Accord de protection des données

Ref: Olaqin_CG_ANNEXE_RGPD_Plateforme_Stellair_202601

1. Introduction

L'Accord de protection des données (ci-après "Accord") vise à régir l'utilisation des Données à caractère personnel des clients (ci-après le "responsable de traitement" ou "Client") de OLAQIN (ci-après le "Sous-traitant" ou "OLAQIN") lorsqu'ils utilisent le service Plateforme Stellair SaaS (ci-après le "Service").

2. Définitions

Les termes "décision d'adéquation", "mesures techniques et organisationnelles", "personnes concernées", "protection dès la conception", "protection par défaut", "registre", "responsable(s) conjoint(s)", "responsable des activités de traitement", "sous-traitant", "traitement", "violation de données à caractère personnel" présents dans l'Accord ont les significations décrites aux articles 4 et suivants du RGPD.

Les autres termes sont définis ci-après :

- « **Accord** » désigne l'annexe au Contrat régissant l'utilisation des Données à caractère personnel du Client conformément aux dispositions de l'article 28 du RGPD aussi intitulé "Data Processing Addendum" ("DPA").
- « **AIPD** » : désigne une analyse d'impact qui permet de vérifier la proportionnalité des traitements de Données à caractère personnel et de prévenir les risques liés à un traitement de Données à caractère personnel
- « **Anonymisation** » : désigne un traitement visant à rendre impossible l'identification des personnes concernées par les traitements réalisés dans le cadre du Service, et ce de manière irréversible
- « **Autorité de contrôle** » : désigne l'autorité de contrôle en matière RGPD compétente pour le Service fourni par le Sous-traitant
- « **Client** » : désigne l'entité ayant souscrit au Service fourni par le Sous-traitant
- « **Contrat** » : désigne le contrat conclu entre le Sous-traitant et le Client afin d'utiliser le Service auquel est annexé le présent Accord
- « **Demande(s) de droit** » : désigne le ou les droits fondamentaux créés par le RGPD aux articles 15 et suivants (ex : droit d'accès, droit d'effacement, etc.).
- « **Données à caractère personnel du Client** » : désigne toute donnée se rapportant à une personne physique identifiée ou identifiable transmise au Sous-traitant et traitée par celui-ci pour le compte du Client dans le cadre du Service et dont la liste détaillée est présentée en annexe
- « **Partie(s)** » : désigne conjointement le Client et le Sous-traitant
- « **RGPD** » : désigne le 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 également intitulé "Règlement général sur la protection des données"
- « **Réglementation applicable en matière de protection des données à caractère personnel** » : désigne ensemble la Loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le RGPD
- « **Réversibilité** » : désigne l'opération visant à permettre le transfert et l'intégration, dans un format utilisable et reconnu, des Données à caractère personnel du Client du Service du Sous-traitant vers un service équivalent proposé par un autre prestataire.
- « **Serveur HDS** » : désigne les serveurs certifiés "Hébergeur de données de santé" par les autorités françaises
- « **Service SaaS** » : désigne un logiciel hébergé par le Sous-traitant et pouvant être utilisé simultanément par un nombre infini de clients
- « **Sous-traitant ultérieur** » : désigne les sous-traitants recrutés par le Sous-traitant pour traiter les Données à caractère personnel du Client dans le cadre exclusif du Service
- « **Utilisateurs finaux** » : désigne les personnes dont les Données à caractère personnel sont traitées par le Sous-traitant pour le compte du Client.

3. Relations contractuelles et durées

L'Accord est une annexe indivisible au Contrat signé entre le Client et le Sous-traitant pour l'utilisation du Service.

En cas de contradiction entre le Contrat conclu pour l'utilisation du Service et l'Accord, les obligations prévues dans l'Accord prévalent sur le Contrat en ce qui concerne le RGPD dans son ensemble.

L'Accord est applicable pendant toute la durée du Contrat conclu dans le cadre de l'utilisation du Service et peut se poursuivre au-delà tant que toutes les obligations prévues aux présentes restent applicables.

4. Rôle des Parties et champ d'application

Le Client agit, dans le cadre de l'Accord, comme responsable des activités de traitement et OLAQIN agit en tant que sous-traitant au sens de l'article 28 du RGPD.

