***Clauses contractuelles de sous-traitance (Annexe RGPD)***

***[Intitulé du Marché]***

**ENTRE**

**L’établissement:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Situé : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

N° SIRET : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

N° FINESS : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Représenté par: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

En sa qualité de: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

Ci-après, nommé le Responsable de Traitement »)

Et avec le Délégué à la Protection des Données désigné : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

D'une part,

**ET**

La société \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

Située \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

Inscrite au Registre du Commerce et des Sociétés de: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

SIRET: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

Représenté par: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

En sa qualité de: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

Et avec, s’il y a lieu, pour Délégué à la Protection des Données désigné : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

Ci-après, nommé « **Sous-traitant** »

D’autre part,

Dans le cadre de présente,

***Responsable de traitement*** Cliquez ici pour taper du texte. est qualifié de « responsable de traitement »

***Sous-traitant*** Cliquez ici pour taper du texte. est qualifié de sous-traitant.

# DEFINITIONS

**DPD ou DPO :** désigne le Délégué à la protection des Données, conformément à l’article 37 du RGPD

**Professionnel de Santé :** désigne toute personne en lien avec le parcours de soins incluant les personnels administratifs en charge de la venue du patient

**Données à Caractère Personnel :** désigne les informations qui concernent des personnes physiques, identifiées ou identifiables, directement ou indirectement, dont l’Acheteur est le Responsable du Traitement, et qui sont traitées par le Titulaire pour le compte du Client

**Données de santé à caractère personnel :** désigne les Données relatives à la santé physique ou mentale d’une personne physique, comprenant notamment les données produites à l’occasion des activités de prévention, de diagnostic, de soin ou de dispensation de médicaments par un Professionnel de santé et tout élément de nature à caractériser la santé d’une personne physique

**Traitement** : toute opération ou ensemble d’opérations effectuées ou non à l’aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l’enregistrement, l’organisation, la structuration, la conservation, l’adaptation ou la modification, l’extraction, la consultation, l’utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l’interconnexion, la limitation, l’effacement ou la destruction

**Responsable de Traitement :** désigne la personne physique ou morale, qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens des traitements de Données à Caractère Personnel

**Sous-Traitant :** la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte d’un responsable du traitement

**Violation de Données Personnelles** : toute destruction, perte, altération, divulgation ou un accès non autorisé à des Données à caractère personnel, de manière accidentelle ou illicite

**Autorité de contrôle :** désigne la Commission Nationale de l’Informatique et des Libertés (CNIL) ou toute autre autorité de contrôle compétente

**RGPD** : Règlement général sur la protection des données

# Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le Titulaire du marché, ci-après nommé « sous-traitant » s’engage à effectuer pour le compte de l’Acheteur, ci-après nommé « responsable de traitement » les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les parties s’engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « le règlement général sur la protection des Données »).

# Durée

Les présentes clauses prennent effet à compter de leur signature. Elles restent en vigueur pendant la durée du marché public.

# Description du traitement faisant l’objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) ***:*** Cliquez ici pour taper du texte.*description du service ou de la prestation*

La nature des opérations réalisées sur les données est Cliquez ici pour taper du texte. .

La ou les finalité(s) du traitement sont Cliquez ici pour taper du texte.

Les données à caractère personnel traitées sont concernant les patients : Cliquez ici pour taper du texte.

Les données à caractère personnel traitées sont concernant les professionnels participants à la prise en charge : Cliquez ici pour taper du texte. *identité, coordonnées, et établissements et service auquel ils sont affectés, etc.*

Les catégories de personnes concernées sont Cliquez ici pour taper du texte. le*s patients et les professionnels participant à la prise en charge, etc.*

