Accord de sous-traitance (DPA)

Annexe aux Conditions Générales de Vente Navi — Article 28 RGPD

SOUS-TRAITANT

Alexis Raitano

Entrepreneur individuel

SIREN 897 833 729

196 rue Germaine Tillion, 92000 Nanterre

alexis.raitano@myffu.fr

RESPONSABLE DE TRAITEMENT (CLIENT)

Raison sociale :

SIREN / N° d'identification :

Adresse :

Email du contact :

La présente annexe constitue l'**accord de sous-traitance** au sens de l'article 28 du Règlement Général sur la Protection des Données (RGPD). Elle fait partie intégrante des Conditions Générales de Vente Navi accessibles sur https://navi.myffu.fr/legal/cgv. **L'acceptation des CGV par le Client emporte acceptation des présentes dispositions.**

A.1 Objet

La présente annexe définit les conditions dans lesquelles Navi (**Sous-traitant**) traite des données à caractère personnel pour le compte du Client (**Responsable de traitement**) dans le cadre de la fourniture du Service.

A.2 Description du traitement

Item	Précision
Nature et finalité	Fourniture du Service Navi : assistance conversationnelle aux visiteurs de la boutique du Client, incluant le conseil produit, le suivi de commande, le service après-vente, la préparation de paniers et la gestion des retours.
Durée du traitement	Pendant toute la durée du contrat, augmentée d'une période de réversibilité de 30 jours après résiliation, puis suppression des systèmes actifs. Les sauvegardes techniques sont purgées au plus tard 90 jours après la résiliation.
Catégories de personnes concernées	Visiteurs de la boutique du Client interagissant avec l'assistant ; représentants et utilisateurs du Client accédant au tableau de bord.
Catégories de données traitées	Contenu des conversations échangées avec l'assistant ; adresses email des visiteurs (lorsque saisies pour l'authentification OTP) ; identifiants de session technique ; identifiants Shopify (numéro de commande, customer_id) ; données de commandes consultées en lecture ; données de paniers créés via l'assistant ; demandes de retour soumises via l'assistant ; identifiants de connexion du Client (email, mot de passe haché).

Données sensibles	Aucune donnée sensible au sens de l'article 9 RGPD n'est traitée.

A.3 Obligations du Sous-traitant

Navi s'engage à :

- ne traiter les données que sur instruction documentée du Client (lesdites instructions étant constituées par les CGV, les paramètres de configuration choisis par le Client dans son tableau de bord, et toute instruction complémentaire écrite) ;
- garantir que les personnes autorisées à traiter les données sont soumises à une obligation de confidentialité ;
- prendre toutes les mesures techniques et organisationnelles appropriées pour assurer la sécurité du traitement (cf. A.5) ;
- respecter les conditions de recours à des sous-traitants ultérieurs (cf. A.4) ;
- aider le Client à répondre aux demandes des personnes concernées (droit d'accès, rectification, effacement, etc.) ;
- aider le Client à respecter ses propres obligations (notifications de violation, analyses d'impact si requises) ;
- notifier le Client sans retard injustifié, et au plus tard 72 heures après en avoir pris connaissance, en cas de violation de données à caractère personnel ;
- mettre à disposition du Client toute information nécessaire pour démontrer le respect des obligations RGPD ;
- supprimer ou restituer les données à la fin du contrat selon les modalités prévues à l'article 8 des CGV (Réversibilité).

A.4 Sous-traitants ultérieurs

Navi est autorisé à recourir aux sous-traitants ultérieurs suivants pour la fourniture du Service :

Sous-traitant	Rôle	Localisation	Cadre juridique
Vercel Inc.	Hébergement du site marketing (navi.myffu.fr)	États-Unis	Clauses contractuelles types (CCT) de la Commission européenne
Railway Corp.	Hébergement de l'infrastructure Navi (widget, automatisations, base vectorielle)	États-Unis	Clauses contractuelles types (CCT) de la Commission européenne
Supabase Inc.	Base de données, authentification et stockage applicatif	Union européenne (région UE)	Hébergement intra-UE
Anthropic PBC	Fourniture du modèle de langage Claude (génération des réponses)	États-Unis	Clauses contractuelles types (CCT) de la Commission européenne
Resend, Inc.		États-Unis	Clauses contractuelles types (CCT) de

