**Convention de traitement de données en sous-traitance**

Version 03/2023

entre

**Nom du cabinet médical :**

**Adresse :**

**Code postal et lieu :**

(« client »)

et

|  |
| --- |
| [Nom][Adresse][Code postal et lieu] |

(« prestataire »)

concernant le traitement de données en sous-traitance par le prestataire

Table des matières

1 Objet et champ d’application 3

2 Responsabilités et garantie 3

3 Pouvoir du client de donner des instructions 3

4 Lieu du traitement des données 4

5 Obligations du prestataire 4

6 Respect du secret professionnel 6

7 Sous-traitance ultérieure 6

8 Obligations d’information et droits d’audit 6

9 Responsabilité 7

10 Durée et effets du contrat 7

11 Dispositions finales 7

12 Droit applicable et for 8

13 Signatures 8

Annexe 1 9

# Objet et champ d’application

## La présente convention précise les obligations des parties en matière de protection des données qui résultent du traitement en sous-traitance décrit dans le contrat du [date] concernant [descriptif du contrat] (« contrat principal »).

## L’ensemble des obligations décrites dans la présente convention s’applique à toutes les activités en lien avec le contrat principal, dans le cadre desquelles le prestataire, son personnel et les tiers auxquels il fait appel entrent ou peuvent entrer en contact avec des données à caractère personnel du client (« données personnelles »). En cas de contradiction entre les dispositions de la présente convention et celles du contrat principal, les dispositions de la convention prévalent dans tous les cas.

## Le prestataire traite les données personnelles pour le compte du client conformément à la description des prestations figurant dans le contrat principal. Cela peut notamment concerner les données personnelles suivantes :

* **Traitements de données effectués :** traitement de données en vertu du contrat, etc.
* **Catégories de données concernées :** données personnelles de base (p. ex. membres du personnel, patientèle, clientèle et partenaires commerciaux) ; données sur la santé ; coordonnées et données de communication (téléphone, e-mail, adresses IP, etc.) ; données contractuelles (p. ex. relations contractuelles, intérêts pour certains produits) ; historiques de la clientèle ; données de facturation et de paiement ; données de planification et de contrôle, etc.
* **Données sensibles :** données médicales de la patientèle (p. ex. résultats, dossiers médicaux, diagnostics, données d’imagerie, documents, etc.) ; données génétiques et biométriques ; données sur la sphère intime, etc.
* **Catégories de personnes concernées :** patientèle, clientèle, personnes intéressées, membres du personnel, fournisseurs et partenaires commerciaux, etc.

# Responsabilités et garantie

## Dans le cadre de la présente convention et des instructions données, le client doit veiller, en tant que « responsable du traitement », à la licéité du traitement des données et au respect des obligations légales d’informer vis-à-vis des tiers. Sur le plan interne, le client et le prestataire sont chacun responsables du respect des dispositions applicables en matière de protection des données dans le cadre des traitements de données qu’ils effectuent.

## Prestataire et client se garantissent mutuellement avoir soumis leur personnel et les tiers auxquels ils font appel à la confidentialité ou que ceux-ci sont soumis au devoir de confidentialité en vertu de la loi. Ils ont en outre attiré l’attention de ces personnes par écrit sur le fait que l’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 le cadre convenu et selon les instructions du client. En particulier, il ne les traite pas à ses propres fins. Sont exceptés les cas dans lesquels le prestataire est tenu d’effectuer un traitement pour des raisons juridiques impératives. Le cas échéant, le prestataire informe le client, dans la mesure où cela est autorisé, des exigences légales correspondantes avant le début du traitement.

## Dans le cadre de la présente convention, le client se réserve le droit de donner des instructions complètes sur la nature, l’étendue et le processus du traitement des données, droit qu’il peut concrétiser ou compléter par des instructions individuelles. Le prestataire doit immédiatement documenter l’instruction par écrit et la soumettre au client pour approbation. Le prestataire informe immédiatement le client s’il estime qu’une instruction constitue une violation d’une loi applicable. Il peut suspendre la mise en œuvre de l’instruction jusqu’à ce que le client la confirme en clarifiant la question de la responsabilité ou la modifie.

