

Registre des activités de traitement

Version 1.1, mise à jour du 2026-10-23

Responsable de traitement

ALBS Agency, éditeur du logiciel Olnis, représentée par Alexandre Elleborgne.

SIRET À compléter

Contact : contact@albs-agency.com

Délégué à la protection des données : contact@albs-agency.com

T01 · Gestion des comptes praticiens

Finalité : Permettre à un ostéopathe libéral de créer et gérer son compte pour utiliser l'application (authentification, préférences, abonnement).

Base légale : Exécution du contrat (RGPD art. 6.1.b)

Personnes concernées : Ostéopathes libéraux abonnés

Catégories de données : - Identité : nom, prénom, email professionnel

- Coordonnées : téléphone, adresse du cabinet

- Identifiants professionnels : n° RPPS, SIRET, forme juridique

- Authentification : mot de passe hashé bcrypt, secret TOTP, codes de récupération hashés

- Historique de connexion (dernier login)

Destinataires : - Praticien lui-même

- Support Olnis (accès restreint aux métadonnées, jamais aux données patients)

Transferts hors UE : Aucun

Durée de conservation : Compte actif : durée de l'abonnement. Suppression : 30 jours après demande, ou 3 ans après dernière connexion pour un compte inactif.

Mesures de sécurité : Mot de passe hashé bcrypt, 2FA TOTP obligatoire, HTTPS, en-têtes de sécurité stricts (HSTS, CSP), rate-limit connexion.

T02 · Gestion des dossiers patients

Finalité : Permettre au praticien de tenir les dossiers de ses patients pour assurer la continuité des soins

ostéopathiques (identité, motif, examen, traitement, suivi).

Base légale : - Obligation légale (RGPD art. 6.1.c) : tenue de dossier prévue par le décret n° 2007-437 relatif à la profession d'ostéopathe

- Article 9.2.h RGPD : nécessaire à la médecine préventive et aux soins

Personnes concernées : Patients du praticien

Catégories de données : - Identité : nom, prénom, date de naissance, sexe

- Coordonnées : téléphone, email, adresse postale

- Données de santé (art. 9 RGPD) : antécédents, allergies, traitements en cours, motif, examen clinique, diagnostic ostéopathique, techniques appliquées, conseils

- Documents : ordonnances, comptes-rendus, examens transmis par le patient

- Historique des rendez-vous

- Champs chiffrés AES-256-GCM (source : code) : birth_date, gender, phone, email, typology, address, postal_code, city, profession, height_cm, weight_kg, allergies, medications, medical_history, surgeries, family_history, lifestyle, general_notes, referring_doctor, emergency_contact, reason, anamnesis, examination, diagnosis, treatment, advice, follow_up, custom_content, description

Destinataires : - Le praticien qui a créé le dossier

- Aucun autre destinataire (les comptables n'accèdent JAMAIS aux données de santé, cf. T05)

Transferts hors UE : Aucun

Durée de conservation : Article R1112-7 CSP transposé : 20 ans à compter du dernier passage. Puis anonymisation. Suppression avant terme sur demande du patient (droit à l'effacement - sauf conservation nécessaire à l'obligation légale).

Mesures de sécurité : Chiffrement AES-256-GCM des champs médicaux, clé dérivée par praticien (HKDF-SHA256), les administrateurs plateforme NE PEUVENT PAS déchiffrer.

T03 · Journal des accès aux dossiers patients

Finalité : Traçabilité obligatoire imposée par le référentiel CNIL "sécurité des données de santé" : chaque consultation d'un dossier patient est enregistrée.

Base légale : Obligation légale (RGPD art. 6.1.c) - référentiel CNIL sécurité santé

Personnes concernées : Praticiens et patients concernés

Catégories de données : - ID utilisateur (praticien)

- ID patient (référence, pas d'identité en clair)

- Type d'action : view, edit, export, delete, note_view, doc_download

- Contexte : ID de la note ou du document

- Horodatage, adresse IP, user-agent

Destinataires : - Praticien : accès à SON journal via /mon-journal.php

- Patient : accès à son journal via demande RGPD

- CNIL : sur réquisition

Transferts hors UE : Aucun

Durée de conservation : 6 ans, conformément aux obligations santé.

Mesures de sécurité : Immuabilité : pas de UPDATE ni DELETE possibles (append-only), pas de FK vers patients pour survivre à la suppression d'un dossier.

T04 · Journal des événements de sécurité

Finalité : Détecter et documenter les incidents de sécurité (échecs de connexion, verrouillages, tentatives CSRF, etc.).

