**Contrat de sous-traitance du traitement des données**(version du 18 février 2020)

entre

**Nom du cabinet médical**Adresse
Code postal, lieu

(ci-après le «Client»)

et

**Nom du prestataire de services en nuage (services cloud)**Adresse
Code postal, lieu

(ci-après le «Prestataire»)

concernant le traitement des données par le Prestataire

# Objet du contrat

## Le présent contrat précise les obligations des parties en matière de protection des données. Il s’applique à toutes les activités relevant de la fourniture des services cloud dans le cadre desquelles le Prestataire, ses collaborateurs et les tiers auxquels il fait appel ont accès à des données à caractère personnel du Client (ci-après «données personnelles»). Les modalités de traitement des données sont précisées ci-après :

* **traitement des données concerné :** fourniture de services cloud conformément au contrat-cadre.
* **catégories de données concernées :** données personnelles de base (par ex. collaborateurs, clients et partenaires commerciaux) ; données médicales des patients (résultats d’examens, diagnostics, données d’images); données de contact et de communication (numéros de téléphone, adresses de courriel, adresses IP)‑; données contractuelles (par ex. relations contractuelles, intérêt pour des produits) ; historiques de clients‑; données de facturation et de paiement‑; données de planification et de contrôle.
* **catégories de personnes concernées :** patients, clients, intéressés, collaborateurs, fournisseurs et partenaires commerciaux.

# Responsabilités et garantie

## Dans le cadre du présent contrat et des instructions données, le Client répond en tant que «responsable du traitement» de la légalité du traitement des données. Il répond en outre du respect des obligations légales d’information envers les tiers. Par ailleurs, le Client et le Prestataire répondent chacun du respect des dispositions relatives à la protection des données dans le cadre du traitement des données auquel ils procèdent.

* 1. Prestataire et Client se garantissent mutuellement qu’ils ont imposé une obligation de confidentialité à leurs collaborateurs et aux tiers auxquels ils font appel, ou que ceux-ci sont soumis à une obligation légale de confidentialité. Ils ont en outre informé ces personnes par écrit que leur obligation de confidentialité perdure après la fin de leur activité.

# Pouvoir du Client de donner des instructions

## Le Prestataire ne traite les données personnelles que dans les limites de ce qui a été convenu et conformément aux instructions du Client. Font exception les situations dans lesquelles le Prestataire est tenu de traiter ces données pour des raisons légales impératives. Dans de telles situations, le Prestataire informe le Client des exigences légales en la matière et ce, dans la mesure du possible, avant le début du traitement.

## Dans le cadre du présent contrat, le Client se réserve le droit de donner au Prestataire des instructions détaillées sur la nature, l’étendue et le déroulement du traitement des données, instructions qu’il peut préciser ou compléter ponctuellement. Le Prestataire informe immédiatement le Client s’il estime qu’une instruction viole la législation applicable. Il peut en suspendre la mise en œuvre jusqu’à ce que le Client l’ait confirmée ou modifiée et que les aspects relatifs à la responsabilité aient été clarifiés.

* 1. Le Prestataire renonce à tout droit de rétention éventuel, fondé sur quelque motif juridique que ce soit, sur les données personnelles faisant l’objet du présent contrat.

# Lieu du traitement des données

Le Prestataire et les tiers auxquels il fait appel ne sont autorisés à traiter les données personnelles qu’en Suisse, dans un État membre de l’Union européenne (UE) ou dans un État signataire de l’accord sur l’Espace économique européen (EEE). Le Prestataire informe le Client par écrit des lieux où sont traitées les données, ainsi que des éventuelles délocalisations dans les pays susmentionnés. Une telle délocalisation est réputée acceptée faute d’opposition écrite du Client dans un délai de trente jours.

Tout traitement des données hors de la Suisse, de l’UE ou de l’EEE nécessite l’accord écrit préalable du Client. Celui-ci consent au traitement des données pour autant qu’il soit établi que le niveau de sécurité est le même dans le lieu concerné et qu’aucune disposition légale applicable au Client ne s’y oppose. Il incombe au Prestataire d’apporter cette preuve.

Si les données sont traitées hors de Suisse, le Prestataire répond en tout état de cause du respect et de la mise en œuvre des exigences légales liées à la garantie d’un niveau de sécurité adéquat pour l’ensemble du traitement et du transfert des données concernées.

# Obligations du Prestataire

## Traitement des données : Le Prestataire s’engage à traiter les données personnelles et les résultats du traitement uniquement dans le cadre des instructions du Client. Le traitement des données aux fins personnelles du Prestataire ou d’un tiers nécessite l’accord écrit du Client. Si le Prestataire reçoit d’une autorité l’injonction de lui remettre les données du Client, il doit – pour autant qu’il y soit autorisé – en informer immédiatement le Client et renvoyer l’autorité à ce dernier.

## Mesures de sécurité : Le Prestataire s’organise de manière à répondre aux exigences particulières liées à la protection des données. Il prend des mesures techniques et organisationnelles pour protéger de manière adéquate les données personnelles contre les abus et les pertes, conformément aux dispositions légales applicables en matière de protection des données. Sur demande, il est tenu de fournir la preuve de ces mesures au Client et aux autorités de surveillance. Cette preuve concerne notamment la mise en œuvre des mesures découlant de l’art. 32 RGPD. À condition de pouvoir en démontrer l’adéquation, le Prestataire peut prendre d’autres mesures pour autant qu’elles satisfassent au niveau de protection convenu.

