Contrat de sous-traitance RGPD (DPA Cabinet) — MyJanalya

Contrat de sous-traitance RGPD (DPA) — MyJanalya

> Annexe indissociable des CGV B2B Janalya IT (art. 28 RGPD)
> Document confidentiel — non publié sur le site, communiqué au Cabinet à la souscription Version 1.0 — [DATE_PUBLICATION]

Préambule

Le présent Contrat de sous-traitance (« **DPA** ») a pour objet de définir les conditions dans lesquelles JANALYA IT (« **le Sous-traitant** ») traite, pour le compte du Cabinet (« **le Responsable de traitement** »), des données à caractère personnel dans le cadre de la fourniture du Service MyJanalya, conformément au Règlement (UE) 2016/679 (« **RGPD** »), notamment son article 28.

Les Parties reconnaissent que : - Le **Cabinet** est responsable de traitement des données qu'il enregistre dans le Service, notamment les données des Patientes (catégorie spéciale art. 9 RGPD — santé). - **Janalya IT** agit en sous-traitant, sur instructions documentées du Cabinet.

Article 1 — Définitions

Les termes utilisés dans le présent DPA ont la signification qui leur est donnée par le RGPD (art. 4), notamment : - **« Données à caractère personnel »** : toute information se rapportant à une personne physique identifiée ou identifiable. - **« Traitement »** : toute opération effectuée sur des données (collecte, enregistrement, conservation, modification, consultation, communication, effacement, etc.). - **« Violation de données »** : toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données.

Article 2 — Objet, durée et nature du traitement

Élément	Description
Objet	Hébergement et traitement technique des données nécessaires au fonctionnement du Service MyJanalya

Durée	Durée de l'Abonnement souscrit par le Cabinet, prolongée des durées légales de conservation (cf. art. 9)
Nature	Hébergement sécurisé, sauvegardes, indexation, génération de documents (PDF), envoi de communications (emails), OCR
Finalités	Gestion de fiches patientes, génération de consentements éclairés, plans de traitement, communication avec les patientes, statistiques cabinet

Article 3 — Catégories de personnes concernées et de données

3.1. Personnes concernées

- **Patientes** du Cabinet
- **Praticiennes** et collaborateurs du Cabinet (utilisateurs du Service)

3.2. Catégories de données — Patientes

Catégorie	Exemples	Sensible (art. 9 RGPD) ?
Identification	Nom, prénom, date de naissance, sexe, photo de profil	Non
Coordonnées	Email, téléphone, adresse postale	Non
Santé	Antécédents médicaux, contre-indications, allergies, traitements en cours	**Oui**
Données cliniques	Photos avant/après, paramètres de soins (énergie laser, durée cryo)	**Oui**
Consentements signés	PDF de consentements éclairés horodatés	**Oui** (preuve consentement Art. 9.2.h)
Historique de prestations	Dates de séances, types de soins, suivi	Indirectement (lié à santé)

3.3. Catégories de données — Praticiennes

- Identification (nom, prénom, email)
- Authentification (mot de passe haché, JWT, logs de connexion)
- Profil professionnel (rôle : Administrateur / Praticien / Lecture seule)

Article 4 — Instructions documentées du Responsable de traitement

4.1. Janalya IT s'engage à ne traiter les données **que sur instructions documentées** du Cabinet, telles que résultant : - Du paramétrage du Compte par le Cabinet (création de fiches, envoi de consentements, etc.) - Des présentes CGV et DPA - Des éventuelles instructions complémentaires écrites données par le Cabinet

4.2. Si Janalya IT est tenue, en vertu du droit de l'Union ou d'un État membre, de procéder à un traitement non prévu par les instructions, elle en informe le Cabinet **avant le traitement**, sauf si ce droit interdit cette information pour des motifs importants d'intérêt public.

Article 5 — Confidentialité

5.1. Janalya IT veille à ce que les personnes autorisées à traiter les données **s'engagent à respecter la confidentialité** ou soient soumises à une obligation légale de confidentialité.

5.2. L'accès aux données de Patientes est strictement limité au personnel de Janalya IT dont l'accès est **nécessaire à la fourniture du Service** et **journalisé**. Aucun accès du personnel Janalya IT au contenu clinique en clair n'a lieu sans autorisation préalable écrite du Cabinet (sauf cas d'incident technique critique documenté).