En aucun cas, les Parties ne peuvent être considérées comme étant responsables conjoints dans le cadre du Service. Toutefois, les Parties conviennent qu'en cas d'erreur ou de modification de leur qualification, les Parties devront se réunir, dans les meilleurs délais, pour modifier l'Accord et prendre toutes les mesures relatives à une telle situation pour se conformer aux exigences de la Réglementation applicable en matière de protection des données à caractère personnel.

L'Accord régit exclusivement les traitements des Données à caractère personnel du Client réalisés dans le cadre du Service en tant que Sous-traitant au sens de l'article 28 du RGPD à l'exclusion des traitements réalisés en tant que responsable du traitement par OLAQIN qui sont encadrés dans le Contrat.

5. Instructions et engagements

Le Sous-traitant s'engage à n'utiliser les Données à caractère personnel du Client dans le cadre de l'utilisation du Service que sur instructions documentées en annexe de l'Accord. Le Sous-traitant informe immédiatement le Client s'il estime qu'une instruction apportée par ce dernier est illégale au regard de la Réglementation applicable en matière de protection des données à caractère personnel. La responsabilité du Sous-traitant ne saurait être engagée dans le cas où, malgré la notification du Sous-traitant concernant l'illégalité de l'instruction, le Client maintient et applique cette instruction par l'intermédiaire du Service.

Le Sous-traitant s'engage à respecter les dispositions du RGPD et, en particulier, à tenir un registre des activités de traitement spécifique au Service et à développer son Service dans le respect des règles de "Protection dès la conception" et de "Protection par défaut".

Le Sous-traitant s'engage à ne jamais transférer les Données à caractère personnel du Client, pour d'autres raisons que la fourniture du Service et s'engage à ne jamais utiliser les Données à caractère personnel du Client pour son propre intérêt, en tant que responsable du traitement.

Le Sous-traitant déclare que l'intégralité du personnel interne ou externe amené à traiter les Données à caractère personnel du Client est engagé par un ou plusieurs actes juridiques contraignants et fait régulièrement l'objet de formations et de sensibilisations.

Le Sous-traitant s'engage à garantir la sécurité des Données à caractère personnel du Client et à mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires pour son Service dont le détail est présenté en annexe de l'Accord.

En revanche, le Sous-traitant n'est jamais responsable des manquements du Client concernant la Réglementation applicable en matière de protection des données à caractère personnel lorsqu'il utilise le Service en tant que responsable du traitement.

6. Assistance pour la réalisation des AIPD

Les AIPD doivent être réalisées par le Client, conformément aux dispositions du RGPD. Néanmoins, le Sous-traitant s'engage à communiquer, sur demande écrite du Client, toutes les informations nécessaires et requises pour que le Client puisse assurer la réalisation d'une AIPD.

Le Sous-traitant n'est en revanche pas tenu de réaliser les AIPD à la place et pour le compte du Client. Toute demande complémentaire à la communication d'informations peut faire l'objet d'un refus.

7. Assistance pour les Demandes de droit

Les Demandes de droit envoyées par les Utilisateurs finaux sont transférées au Client dans les meilleurs délais. Le Sous-traitant n'est pas tenu de tenir un inventaire des Demandes de droit pour le compte du Client et n'est pas responsable des manquements du Client dans la gestion des Demandes de droit.

Le Sous-traitant exécute, sur demande écrite du Client, les actions techniques à entreprendre pour que le Client puisse s'acquitter de son obligation de donner suite aux demandes des personnes concernées.

Le Client accepte et comprend que le Sous-traitant n'est pas tenu de gérer les Demandes de droits des personnes effectuées dans le cadre du Service à la place et pour le compte du Client. Toute demande complémentaire visant à assurer une telle gestion fera l'objet d'un refus.

Les Demandes de droit envoyées au Sous-traitant en tant que responsable du traitement sont traitées exclusivement par le Sous-traitant et ne sont pas transférées au Client.

8. Assistance sur les mesures de sécurité

Le Sous-traitant s'engage à communiquer toutes les informations nécessaires et requises sur les mesures de sécurité techniques et organisationnelles à mettre en œuvre pour garantir la sécurité des Données à caractère personnel du Client dans le cadre de la fourniture du Service.