# Lieu du traitement des données

## Le prestataire et les tiers auxquels il fait appel ne peuvent traiter des 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 de traitement des données ainsi que des éventuels transferts au sein des pays susmentionnés. En l’absence d’opposition motivée par écrit dans un délai de 30 jours, un tel transfert est considéré comme accepté.

## Tout traitement de données hors de Suisse, de l’UE ou de l’EEE requiert le consentement écrit préalable du client. Ce dernier consent au traitement des données, pour autant qu’un niveau de protection des données équivalent au lieu en question soit démontré et qu’aucune disposition légale qui lui est applicable ne s’y oppose. L’obligation d’en apporter la preuve incombe au prestataire.

## Lorsque des données sont traitées hors de Suisse, le prestataire est dans tous les cas responsable du respect et de la mise en œuvre des exigences légales visant à garantir un niveau de sécurité adéquat lors du traitement et du trafic des données.

# Obligations du prestataire

## **Traitement des données :** Le prestataire s’engage à ne traiter les données personnelles et les résultats du traitement que dans le cadre des instructions du client. Si le prestataire reçoit une injonction des autorités lui ordonnant de transmettre des données du client, il doit, dans la mesure où cela est permis, en informer immédiatement le client et renvoyer l’autorité vers lui.

## **Mesures de sécurité :** Le prestataire conçoit son organisation de manière à répondre aux exigences particulières de la protection des données. Il prend toutes les mesures techniques et organisationnelles appropriées au risque et conformes à l’état de la technique pour garantir la confidentialité, la disponibilité et l’intégrité des données personnelles, la traçabilité du traitement ainsi que la résilience de ses services dans ce domaine. Ce faisant, il respecte au moins les mesures de sécurité définies à l’annexe 1. Sur demande, il justifie de ces mesures et de leur mise en œuvre vis-à-vis du client et des autorités de surveillance.

## **Registre des activités de traitement et règlement de traitement :** Le prestataire tient un registre des activités de traitement effectuées chez lui, dans la mesure où lui-même ou le client sont soumis à une telle obligation. Il met en tout temps à la disposition du client, à la demande de ce dernier, son registre des activités de traitement ainsi que les informations nécessaires à l’établissement d’un tel registre côté client. En cas de traitement automatisé de données sensibles à grande échelle, le prestataire doit établir un règlement de traitement, qui doit notamment contenir des indications sur l’organisation interne, la procédure de traitement et de contrôle des données ainsi que les mesures destinées à garantir la sécurité des données. Le client et le prestataire doivent régulièrement mettre à jour le règlement.

## **Analyse d’impact relative à la protection des données :** Si le client doit procéder à une analyse d’impact relative à la protection des données, le prestataire fournit les faits et informations techniques nécessaires à l’analyse concernant les traitements de données personnelles qu’il effectue pour le client et assiste ce dernier en conséquence lors de consultations des autorités de surveillance.

## **Obligations de soutien :** Le prestataire aide le client à respecter ses obligations légales en matière de protection des données (p. ex. mesures de sécurité des données, annonces des violations à l’autorité de surveillance, information de la personne concernée par une violation). En particulier, le prestataire informe immédiatement le client de toute violation de prescriptions ou d’instructions concernant les données personnelles dont il a connaissance et prend toutes les mesures nécessaires pour sauvegarder les intérêts des personnes concernées et atténuer les éventuelles conséquences négatives sur elles.