Article 6 — Sécurité du traitement (Article 32 RGPD)

Janalya IT met en œuvre les mesures techniques et organisationnelles suivantes :

6.1. Mesures techniques

- **Chiffrement en transit** : TLS 1.3 obligatoire (HSTS preload, redirection HTTP→HTTPS forcée)
- **Chiffrement au repos** : base PostgreSQL chiffrée, sauvegardes AES-256
- **Authentification forte** : bcrypt pour mots de passe, JWT 12h, rate-limit anti-bruteforce (5 tentatives / 15 min)
- **Isolation multi-tenant** : `cabinet_id` requis sur toutes les requêtes, tests de régression IDOR automatisés en CI (GitHub Actions quotidien)
- **Validation des entrées** : magic bytes sur uploads (PDF + 16 formats), protection path traversal
- **Headers de sécurité** : CSP strict, X-Frame-Options DENY, X-Content-Type-Options nosniff, Referrer-Policy strict-origin-when-cross-origin, Permissions-Policy
- **WAF + protection DDoS** : Cloudflare en front
- **Pentest** : interne semestriel, externe (à programmer pour >30 cabinets)

6.2. Mesures organisationnelles

- Sauvegardes chiffrées quotidiennes hors site (NAS dédié, lien VPN Tailscale)
- Plan de reprise d’activité (PRA) documenté et testé
- Journalisation des actions sensibles (création/suppression/export de données)
- RBAC : 3 rôles (Administrateur, Praticien, Lecture seule)
- Mises à jour de sécurité : CVE critiques sous 48h
- Cycle de vie sécurisé (revue de code, dépendances, audits réguliers)

6.3. Évolution des mesures

Les mesures ci-dessus peuvent évoluer pour intégrer les meilleures pratiques de l’état de l’art. Toute évolution sera notifiée au Cabinet par mise à jour du présent DPA dans son espace client.

Article 7 — Sous-traitants ultérieurs

7.1. Le Cabinet **autorise** Janalya IT à recourir à des sous-traitants ultérieurs (« **sous-sous-traitants** ») pour la fourniture du Service.

7.2. **Liste des sous-traitants ultérieurs au jour de signature** :

Sous-traitant	Activité	Pays	Garanties RGPD
Hetzner Online GmbH	Hébergement serveurs	□□ Allemagne (UE)	DPA signé + ISO 27001
Brevo SA	Envoi emails transactionnels	□□ France (UE)	DPA signé
Cloudflare, Inc.	CDN, WAF, protection DDoS	□□ États-Unis	DPA + CCT UE-US
Stripe Payments Europe Ltd.	Paiement abonnements	□□ Irlande (UE)	DPA signé
Anthropic, PBC	OCR (reconnaissance texte sur photos formulaires)	□□ États-Unis	DPA + CCT UE-US + ZDR 30j

7.3. **Ajout ou changement de sous-traitant** : Janalya IT informe le Cabinet par email au moins **30 jours avant** tout ajout ou remplacement de sous-traitant. Le Cabinet peut s’opposer au changement par notification écrite motivée. À défaut d’opposition dans ce délai, le changement est réputé accepté.

7.4. **En cas d’opposition légitime** non levée par accord amiable, le Cabinet peut résilier l’Abonnement sans frais et obtenir le remboursement prorata temporis des sommes payées d’avance.

7.5. Janalya IT impose contractuellement à chaque sous-traitant ultérieur **les mêmes obligations de protection des données** que celles fixées dans le présent DPA, et demeure pleinement responsable devant le Cabinet de l’exécution des obligations par lesdits sous-traitants.

Article 8 — Transferts de données hors UE

8.1. Les transferts vers des sous-traitants situés hors UE (Cloudflare, Anthropic) sont encadrés par les **Clauses Contractuelles Types** (Décision UE 2021/914), signées avec chaque sous-traitant concerné.

8.2. Mesures supplémentaires en place : - Chiffrement TLS de bout en bout - Minimisation des données envoyées (Anthropic : photos OCR uniquement, sans nom de Patiente associé) - Anthropic : rétention nulle au-delà de 30 jours sur les API payantes (à confirmer en signature explicite Zero Data Retention)

Article 9 — Droits des personnes concernées

9.1. Janalya IT **assiste** le Cabinet, dans la mesure du possible et compte tenu de la nature du traitement, pour répondre aux demandes des personnes concernées (Patientes et Praticiennes) au titre de leurs droits (art. 15 à 22 RGPD).