Base légale : Intérêt légitime du responsable de traitement (RGPD art. 6.1.f) et obligation légale de sécurité (art. 32 RGPD).

Personnes concernées : Toute personne utilisant l'application

Catégories de données : - ID utilisateur si connu, sinon null

- Type d'événement : login_ok, login_fail, login_2fa_ok, login_2fa_fail, password_changed, account_locked, csrf_fail

- Sévérité : info, warning, critical

- Adresse IP, user-agent

- Détails techniques

Destinataires : - Équipe support et sécurité Olnis

Transferts hors UE : Aucun

Durée de conservation : 12 mois glissants (recommandation CNIL, délibération 2005-208).

Mesures de sécurité : Base MySQL protégée, pas d'accès direct.

T05 · Partenariat avec un cabinet comptable (optionnel)

Finalité : Permettre au praticien qui le souhaite d'autoriser un cabinet comptable partenaire à consulter uniquement ses données financières (recettes, dépenses, immobilisations) pour la tenue de sa comptabilité BNC.

Base légale : Consentement explicite du praticien (RGPD art. 6.1.a).

Personnes concernées : Praticiens ayant consenti ; comptables partenaires.

Catégories de données : - Comptables ne voient QUE : recettes encaissées, dépenses, immobilisations, note de frais du praticien.

- Comptables ne voient JAMAIS : identité des patients, données de santé, notes cliniques.

Destinataires : - Cabinet comptable désigné par le praticien

Transferts hors UE : Aucun

Durée de conservation : Jusqu'à révocation par le praticien (fonctionnalité disponible dans Paramètres).

Mesures de sécurité : Contrôle d'accès par rôle (RBAC), journal `accountant_access_log` de chaque consultation.

T06 · Facturation et abonnement

Finalité : Facturer l'abonnement Olnis Pro au praticien via Stripe.

Base légale : Exécution du contrat (RGPD art. 6.1.b) et obligation légale comptable (art. 6.1.c).

Personnes concernées : Praticiens abonnés

Catégories de données : - Email, nom, prénom, adresse du cabinet
- Historique des paiements (montant, date, statut)
- ID client et abonnement Stripe (aucun numéro de carte stocké chez Olnis)

Destinataires : - Stripe Payments Europe Ltd (Irlande) - sous-traitant PCI-DSS.
- Expert-comptable d'ALBS Agency pour la comptabilité de l'éditeur.

Transferts hors UE : Stripe : traité en UE.

Durée de conservation : Factures : 10 ans (obligation comptable).

Mesures de sécurité : Numéros de carte JAMAIS transitent par Olnis. Session Stripe Checkout hébergée par Stripe.

T07 · Emails transactionnels

Finalité : Envoyer les emails nécessaires au service : vérification d'email, réinitialisation de mot de passe, alertes de sécurité, note d'honoraires envoyée aux patients depuis le compte praticien.

Base légale : Exécution du contrat (RGPD art. 6.1.b). Ces envois ne sont pas de la prospection et ne peuvent pas faire l'objet d'une opposition, voir le traitement T10.

Personnes concernées : Praticiens, et patients recevant leur note d'honoraires par email (avec le praticien en From ou Reply-To).

Catégories de données : - Email destinataire
- Contenu (PDF facture, code de vérification, lien de reset)

Destinataires : - Serveur SMTP : `mail.albs-agency.com`

Transferts hors UE : Aucun

Durée de conservation : Logs de délivrance : 3 mois.

Mesures de sécurité : SMTP chiffré TLS, DKIM/SPF configurés.

T08 · Demandes RGPD

Finalité : Traiter les demandes d'exercice de droits RGPD des praticiens (accès, portabilité, effacement).

Base légale : Obligation légale (RGPD art. 12 à 22).

Personnes concernées : Praticiens abonnés

Catégories de données : - ID utilisateur

- Type de demande
- Statut
- Fichier export généré (48h max)

Destinataires : - Le praticien demandeur

Transferts hors UE : Aucun

Durée de conservation : Traces de la demande : 3 ans. Fichier export : supprimé 48h après téléchargement.

Mesures de sécurité : Export chiffré, lien à usage unique et signé.

T09 · Preuve d'acceptation du DPA (contrat de sous-traitance)

Finalité : Conserver la preuve que le praticien a accepté l'accord de sous-traitance (art. 28 RGPD) au moment de son abonnement.

Base légale : Obligation légale (RGPD art. 28) et intérêt légitime (preuve contractuelle).