9. Violations de Données à caractère personnel

Le Sous-traitant s'engage à notifier au Client, dans les meilleurs délais et, au plus tard, 48 heures ouvrées après en avoir pris connaissance, toute violation de données à caractère personnel en lien avec le Service susceptible de concerner les Données à caractère personnel du Client ainsi que toutes les informations nécessaires et requises en sa possession pour réduire les effets de la violation de données à caractère personnel. Le Client accepte et reconnaît que le délai de 72h s'appliquant à lui ne démarre qu'à compter de la connaissance de la violation de données à caractère personnel et, qu'à ce titre, le délai de 48h ouvrées respecte le RGPD.

Le Sous-traitant n'est pas autorisé à prendre en charge les notifications de violation de données à caractère personnel auprès de l'Autorité de contrôle et à informer, pour le compte du Client, les Utilisateurs finaux. Toute demande en ce sens de la part du Client fera l'objet d'un refus.

10. Sous-traitants ultérieurs

Le client autorise le sous-traitant à sous-traiter l'hébergement des Données Personnelles relatives à la santé auprès d'un hébergeur ayant reçu l'agrément « Hébergement des données de santé .

Plus généralement, le Client octroie au Sous-traitant l'autorisation générale de recruter des Sous-traitants ultérieurs à condition d'être informé de tout changement sur ces Sous-traitants ultérieurs dans les meilleurs délais afin de permettre au Client d'émettre des objections. Le Client accepte et reconnaît qu'une autorisation spécifique, pour un outil SaaS, n'est pas applicable et pourrait mener à un blocage du Service.

A défaut d'objections soulevées par le Client sous huit (8) jours à compter de la notification, le nouveau Sous-traitant ultérieur est définitivement recruté sans que le Client puisse s'y opposer, réclamer des dommages intérêts ou demander la résiliation du Contrat. Si l'objection formulée dans les délais est considérée comme recevable par le Sous-traitant, ce dernier peut proposer au Client l'une des solutions suivantes : i) le retrait du Sous-traitant ultérieur, ii) la mise en œuvre de mesures complémentaires pour garantir la sécurité des Données à caractère personnel du Client, iii) l'arrêt du Service sans que le Client puisse réclamer des dommages intérêts.

Pour être considérées comme recevables par le Sous-traitant, les objections doivent être objectives et sérieuses et être dûment démontrées. Les Parties acceptent que les situations suivantes soient, par défaut, considérées comme recevables : i) le Sous-traitant ultérieur proposé est un concurrent direct du Client, ii) le Sous-traitant ultérieur est dans une situation de contentieux avec le Client, iii) le Sous-traitant ultérieur a fait l'objet d'une condamnation par une Autorité de contrôle dans les 12 mois précédant son recrutement et iv) le Sous-traitant ultérieur ne respecte pas, si applicable, les règles applicables prévues en matière de transferts en dehors de l'Union européenne.

Le Sous-traitant s'engage à ne recruter que des Sous-traitants ultérieurs qui, après contrôle, présentent les garanties nécessaires et suffisantes pour assurer la sécurité et la confidentialité des Données à caractère personnel du Client. La relation entre le Sous-traitant et le Sous-traitant ultérieur doit être encadrée dans un accord présentant des obligations similaires au présent Accord.

Le Sous-traitant reste responsable, dans les limites de responsabilité prévues au Contrat, des manquements au RGPD que pourraient réaliser ses Sous-traitants ultérieurs dans le cadre du Service.

11. Hébergement et transferts en dehors de l'Union européenne

11.1. Hébergement des données

Le Sous-traitant s'engage à faire son nécessaire pour héberger les Données à caractère personnel du Client exclusivement au sein d'un Etat membre de l'Union européenne. Le Client octroie l'autorisation au Sous-traitant de choisir l'Etat membre de l'Union européenne de son choix. En cas d'hébergement des Données à caractère personnel au sein d'un pays situé en dehors de l'Union européenne, le Sous-traitant s'engage à obtenir l'autorisation préalable du Client et à mettre en œuvre tous les mécanismes requis pour encadrer ce transfert comme conclure des Clauses contractuelles types et, le cas échéant, à mettre en œuvre des mesures techniques complémentaires visant à renforcer la sécurité des Données à caractère personnel du Client.

