

ANNEXE DE SOUS-TRAITANCE DE DONNEES A CARACTERE PERSONNEL

1. Objet

Dans le cadre de l'utilisation du Programme, Orthalis est amenée à traiter des données à caractère personnel pour le compte du Client, pour fournir, selon les options choisies par le Client, des services de maintenance, de sauvegarde, d'hébergement du Programme ainsi que des prestations de formation à l'utilisation dudit Programme.

Dans ce contexte, le Client est le responsable du traitement et Orthalis est le sous-traitant, au sens du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (« **Règlement Général sur la Protection des Données** » ou « **RGPD** »).

La présente annexe a pour objet d'identifier les traitements en question et de définir les conditions de leur réalisation.

2. Description du traitement faisant l'objet de la sous-traitance

Orthalis est autorisée à effectuer pour le compte du Client les traitements de données à caractère personnel suivants :

- (i) Les catégories de personnes concernées par les traitements de données à caractère personnel sont :
- Les patients des Clients ;
 - Les professionnels de santé exerçant au sein de la structure du Client ;
 - Les prospects ayant sollicité la réalisation de devis.

Ensemble dénommées au sein de cette annexe les « **Personnes Concernées** ».

- (i) Les types de données à caractère personnel comprennent, notamment :
- Les données d'identification des patients, à savoir les noms, prénoms, numéro de téléphone, adresse postale, adresse électronique, numéro de sécurité sociale ;
 - Les informations liées au suivi médical du patient, à savoir les comptes rendus de consultation, les clichés photographiques et radios ;
 - Les rendez-vous médicaux pris par les patients ;
 - Les échanges de correspondance entre le Client et les patients ;
 - Les informations financières relatives à la facturation des soins réalisés, le cas échéant les relances et encaissements réalisés ;
 - Les plannings des différents professionnels de santé exerçant au sein de la structure du Client.

Ensemble dénommées au sein de cette annexe les « **Données Confiées** ».

- (ii) La nature des opérations réalisées sur les Données Confiées dépend des prestations souscrites par le Client telles qu'indiquées au sein du Bon de commande :

- Maintenance du Programme ;
- Hébergement du Programme ;
- Sauvegarde du Programme ;
- Accès et manipulation des Données confiées dans le cadre de sessions de formation réalisées pour les besoins du Client ;

- (iii) Les finalités du traitement sont les suivantes :

- Gestion de la relation patient (suivi des rendez-vous et correspondance, suivi de prestations de soins et de la tarification, fourniture de questionnaires médicaux) pour le compte du Client ;
- Élaboration des plannings pour les praticiens ;
- Réalisation de statistiques par le Client.

3. Engagement d'Orthalis

Orthalis s'engage à :

- Traiter les Données Confiées uniquement pour les finalités détaillées dans la présente annexe ;
- Ne traiter les Données Confiées que conformément aux instructions documentées du Client figurant au sein des contrats et/ou offres commerciales communiquées dans toute correspondance écrite spécifique ultérieure, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou auprès d'une organisation internationale (à l'exception du cas où Orthalis est tenue de procéder à un traitement des Données Confiées en vertu du droit de l'Union européenne ou d'un État membre) ;
- Informer le Client au préalable lorsqu'elle est tenue de procéder à un tel traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;
- Informer immédiatement le Client, si elle considère qu'une instruction de ce dernier constitue une violation du RGPD ou de toute autre disposition du droit de l'Union européenne ou du droit des États membres relative à la protection des données ;
- Veiller à ce que les personnes autorisées à traiter les Données Confiées, s'engagent à respecter la confidentialité des Données Confiées ou soient soumises à une obligation légale appropriée de confidentialité et reçoivent la formation nécessaire en matière de protection des données à caractère personnel.

4. Engagement du Client

Le Client s'engage à respecter toutes les obligations spécifiques lui incombant en sa qualité de responsable du traitement des Données Confiées, au titre de la réglementation application et notamment du RGPD. Il est rappelé à ce titre que :

- En tant que responsable du traitement, il appartient au Client de s'assurer qu'il a une base légale valable

au sens de la réglementation applicable permettant le traitement des Données Confiées et que toute Donnée Confiée qu'il communique à Orthalis a été collectée de façon licite et loyale. Le Client déclare qu'il a collecté tous les consentements dont il a besoin, le cas échéant, pour permettre de traitement des données à caractère personnel des Personnes Concernées dans le respect de la réglementation applicable.

- Il appartient au Client, en tant que responsable du traitement, de fournir aux Personnes Concernées une information complète en vertu de la réglementation applicable, et notamment, selon le cas, des articles 13 et/ou 14 du RGPD.
- Le Client s'engage par ailleurs à documenter par écrit toute instruction concernant le traitement des données par Orthalis et à veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le RGPD sur la protection des données de la part d'Orthalis.

5. Sous-traitance ultérieure

Afin de réaliser les traitements des Données Confiées nécessaires pour fournir au Client les prestations prévues par le contrat, Orthalis peut avoir recours à des sous-traitants ultérieurs, lesquels mèneront des activités de traitements spécifiques pour le compte du Client. Le Client reconnaît ce fait et autorise le recours par Orthalis aux prestataires suivants, afin de traiter les Données Confiées, selon les prestations choisies et fournies au Client :

- (i) L'hébergement des données en France dans le cadre de la fourniture du service SaaS : la société AWS ;
- (ii) La sauvegarde des données en France : la société Arx One ;
- (iii) La réalisation de mission de maintenance et de support dans le cadre de l'utilisation du Programme : des prestataires externes implémentés au Maroc ;
- (iv) La société JUXTA pour la fourniture des licences de télétransmission FSV en France.