9.2. **Fonctionnalités intégrées au Service** facilitant l'exercice de ces droits : - Export ZIP de l'ensemble des données d'une Patiente (portabilité) - Suppression d'une fiche Patiente - Anonymisation à la place de la suppression (option configurable) - Modification des données

9.3. Si une Patiente s'adresse directement à Janalya IT, Janalya IT redirige la demande vers le Cabinet et l'en informe sans délai.

Article 10 — Notification de violation de données

10.1. Janalya IT notifie au Cabinet toute violation de données la concernant **dans les meilleurs délais** après en avoir pris connaissance, et **au plus tard 48 heures**.

10.2. La notification précise : - La nature de la violation - Les catégories et le nombre approximatif de personnes concernées - Les catégories et le nombre approximatif d'enregistrements concernés - Les conséquences probables - Les mesures prises ou proposées pour remédier à la violation

10.3. **Le Cabinet, en sa qualité de Responsable de traitement, reste seul tenu** de notifier la violation à la CNIL (sous 72h, art. 33 RGPD) et, le cas échéant, aux personnes concernées (art. 34 RGPD). Janalya IT lui apporte toute l'assistance nécessaire.

Article 11 — Analyse d'impact (DPIA)

Janalya IT met à la disposition du Cabinet, sur demande, les informations utiles à la réalisation par le Cabinet d'une analyse d'impact relative à la protection des données (DPIA, art. 35 RGPD), notamment compte tenu du caractère sensible des données traitées (santé).

Article 12 — Audit

12.1. Le Cabinet (ou un auditeur tiers mandaté par lui, soumis à une obligation de confidentialité) peut **demander un audit** des mesures de sécurité mises en œuvre par Janalya IT, dans la limite de **1 audit par an** sauf incident.

12.2. Modalités : - Préavis : 30 jours - À la charge du Cabinet, sauf découverte d'un manquement significatif (alors à la charge de Janalya IT) - Périmètre raisonnable et proportionné (pas d'accès aux données d'autres Cabinets) - Engagement de confidentialité de l'auditeur

12.3. **Alternative** : Janalya IT peut fournir un rapport d'audit indépendant récent (ex. attestation ISO 27001, rapport de pentest externe) en lieu et place d'un audit sur site.

Article 13 — Suppression ou restitution des données

13.1. À la fin de l'Abonnement, et selon le choix exprès du Cabinet : - **Restitution** : Janalya IT met à disposition un export complet des données (format JSON + PDF) dans un délai de **15 jours**. - **Suppression** : Janalya IT procède à la suppression irréversible de toutes les données du Cabinet dans un délai de **30 jours**.

13.2. **Cas particulier — données médicales (10 ans)** : si le Cabinet n'a pas procédé à la récupération de l'archive médicale dans le délai légal de 30 jours post-résiliation, Janalya IT peut conserver les données dans un coffre-fort technique pendant la durée légale (10 ans, Art. 2226 Code civil — prescription décennale RC pro), à la charge financière du Cabinet (devis spécifique). À défaut d'accord, les données sont supprimées et le Cabinet en assume seul la responsabilité juridique.

13.3. Janalya IT remet au Cabinet un **certificat de suppression** attestant de la destruction des données.

13.4. **Sauvegardes** : les sauvegardes contenant des données du Cabinet sont conservées pendant **30 jours** maximum après la suppression principale, puis détruites automatiquement par rotation.

Article 14 — Coordonnées du contact RGPD

Partie	Contact
Janalya IT — Contact RGPD	`rgpd@janalya-app.fr`
Cabinet	(renseigné au moment de la souscription)

Si l'une des Parties désigne un Délégué à la Protection des Données (DPO), elle communique ses coordonnées à l'autre Partie.

Article 15 — Modifications

Le présent DPA peut être modifié pour tenir compte des évolutions législatives (RGPD, jurisprudence CJUE, lignes directrices CNIL/EDPB) ou techniques. Les modifications substantielles sont notifiées au Cabinet au moins **30 jours avant** leur entrée en vigueur, selon les modalités prévues à l'article 3.3 des CGV.

Article 16 — Loi applicable et juridiction

Le présent DPA est régi par le droit français. Tout litige relève de la compétence exclusive du Tribunal de commerce de Melun, sauf disposition légale d'ordre public contraire.

Annexe aux CGV B2B Janalya IT, version 1.0.