Personnes concernées : Praticiens abonnés

Catégories de données : - ID utilisateur

- Date et heure d'acceptation
- Version du DPA acceptée (courante)
- Adresse IP au moment de l'acceptation

Destinataires : - Éditeur (preuve interne), CNIL sur réquisition

Transferts hors UE : Aucun

Durée de conservation : Durée du contrat + 5 ans (prescription civile).

Mesures de sécurité : Colonnes dédiées sur la table users, base protégée.

T10 · Prospection et communications commerciales

Finalité : Faire connaître le service à des ostéopathes sur leur adresse professionnelle, et informer les

utilisateurs des évolutions et offres portant sur un service analogue au leur.

Base légale : Intérêt légitime (RGPD art. 6.1.f), prospection entre professionnels sur adresse professionnelle et pour un contenu en rapport avec l'activité du destinataire. Opposition possible à tout moment, sans justification.

Personnes concernées : Praticiens utilisateurs du service, et ostéopathes non clients dont les coordonnées professionnelles ont été collectées.

Catégories de données : - Email professionnel

- Nom, prénom
- Nom du cabinet
- Ville
- Statistiques d'ouverture et de clic
- Source de la collecte

Destinataires : - Serveur SMTP : mail.albs-agency.com

Transferts hors UE : Aucun

Durée de conservation : Jusqu'à opposition. En cas d'opposition, seule l'adresse est conservée en liste de suppression, afin de garantir qu'elle ne soit plus sollicitée.

Mesures de sécurité : Origine des données mentionnée dans chaque message (RGPD art. 14). Lien de désinscription en un clic et en-têtes List-Unsubscribe (RFC 8058). Liste de suppression permanente contrôlée avant chaque envoi. Aucune donnée de patient n'est utilisée.

T11 · Mesure d'usage du service

Finalité : Comprendre comment les praticiens découvrent et utilisent l'application, pour l'améliorer et en piloter l'activité : jours d'utilisation, étapes de configuration franchises, échéances d'abonnement payées.

Base légale : Intérêt légitime du responsable de traitement (RGPD art. 6.1.f).

Personnes concernées : Ostéopathes libéraux inscrits

Catégories de données : - Jours d'utilisation : date, heures de première et de dernière activité, nombre de minutes actives

- Échéances d'abonnement payées : montant, période couverte, identifiants Stripe
- Aucune donnée patient, aucun contenu consulté

Destinataires : - Administrateurs Olnis, sous forme de statistiques agrégées

Transferts hors UE : Aucun

Durée de conservation : Jours d'utilisation : 13 mois glissants. Échéances payées : durée de la relation contractuelle, puis 3 ans.

Mesures de sécurité : Base MySQL protégée, lecture réservée aux administrateurs.

T12 · Répertoire d'annonces de remplacement publiées sur d'autres sites

Finalité : Signaler aux ostéopathes candidats les annonces de remplacement, de collaboration et de cession publiées publiquement sur d'autres sites d'annonces, en renvoyant vers le site d'origine ; leur permettre de les garder en favori ou de les masquer.

Base légale : Intérêt légitime du responsable de traitement (RGPD art. 6.1.f) : faciliter la recherche de remplacements, à partir d'annonces rendues publiques par leurs auteurs.

Personnes concernées : Auteurs d'annonces publiées sur les sites parcourus ; utilisateurs d'Olnis ayant un profil candidat

Catégories de données : - Annonces : titre, adresse de la page d'origine, type de mission, code postal ou département, dates, extrait de 260 caractères au plus

- Aucun téléphone ni adresse électronique : ils sont retirés de l'extrait avant enregistrement

- Utilisateurs : annonces mises en favori ou masquées

Destinataires : - Utilisateurs d'Olnis ayant un profil candidat

- Administrateurs Olnis

Transferts hors UE : Aucun

Durée de conservation : Une annonce qui n'apparaît plus sur son site d'origine cesse d'être affichée après 21 jours et est supprimée après 90 jours, avec les favoris et masquages qui s'y rapportent.

Mesures de sécurité : Base MySQL protégée. Collecte limitée aux sites activés par l'équipe, dans le respect de leur robots.txt.

Sous-traitants (article 28)

Scalingo (France (UE)) : Hébergement de l'application et de la base de données (PaaS). Certifié HDS (Hébergeur de Données de Santé) et ISO 27001. Données hébergées en France. Contrat de sous-traitance / convention HDS.

Stripe Payments Europe Ltd (Irlande (UE)) : Paiement des abonnements (Checkout + Billing Portal). Certifié PCI-DSS niveau 1. Aucun numéro de carte ne transite par Olnis.

mail.albs-agency.com (UE) : Acheminement des e-mails transactionnels (SMTP). Transport chiffré TLS, SPF/DKIM configurés.