## **Droits des personnes concernées :** Le prestataire prend les mesures techniques et organisationnelles nécessaires pour permettre au client de respecter les droits de la personne concernée en vertu de la législation sur la protection des données applicable, notamment quant à l’information, à l’accès, à la rectification et à l’effacement (ou à l’anonymisation), à la portabilité des données, à l’opposition et à la prise de décision automatisée dans le cas d’espèce dans le délai légal, et transmet au client toutes les informations nécessaires à cet effet. Si une demande en ce sens est adressée au prestataire, celui-ci la transmettra immédiatement au client pour traitement.

## **Obligation d’effacement et de remise :** Le prestataire ne rectifie, n’efface (ou anonymise) ou ne bloque les données personnelles que sur instruction du client et garantit ce faisant des processus conformes à la protection des données. Les obligations de renseigner et de remise demeurent réservées. À la fin du contrat ou sur demande du client, le prestataire est tenu de remettre à ce dernier tout ou partie des résultats du traitement et des documents contenant des données personnelles ou, selon entente, de les détruire à sa demande. Si le prestataire traite les données dans un format technique spécial, il est tenu, moyennant un dédommagement raisonnable, de les remettre soit dans ce format, soit, à la demande du client, dans un autre format courant, de manière à ce qu’elles puissent être exportées vers une nouvelle application sans perte, tout en conservant leur structure et leur logique.

## **Journalisation :** Lors de traitements automatisés à grande échelle de données sensibles ou de profilage à risque élevé, le prestataire journalise au moins l’enregistrement, la modification, la lecture, la communication, l’effacement et la destruction des données. La journalisation est notamment nécessaire lorsque, sans cette mesure, il n’est pas possible de vérifier a posteriori que les données ont été traitées conformément aux finalités pour lesquelles elles ont été collectées ou communiquées. La journalisation doit fournir des informations sur l’identité de la personne qui a effectué le traitement, la nature, la date et l’heure du traitement et, le cas échéant, l’identité du destinataire des données. Les procès-verbaux de journalisation sont conservés durant au moins un an, séparément du système dans lequel les données personnelles sont traitées. Ils sont accessibles uniquement aux organes et aux personnes chargés de vérifier l’application des dispositions relatives à la protection des données ou de préserver ou de restaurer la confidentialité, l’intégrité, la disponibilité et la traçabilité des données, et peuvent être utilisés qu’à cette fin.

## **Insolvabilité :** Si une saisie, un séquestre, une procédure d’insolvabilité ou de concordat, ou d’autres incidents ou mesures de tiers mettent en péril les données du client qui se trouvent chez le prestataire, ce dernier est tenu d’en informer immédiatement le client. Le prestataire informera immédiatement toutes les autorités impliquées dans ce contexte que le client est seul souverain et propriétaire des données.

## **Obligation de contrôle :** Le prestataire contrôle et documente le respect des obligations susmentionnées et, à la demande du client, en apporte la preuve de manière appropriée.

# Respect du secret professionnel

## Il se peut que le prestataire traite ou accède à des données tombant sous le coup du secret professionnel au sens de l’art. 321 CP et dont la divulgation non autorisée est punissable en vertu du CP et de la LPD. Il s’engage à respecter le secret professionnel et à ne prendre connaissance de ces données que dans la mesure nécessaire à l’exécution des tâches qui lui sont confiées. Le prestataire doit, le cas échéant, faire usage du droit de refuser de témoigner selon l’art. 171 CPP et de l’interdiction de séquestre selon l’art. 262 CPP.

## Le prestataire veille à ce que le personnel et les tiers auxquels il fait appel se soient engagés par écrit à ne pas révéler sans autorisation les secrets professionnels auxquels ils ont eu accès et aient confirmé avoir été informés des éventuelles peines prévues par le CP et la LPD.

## Le prestataire doit choisir avec soin ses éventuels sous-traitants et les obliger à traiter de manière confidentielle les données soumises au secret professionnel auxquelles ils ont accès. Ces sous-traitants doivent en outre obliger par écrit leur personnel à garder le secret et l’informer des conséquences d’une violation de ces obligations. Ceci vaut par analogie pour tous les autres sous-traitants.