11.2. Transferts des données

Le Client octroie au Sous-traitant une autorisation générale de transferts en dehors de l'Union européenne si, de manière cumulative, i) les transferts sont effectués exclusivement auprès de Sous-traitants ultérieurs conformes au RGPD et que ii) les transferts sont effectués exclusivement vers un pays bénéficiant d'une décision d'adéquation ou sont encadrés par des garanties appropriées comme, en particulier, des Clauses contractuelles types. Si ces conditions ne sont pas respectées, les transferts hors de l'Union européenne ne sont autorisés qu'avec l'accord préalable du Client. Des mesures de sécurité techniques complémentaires visant à renforcer la sécurité des Données à caractère personnel du Client doivent être obligatoirement mises en œuvre dans le cas où les Données à caractère personnel seraient transférées vers un pays non démocratique.

11.3. Hébergement et transferts des données de santé

Par exception aux dispositions précédentes, le Sous-traitant s'engage à ce que les données sensibles de santé traitées dans le cadre du Service soient hébergées exclusivement sur des Serveurs "HDS" situés en France. De même, le Sous-traitant s'engage à ne jamais transférer de données sensibles de santé en dehors de l'Union européenne sauf accord préalable ou instructions du Client.

12. Durées de conservation et sort des Données à caractère personnel du Client

Le Sous-traitant s'engage à ne conserver les Données à caractère personnel du Client que pour la durée de l'utilisation du Service, conformément aux instructions détaillées en annexe, et à les supprimer à la fin du Contrat. Le Sous-traitant atteste, sur demande écrite, de la suppression des Données à caractère personnel et de toutes les copies existantes.

Le Client est informé qu'il doit récupérer ses Données à caractère personnel avant la fin de l'Accord. A défaut, le Client ne peut plus récupérer ses Données à caractère personnel, la suppression des données à caractère personnel étant irréversible et définitive. Le Sous-traitant ne pourra être tenu responsable d'une perte des Données à caractère personnel après leur suppression, le Client en assumant l'entière responsabilité. Le Client accepte que l'anonymisation totale et irréversible et définitive des Données à caractère personnel du Client soit utilisée comme moyen de suppression et que le Sous-traitant conserve les données anonymisées pour l'amélioration du Service, comme cela est accepté pour les Autorités de contrôle.

Le Sous-traitant informe le Client que la restitution des Données à caractère personnel prévue dans le RGPD ne constitue pas une Réversibilité des données vers un nouveau sous-traitant et que toute demande en ce sens sera toujours refusée par le Sous-traitant.

13. Audits

Le Client dispose du droit de réaliser un audit sous forme de questionnaire écrit une fois par an pour vérifier le respect du présent Accord. Le questionnaire a la force d'un engagement sur l'honneur qui engage le Sous-traitant. Le questionnaire peut être communiqué sous n'importe quelle forme au Sous-traitant qui s'engage à y répondre dans les meilleurs délais à compter de sa réception.

Le Client dispose également du droit de réaliser, une fois par an et à ses frais, un audit sur site, le cas échéant dans les locaux du Sous-traitant en cas de violation de données due à un manquement avéré et démontré du Sous-traitant ayant entraîné un préjudice dûment justifié au Client. Un audit dans les locaux du Sous-traitant peut être mené soit par le Client soit par un tiers indépendant désigné par le Client et doit être notifié par écrit au Sous-traitant au minimum trente (30) jours avant la réalisation de l'audit. Le Sous-traitant dispose du droit de refuser le choix du tiers indépendant si ce dernier est i) un concurrent direct ou indirect du Sous-traitant, ii) en situation de conflit d'intérêts avec le Sous-traitant (ex : conseil d'un concurrent du Sous-traitant) ou ii) en précontentieux ou contentieux avec le Sous-traitant. Dans ce cas, le Client s'engage à choisir un nouveau tiers indépendant pour réaliser l'audit. Le Sous-traitant peut refuser l'accès à certaines zones pour des raisons de confidentialité ou de sécurité. Dans ce cas, le Sous-traitant effectue l'audit dans ces zones et communique les résultats au Client.