	Envoi des emails transactionnels (notifications, OTP)		la Commission européenne
Shopify International Limited	Lecture du catalogue, des commandes et des données boutique du client (intégration Shopify)	Irlande (Union européenne)	Hébergement intra-UE
Stripe Payments Europe Limited	Traitement des paiements (abonnements et facturation)	Irlande (Union européenne)	Hébergement intra-UE

Toute évolution de cette liste (ajout, modification de localisation) fera l'objet d'une notification écrite préalable au Client, avec un préavis raisonnable (a minima 30 jours), permettant au Client de s'y opposer pour motif raisonnable et, le cas échéant, de résilier le contrat sans frais si l'opposition est justifiée et qu'aucune solution alternative ne peut être trouvée.

A.5 Mesures techniques et organisationnelles de sécurité

- chiffrement des données en transit (TLS 1.2+) ;
- chiffrement des données au repos pour les bases de données et sauvegardes ;
- hachage des mots de passe administrateurs via bcrypt (rounds 10) ;
- cloisonnement strict des données par locataire (isolation multi-tenant via shop_domain, politique Row-Level Security au niveau de la base de données) ;
- contrôle d'accès basé sur les rôles (RBAC) avec principe du moindre privilège ;
- journalisation des accès et des opérations sensibles, conservation 12 mois ;
- authentification forte recommandée pour les comptes administrateurs ;
- sauvegardes automatisées et procédures de restauration testées ;
- séparation stricte des environnements (production / pré-production / développement) ;
- gestion continue des vulnérabilités et veille sécurité ;
- aucune donnée client n'est utilisée pour l'entraînement de modèles d'intelligence artificielle.

A.6 Droits du Client (audit)

Le Client dispose d'un droit d'information et de contrôle sur le traitement effectué par Navi. Il peut :

- demander tout justificatif relatif aux mesures de sécurité mises en œuvre (questionnaire, attestations, rapports d'audit type SOC 2 ou ISO 27001 lorsque disponibles) ;
- demander la communication de tout document permettant de démontrer le respect des obligations du Sous-traitant.

Compte tenu de la nature SaaS du Service, les audits sur site (physiques) ne sont pas effectués par défaut. Ils peuvent être conduits par un tiers indépendant, à la charge du Client, sur préavis raisonnable (a minima 30 jours), aux frais du Client, et dans des conditions n'affectant pas la sécurité ou la disponibilité du Service.

A.7 Transferts hors Union européenne

Les transferts de données à caractère personnel vers des sous-traitants ultérieurs situés hors de l'Union européenne sont encadrés par les **clauses contractuelles types (CCT)** adoptées par la Commission européenne, ainsi que, le cas échéant, par le mécanisme *Data Privacy Framework* pour les sous-traitants certifiés.

A.8 Fin du traitement

À la résiliation du contrat, conformément à l'article 8 des CGV (Réversibilité) :

- le Client dispose de 30 jours pour demander l'export de ses données (format JSON ou CSV) ;
- à l'expiration de ce délai, ou immédiatement sur demande écrite du Client, Navi supprime les données des systèmes actifs dans un délai maximum de 30 jours ;
- les sauvegardes techniques sont purgées selon le calendrier de rotation des sauvegardes (au plus tard 90 jours après la résiliation).

A.9 Hiérarchie des normes

En cas de contradiction entre les présentes dispositions (Annexe DPA) et le corps des CGV, **les présentes dispositions prévalent pour les questions de protection des données à caractère personnel**. Pour toute autre question, les CGV prévalent.

Signature des parties

POUR LE SOUS-TRAITANT

Alexis Raitano

Entrepreneur individuel, responsable de publication

Date :

Signature :

POUR LE RESPONSABLE DE TRAITEMENT (CLIENT)

Nom et qualité :

Date :

Signature :