# Sous-traitance ultérieure

## Si, pour traiter des données personnelles, le prestataire recourt à des prestations de tiers qui traitent des données personnelles pour son compte (« sous-traitant »), il indique leurs nom, adresse et domaine d’activité ci-après.

|  |  |  |
| --- | --- | --- |
| **Nom/adresse** | **Domaine d’activité** | **Lieu du traitement des données** |
|  |  |  |
|  |  |  |

## Le recours éventuel à d’autres sous-traitants doit être communiqué par écrit au client. En l’absence d’opposition motivée par écrit dans un délai de 30 jours, le recours à ces tiers est considéré comme accepté.

# Obligations d’information et droits d’audit

## Le prestataire informe le client de manière exhaustive sur toutes les circonstances susceptibles de porter atteinte à la fourniture des prestations. En cas d’incidents relatifs à la sécurité et à la protection des données, il informe le client par écrit dès que possible, mais au plus tard dans les 72 heures à compter du moment où il a eu connaissance d’un incident dans une mesure suffisante. Il transmet immédiatement les informations qu’il n’aurait acquises qu’ultérieurement. Il assiste le client lors des travaux de préparation et met à disposition les documents auxquels il a accès. Il incombe ensuite au client de procéder aux dénonciations nécessaires auprès des autorités de protection des données, de poursuite pénale ou de surveillance. Ce dernier informe le prestataire de manière transparente de la procédure prévue.

## Le prestataire démontre avoir respecté les prescriptions en matière de protection des données par des moyens appropriés et fournit au client, à la demande de ce dernier, tous les renseignements requis. Le client peut contrôler le respect de ces obligations dans la mesure nécessaire. Si, dans un cas particulier, une inspection par une autorité de surveillance, par le client ou par un auditeur mandaté par celui-ci s’avère nécessaire, celle-ci a lieu aux heures de bureau après annonce appropriée et en tenant compte de la marche des affaires du prestataire. Le prestataire peut subordonner l’inspection à une déclaration de confidentialité concernant les données d’autres clients et les mesures techniques et organisationnelles mises en place, pour autant qu’aucune obligation de confidentialité sanctionnée pénalement ne s’applique. Il ne peut en aucun cas être fait appel à des concurrents du prestataire pour procéder au contrôle. Le client remboursera au prestataire les frais encourus dans une mesure appropriée.

# Responsabilité

## Dans leurs rapports externes, le prestataire et le client répondent conjointement à l’égard de la personne concernée du dommage causé par un traitement non conforme à la loi ou à la convention.

## Le prestataire ne répond que des dommages résultant d’un traitement qu’il a effectué et dans le cadre duquel il (a) n’a pas respecté ses obligations légales ou contractuelles, (b) a agi en méconnaissance des instructions licites données par le client ou (c) a agi à l’encontre des instructions licites du client.

## Si le client est tenu de verser des dommages-intérêts à la personne concernée, il se réserve le droit de se retourner contre le prestataire. Demeurent réservées les prétentions en responsabilité plus étendues prévues par les dispositions légales générales.

# Durée et effets du contrat

## La présente convention entre en vigueur à sa signature par les deux parties. Elle remplace toutes les conventions de même nature et prévaut en tous les cas sur toutes les autres conventions en cas de contradiction.

## Sa durée dépend de la durée du contrat principal, sauf disposition contraire de la présente convention de confidentialité. Elle reste en vigueur au moins aussi longtemps que le prestataire traite, peut traiter ou est tenu de traiter des données personnelles du client, à moins qu’elle ne soit remplacée par un autre contrat de traitement de données en sous-traitance valable répondant aux exigences légales.

## Le prestataire renonce par la présente à tout droit de rétention existant éventuellement sur les données personnelles faisant l’objet du contrat, quel qu’en soit le fondement juridique.