En cas d'écart constaté dans le cadre de l'audit, le Sous-traitant s'engage à mettre en œuvre, sans délai et à ses frais, les mesures nécessaires pour être en conformité avec le présent Accord. Les écarts ne peuvent concerner que la Réglementation applicable en matière de Données à caractère personnel du Client et ne sauraient concerner des procédures ou des mesures internes mises en œuvre par le Client à titre spécifique. Les écarts doivent être dûment démontrés, justifiés et documentés.

En cas de contestation par le Sous-traitant des écarts identifiés, le Sous-traitant peut, au choix et sur acceptation écrite et préalable du client, proposer de i) se réunir afin de trouver une solution amiable et un compromis, ii) saisir l'Autorité de contrôle afin d'obtenir un arbitrage sur le litige, et iii) saisir un expert indépendant pour arbitrer le litige.

14. Coopération avec les autorités

Le Sous-traitant s'engage à coopérer avec la CNIL, l'Autorité de contrôle compétente, en cas de contrôle concernant les traitements réalisés dans le cadre du Service et s'engage à notifier dans les plus brefs délais le Client en cas de demandes concernant ses Données à caractère personnel formulées par l'Autorité de contrôle ou par une autorité administrative, judiciaire ou policière.

15. Contact

Le Client et le Sous-traitant désignent chacun un interlocuteur chargé du présent Accord qui sera le destinataire des différentes notifications et communications devant intervenir dans le cadre de l'Accord.

Le Sous-traitant informe le Client qu'il a nommé la société Dipeeo SAS comme Délégué à la protection des données qui peut être contactée aux coordonnées suivantes :

- Adresse email : dpo@olaqin.fr
- Adresse postale : Société Dipeeo SAS, 95 avenue du Président Wilson, 93100 Montreuil, France
- Numéro de téléphone : 01 59 06 81 85

16. Révisions

Le Sous-traitant se réserve la possibilité de modifier le présent Accord en cas d'évolution des règles applicables en matière de protection des Données à caractère personnel ou en cas de modification du Service qui auraient pour effet de modifier l'une de ses dispositions.

ANNEXES DPA
Annexe 1 - Instructions détaillées du Client

Ref: Olaqin_CG_ANNEXES_DPA_INSTRUCTION_CLIENTS_202601

17. Liste des traitements

17.1. Finalités et fondements légaux

Le Service fourni par le Sous-traitant a pour objectif de permettre au client (le Responsable de traitement) de bénéficier de la plateforme Stellair d'Olaqin.
La plateforme Stellair constitue une infrastructure technologique cloud conçue pour mettre à disposition des briques techniques et/ou réglementaires nécessaires aux services proposés par Olaqin, notamment :

- la facturation sécurisée SESAM-Vitale,
- la télé-mise à jour de la carte Vitale,
- la gestion et le suivi des paiements,
- l'accès et l'intégration de fonctionnalités réglementaires dans le cadre du parcours de soins,
- la sécurisation des échanges entre le client et les organismes payeurs (Assurance Maladie, mutuelles).

La plateforme est hébergée dans le cloud, ce qui assure une accessibilité permanente et sécurisée depuis tout type de terminal connecté (ordinateur, tablette, smartphone).

Elle propose en particulier des APIs REST sécurisées, permettant aux partenaires BtoB, d'intégrer directement les fonctionnalités de facturation, de mise à jour des cartes santé et de gestion des droits patients dans leurs propres solutions logicielles (ex. logiciel de gestion officinale).

Dans le cadre de la fourniture du Service, le Sous-traitant met en œuvre, pour le compte du Responsable de traitement, les traitements suivants :

- **Hébergement et stockage** des données à caractère personnel des patients nécessaires à la facturation SESAM-Vitale et à la gestion des flux de paiement ;
- **Duplication et sauvegarde** de ces données sur des serveurs redondants afin d'assurer la continuité de service et la restauration en cas d'incident ;
- **Traitement et gestion** des données patients (identification, droits ouverts, remboursement, suivi des paiements) dans le cadre du Service ;
- **Gestion de la sécurité, supervision et maintenance** de la plateforme, y compris la mise en œuvre de mesures techniques et organisationnelles pour garantir la confidentialité, l'intégrité et la disponibilité des données ;
- **Hébergement et traitement des zones de commentaires libres** saisis par les professionnels de santé dans le cadre de l'utilisation du Service ;
- **Traçabilité des accès et des opérations** réalisées sur les données, afin d'assurer la conformité aux obligations légales et réglementaires applicables (RGPD, règles CNIL, référentiels de l'Assurance Maladie).