En cas de modification prévue des sous-traitants ultérieurs, soit en raison du remplacement d'un sous-traitant ultérieur, soit en raison du recrutement d'un nouveau sous-traitant ultérieur, Orthalis en informera le Client au préalable et le Client aura la possibilité d'émettre des objections à l'encontre des changements envisagés.

Tout sous-traitant ultérieur sera tenu de respecter des obligations en matière de protection des données au moins équivalentes à celles prévues dans le contrat. Ces obligations seront fixées au sein d'un contrat ou tout autre acte juridique entre Orthalis et le sous-traitant ultérieur. Lorsque le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, Orthalis demeure pleinement responsable devant le Client de l'exécution par le sous-traitant ultérieur desdites obligations.

6. Exercice des droits des personnes

Le Client est responsable de la gestion de toutes demandes des Personnes Concernées relatives à l'exercice de leurs droits en vertu de la réglementation applicable en matière de protection des données, notamment le droit d'accès, le droit de rectification, le droit d'effacement et d'opposition, le droit à la limitation du traitement, le droit à la portabilité des données et le droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage). Dans toute la mesure du possible, raisonnable et proportionné, et dans la limite de ce qui lui concerne, Orthalis apportera son aide au Client afin que celui-ci puisse s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des Personnes Concernées. L'assistance fournie par Orthalis dans ce cadre sera aux frais du Client.

7. Notification des violations de données à caractère personnel

Orthalis notifie au Client toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance. Orthalis fournira une assistance raisonnable afin de permettre au Client de respecter ses éventuelles obligations de notification de l'autorité de contrôle compétente et/ou de communication à la personne concernée par rapport à cette violation, aux frais du Client.

8. Aide d'Orthalis dans le cadre du respect par le Client de ses obligations

Compte-tenu de la nature du traitement et des informations à sa disposition, Orthalis apportera son aide raisonnable au Client pour la réalisation d'analyses d'impact relative à la protection des données et de la consultation préalable de l'autorité de contrôle, aux frais du Client.

9. Mesures de sécurité

Dans les conditions de l'article 32 du RGPD, à prendre toutes les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques pour les droits et libertés des personnes concernées, ainsi qu'à aider le Client à satisfaire à ses propres obligations à cet égard en regard du traitement des Données Confiées en vertu du contrat. Les mesures de sécurité fournies dépendent des prestations souscrites et choisies par le Client. A cet effet notamment, lorsque l'hébergement du Programme et la sauvegarde des données de celui-ci sont réalisés par le Client, le Client est seul responsable de la bonne exécution de ceux-ci.

Le Client s'engage à prendre toutes les mesures techniques et organisationnelles appropriées, conformément à l'article 32 du RGPD, afin d'assurer un niveau de sécurité adapté au risque dans le cadre de l'utilisation du Programme.

10. Durées de conservation et sort des Données Confiées

La durée pendant laquelle d'Orthalis est autorisée par le Client à conserver les Données Confiées pourra être précisée au sein d'instructions documentées. Sauf instruction documentée contraire de la part du Client, l'ensemble des données collectées, stockées, agrégées et analysés seront conservées au sein du Programme proposé par d'Orthalis pendant toute la durée du contrat conclu

entre Orthalis et le Client. Au terme de la prestation de services relative au traitement des Données Confiées, Orthalis s'engage à supprimer ou à anonymiser toutes les Données Confiées dans les 30 jours suivant la fin du contrat (à moins que le droit de l'Union européenne ou le droit applicable d'un l'État membre n'exige la conservation desdites données). Sur demande écrite du Client, Orthalis renverra au Client, aux frais de ce dernier, toutes les Données Confiées préalablement à leur suppression des systèmes d'Orthalis.

11. Contrôle du respect des obligations d'Orthalis

Orthalis met à la disposition du Client toutes les informations nécessaires pour démontrer le respect de ses obligations prévues dans la présente annexe et permettra à ces fins la réalisation d'audits dans les conditions suivantes :

- Le Client ne pourra pas mener plus d'un audit par période de douze (12) mois.
- Le Client supportera seul tous les coûts de l'audit.
- L'audit doit être effectué pendant les heures ouvrées et ne doit pas dépasser 2 jours ouvrés.
- L'audit pourra être réalisé par le Client directement ou par l'intermédiaire d'un tiers indépendant. Dans ce dernier cas, la sélection des auditeurs externes sera convenue entre les Parties. Les auditeurs doivent être titulaires d'une assurance responsabilité professionnelle garantissant l'audit, leur responsabilité pouvant être recherchée par Orthalis en cas de dommage causé à ce dernier.
- Le Client notifiera Orthalis avec un préavis écrit de trente (30) jours minimum, afin que les Parties puissent convenir mutuellement d'une date d'audit.
- Le Client doit s'assurer que le déroulement de l'audit ne perturbe pas l'exécution par Orthalis de ses obligations au titre du contrat, ni l'activité d'Orthalis en général.
- Au cas où l'audit entraîneraient des interruptions de tout ou partie des prestations d'Orthalis, les Parties conviennent que ces interruptions ne seront pas prises en compte dans l'évaluation du respect des engagements de qualité de service d'Orthalis et qu'Orthalis ne pourra en être tenu responsable.
- Tous les documents, informations ou données, quel qu'en soit le support, confiés par Orthalis aux auditeurs et/ou au Client pendant l'audit, ont un caractère confidentiel et devront être traités comme tels.
- Orthalis s'engage à contribuer aux audits, aux frais du Client.
- Le Client est responsable de toute perte ou dommage occasionné à Orthalis en raison de l'audit, que l'audit soit effectué par le Client directement ou par des auditeurs externes.