## Registre des activités de traitement : Le Prestataire tient un registre des activités de traitement auxquelles il procède, conformément à l’art. 30 RGPD. À la demande du Client, il lui fournit en tout temps les informations requises en vertu de l’art. 30 RGPD et lui présente ledit registre.

## Analyse d’impact relative à la protection des données : Le Prestataire assiste le Client dans le cadre de l’analyse d’impact relative à la protection des données en lui fournissant toutes les informations dont il dispose et, sur demande, lui fournit notamment les catalogues de mesures pertinents ou lui apporte son concours lors des consultations des autorités de surveillance.

## Délégué à la protection des données : Le Prestataire confirme qu’il a désigné un délégué à la protection des données. Il veille à ce que celui-ci possède les qualifications requises et l’expertise nécessaire. Les coordonnées du délégué à la protection des données sont indiquées sur le site internet du Prestataire.

##  Devoirs d’assistance : Le Prestataire aide le Client à respecter ses obligations légales en matière de protection des données (p. ex. mesures de sécurité des données, notification de violations à l’autorité de surveillance, avis à la personne concernée par une violation). En particulier, le Prestataire informe immédiatement le Client de toute violation des prescriptions ou instructions relatives aux données personnelles dont il a connaissance et prend toutes les mesures nécessaires pour sauvegarder les données et atténuer les éventuelles incidences négatives pour les personnes concernées.

## Droits des personnes concernées : Le Prestataire prend les mesures techniques et organisationnelles nécessaires pour que le Client puisse faire valoir les droits de la personne concernée conformément au RGPD (droits d’information, d’accès, de rectification et d’effacement, droit à la portabilité des données, droit d’opposition, et droit de ne pas faire l’objet d’une décision automatisée dans certains cas) dans le délai légal, et fournit au Client toutes les informations nécessaires à cette fin. Si le Prestataire reçoit une demande dans ce sens, il la transmet immédiatement au Client pour traitement.

## Obligation de destruction et de restitution : Le Prestataire ne rectifie, ne détruit ou ne bloque des données personnelles que sur instruction du Client et en respectant des procédures satisfaisant à la protection des données. Lorsque le contrat prend fin, le Prestataire est tenu de remettre au Client tous les résultats du traitement et les documents contenant les données personnelles ou, après accord du Client, de les détruire pour le compte de ce dernier. Si le Prestataire traite les données dans un format technique spécial, il est tenu, moyennant une indemnisation équitable, de communiquer les données au Client soit dans ce format, soit, à la demande du Client, dans un autre format courant.

## Insolvabilité : Si les données du Client se trouvant chez le Prestataire sont menacées d’une saisie ou d’un séquestre, d’une procédure d’insolvabilité ou d’une procédure concordataire, ou encore d’autres événements ou mesures du fait de tiers, le Prestataire doit immédiatement en informer le Client. Le Prestataire informe immédiatement tous les responsables concernés que le Client a la maîtrise et la propriété exclusives des données en sa qualité de «responsable du traitement».

* 1. **Obligation de contrôle** : Le Prestataire contrôle et documente l’exécution des obligations susmentionnées et, à la demande du Client, lui en fournit la preuve sous une forme appropriée.

# Rapports de sous-traitance

Le Prestataire fait appel aux services des tiers suivants qui traitent les données personnelles pour son compte («sous-traitants») :

|  |  |
| --- | --- |
| **Nom et adresse du sous-traitant** | **Description des prestations partielles** |
| Exemple S.A. | Hébergement du serveur  |
| Exemple S.A. | Hébergement du serveur |
| Exemple S.A. | Hébergement du serveur |
| Exemple S.A. | Hébergement du serveur |

## Le prestataire est tenu d’informer le Client par écrit de toute attribution de mandat à un autre sous-traitant. Faute d’opposition écrite et motivée dans un délai de trente jours, le Client est réputé accepter cette attribution.

# Droit de contrôle du Client

## Le Client est en droit de contrôler, dans la mesure nécessaire, le respect, par le Prestataire, des dispositions légales relatives à la protection des données, ainsi que le respect des dispositions contractuelles convenues entre les parties et de ses instructions. En particulier, le Prestataire s’engage à fournir au Client, sur demande écrite de celui-ci et dans un délai raisonnable, toutes les informations nécessaires pour pouvoir procéder à des contrôles.

## Après notification préalable, le Client peut procéder à des contrôles dans les locaux du Prestataire pendant les heures de bureau usuelles. Le Client est tenu de veiller à ce que les contrôles n’excèdent pas la mesure nécessaire, pour ne pas perturber de manière disproportionnée le processus d’exploitation du Prestataire. Le Client s’acquitte envers le Prestataire d’une indemnisation équitable pour les dépenses qui en découlent.

## En cas de mesures prises par l’autorité de surveillance à l’encontre du Client, le Prestataire doit communiquer à ce dernier toutes les informations nécessaires et permettre à l’autorité de surveillance compétente de procéder à des contrôles sur place. Le Prestataire doit informer le Client des mesures envisagées.

# Droit applicable et for

## Le présent contrat est soumis au droit suisse, sous réserve des dispositions du droit international suisse en matière de conflit de lois et de la Convention des Nations Unies sur les contrats de vente internationale de marchandises. Le for exclusif se trouve au siège social du Client.

# Signatures

Pour le Prestataire : Pour le Client :

Lieu et date : Lieu et date :

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature : Signature :

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_