Les traitements mis en œuvre sont réalisés exclusivement dans le cadre de l'exécution du Contrat.

17.2. Personnes concernées

Les personnes concernées dans le cadre du Service sont :

- Les Utilisateurs finaux/patients

17.3. Opérations de traitements

Les opérations de traitement réalisées dans le cadre du Service sont détaillées ci-après :

- Adaptation
- Communication aux Sous-traitants ultérieurs
- Conservation
- Collecte
- Enregistrement
- Modification
- Organisation
- Suppression
- Utilisation

17.4. Catégories de données traitées

Les Données à caractère personnel du Client traitées dans le cadre du Service sont les suivantes :

Données "standards" des Utilisateurs finaux :

- Données d'identification et coordonnées

Données "spécifiques" des Utilisateurs finaux :

- Carte vitale ou numéro de sécurité sociale

Données "sensibles" des Utilisateurs finaux :

- Santé

17.5. Durées de conservation

Les Données à caractère personnel du Client sont conservées pour la durée d'exécution du contrat.

- **Double électronique et accusés de réception** : conservés pendant **90 jours** à compter de la transmission des feuilles de soins, conformément à l'article **R.161-47 du Code de la sécurité sociale**.
- **Données de santé** : conservées pendant **10 ans** lorsqu'elles sont nécessaires pour la gestion d'un éventuel contentieux.
- **Numéros NIR : supprimés immédiatement**, aucune conservation n'étant autorisée ou requise.
- **Données d'identification des patients** : conservées pendant une durée maximale de 5 ans, en cohérence avec les finalités liées au suivi administratif et à la traçabilité.
- **Données de remboursement** : conservées pour la durée strictement nécessaire au traitement des demandes, puis archivées ou supprimées conformément aux obligations légales et réglementaires applicables.

18. Mesures de sécurité

18.1. Mesures de sécurité techniques

- Déconnexion automatique du compte utilisateur du Service après une certaine période d'inactivité
- Mots de passe complexes imposés aux utilisateurs du Service à la connexion
- Déconnexion automatique du compte Utilisateur en Back-office après une certaine période d'inactivité
- Double authentification des Utilisateurs en Back-office
- Mots de passe complexes imposés aux Utilisateurs en Back-office à la connexion
- Plateforme en https
- Tests d'intrusion à intervalles réguliers
- Traçabilité des accès
- Anti-spam pour les salariés
- Antivirus et firewall pour les salariés
- Empreintes digitales pour les salariés
- Mots de passe complexes pour les salariés
- Serveurs HDS
- Mots de passe fréquemment modifiés des salariés
- Système de limitation de tentatives d'accès pour les salariés
- VPN pour les ordinateurs des salariés

18.2. Mesures de sécurité organisationnelles

- Alarme
- Badges d'accès
- Charte des systèmes d'information
- Clause dédiée à la protection des données dans les contrats de travail
- Procédure d'habilitation
- Procédure en cas de demandes de droit des Utilisateurs finaux
- Procédure en cas de violation de données à caractère personnel
- PSSI
- Règles de bonne conduite
- Sensibilisation deux fois par an
- Vidéoprotection dans les locaux

Annexe 2 - Inventaire des Sous-traitants ultérieurs et des transferts hors UE

Ref: Olaqin_CG_ANNEXES_DPA_INVENTAIRE_SSTRAITANTS_202601

Nom du sous-traitant	Finalité	Localisation	Garanties appropriées	Transfert hors UE
CLARANET	Hébergement et sauvegarde des données patients	France	Certification HDS	Aucun transfert hors UE
HUBSPOT	Hébergement de données clientes	Allemagne	Respect RGPD	Aucun transfert hors UE
ASSURANCE MALADIE / GIE	Pro Santé Connect	France	Certification HDS	Aucun transfert hors UE