# Dispositions finales

## Le contrat et ses annexes régissent le contenu du contrat de manière exhaustive. Toute adaptation contractuelle requiert la forme écrite. La renonciation à cette exigence de forme doit revêtir la forme écrite. Cela peut parfois exclure toute modification contractuelle au moyen de « Shrink-Wrap Terms » ou de « Click-Wrap Terms ».

## Les droits et obligations découlant de la relation contractuelle ne peuvent être ni cédés, ni transférés, ni mis en gage sans l’accord écrit de l’autre partie.

## Si une ou plusieurs dispositions de la présente convention se révèlent nulles, cela n’affecte pas la validité des autres dispositions. En pareil cas, les parties adapteront la convention de telle manière à ce que le but poursuivi par la partie invalide soit atteint dans toute la mesure du possible.

# Droit applicable et for

La présente convention de traitement de données en sous-traitance est exclusivement soumise au droit suisse, à l’exclusion des règles internationales de conflit de lois et de la Convention des Nations Unies sur les contrats de vente internationale de marchandises. Le for exclusif est toujours au siège du client.

# Signatures

Pour le prestataire : Pour le client :

Lieu et date : Lieu et date :

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

Signature : Signature :

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

# Annexe 1

Pour garantir la **confidentialité**, le prestataire doit prendre des mesures afin que :

1. les personnes autorisées n’aient accès qu’aux données personnelles dont elles ont besoin pour accomplir leurs tâches (contrôle des autorisations) ;
Mesures adéquates :
2. seules les personnes autorisées aient accès aux locaux et aux installations où des données personnelles sont traitées (contrôle des accès) ;
Mesures adéquates :
3. les personnes non autorisées ne puissent pas utiliser les systèmes de traitement automatisé des données au moyen d’installations de transmission de données (contrôle des utilisateurs).
Mesures adéquates :

Pour garantir la **disponibilité** et l’**intégrité**, le prestataire doit prendre des mesures afin que :

1. des personnes non autorisées ne puissent pas lire, copier, modifier, déplacer, effacer ou détruire des supports de données (contrôle des supports de données) ;
Mesures appropriées :
2. des personnes non autorisées ne puissent pas enregistrer, lire, modifier, effacer ou détruire des données personnelles en mémoire (contrôle du stockage) ;
Mesures appropriées : \_\_\_
3. des personnes non autorisées ne puissent pas lire, copier, modifier, effacer ou détruire des données personnelles, en cas de divulgation de ces dernières ou lors du transport de supports de données (contrôle du transport) ;
Mesures appropriées :
4. la disponibilité des données personnelles et l’accès à celles-ci puissent être rapidement rétablis en cas d’incident physique ou technique (restauration) ;
Mesures appropriées :
5. toutes les fonctions du système de traitement automatisé de données soient disponibles (disponibilité), que les dysfonctionnements soient signalés (fiabilité) et que les données personnelles enregistrées ne puissent pas être endommagées par des dysfonctionnements du système (intégrité des données) ;
Mesures appropriées :
6. les systèmes d’exploitation et les logiciels d’application soient toujours maintenus au niveau de sécurité le plus récent et les lacunes critiques connues soient comblées (sécurité du système).
Mesures appropriées :

Pour garantir la **traçabilité**, le prestataire doit prendre des mesures afin de :

1. pouvoir vérifier quelles données personnelles sont saisies ou modifiées dans le système de traitement automatisé de données, à quel moment et par qui (contrôle des saisies) ;
Mesures appropriées :
2. pouvoir vérifier à qui des données personnelles sont communiquées à l’aide d’installations de transmission de données (contrôle des communications) ;
Mesures appropriées :
3. pouvoir détecter rapidement des violations de la sécurité des données (détection) et de prendre des mesures pour réduire ou éliminer les conséquences (élimination).
Mesures appropriées :