelles
- **Annexe 3** — Transferts hors Union européenne et garanties
- **Annexe 4** — Analyse d'impact (DPIA, méthode CNIL)
- **Annexe 5** — Registre des traitements (article 30)
- **Annexe 6** — Liste des composants logiciels (SBOM)

Les annexes font partie intégrante du présent DPA.

© 2026 MENDI HORIZON SASU · SIREN 101 661 429

contact@mendi.tech