*Exemple de tableau (s’appuyer sur la ou les fiche registre de traitement)*

*Ne conserver que les traitements faisant l’objet d’une sous-traitance et ajouter ceux qui ne figurent pas*

|  |  |  |  |
| --- | --- | --- | --- |
| **Finalité et Traitement** | **Catégories de DCP** | **Personnes concernées** | **Durées de conservation** |
| **Fourniture d’un accès à la Plateforme/logiciel (indiquer le nom)**  *(collecte des données du RT)* | Données d’identification  [à détailler] | [A compléter] | [A compléter] |
| **Administration des comptes et profil**  *(collecte, désactivation, mise à jour suppression)* | Données d’identification du professionnel  [à détailler]  Journaux : horodatage, identification de l’utilisateurs, actions réalisées [à détailler] | Professionnels utilisateurs du Service (détailler les profils) | [A compléter] Désactivation/suppression (à décrire)  Durée de conservation des logs (durée) |
| **Hébergement**  *Stockage des données pour le compte du RT* | [à détailler] | [A compléter] | [A compléter] |
| **Maintenance corrective et évolutive** | Toutes les catégories | Toutes les personnes concernées | [A compléter]  Lecture seule, si rapatriement indiquer la durée de conservation |
| **Support de niveau 1,2 et 3** | [A compléter] | [A compléter] | [A compléter] |
| **Fourniture d’un service de mail** |  |  |  |
| **SOUS-TRAITANT – INTERLOCUTEUR PRIVILEGIE** | | | |
| **Identité du sous-traitant** | [A compléter] | | |
| **Interlocuteur et Fonction** | Délégué à la protection des données | | |
| **Nom, prénom** | [A compléter] | | |
| **Coordonnées** | [A compléter] | | |
| **SOUS-TRAITANTS ULTERIEURS (second rang)** | | | |
| **Nom** | **Coordonnées** | **Activités sous-traité et DCP traitées** | **Date du contrat** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Obligations du sous-traitant vis-à-vis du responsable de traitement

## Généralités

Le sous-traitant s'engage à:

1. Traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l’objet de la sous-traitance
2. Traiter les données conformément aux instructions documentées du responsable de traitement. Si le sous-traitant considère qu’une instruction constitue une violation du RGPD ou de toute autre disposition du droit de l’Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement le responsable de traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l’Union ou du droit de l’Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public
3. Garantir la confidentialité des données à caractère personnel traitées, conformément à la réglementation applicable, et à ne fournir aucune information sur les finalités et les moyens du traitement à des tiers sans le consentement écrit préalable du responsable de traitement
4. Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu des présentes clauses:

* s’engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité
* reçoivent la formation nécessaire en matière de protection des données à caractère personnel

1. Prendre en compte, s’agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut

## Sous-traitance

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques (acheminement par voie postal des courriers notamment). Dans ce cas, il informe préalablement le responsable de traitement de tout changement envisagé concernant l’ajout ou le remplacement d’autres sous-traitants. Cette information peut être transmise au moyen d’une communication par courriel. Cette information doit indiquer clairement les activités de traitement sous-traitées, l’identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le responsable de traitement dispose d’un délai minimum de 30 jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations des présentes clauses pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s’assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences de la réglementation. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l’exécution par l’autre sous-traitant de ses obligations.

## Droit d’information des personnes concernées

*Choisir l’une des deux options :*

***Option A***

Il appartient au responsable de traitement de fournir l’information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

***Option B***

Le sous-traitant, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l’information relative aux traitements de données qu’il réalise. La formulation et le format de l’information doit être convenue avec le responsable de traitement avant la collecte de données.

## Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s’acquitter de son obligation de donner suite aux demandes d’exercice des droits des personnes concernées: droit d’accès, de rectification, d’effacement et d’opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l’objet d’une décision individuelle automatisée (y compris le profilage).

***Option A***

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d’exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à [...] (*indiquer un contact au sein du responsable de traitement*).

***Option B***

Le sous-traitant doit répondre, au nom et pour le compte du responsable de traitement et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d’exercice de leurs droits, s’agissant des données faisant l’objet de la sous-traitance prévue par le présent contrat.

## Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 48 heuresaprès en avoir pris connaissance et par le moyen suivant : *mail adressé au DPO du responsable de traitement.* Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l’autorité de contrôle compétente.

La notification contient au moins :

* La description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
* Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
* La description des conséquences probables de la violation de données à caractère personnel ;
* La description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n’est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord du responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique. La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel.

## Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations

Le sous-traitant aide le responsable de traitement pour la réalisation d’analyses d’impact relatives à la protection des données.

Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l’autorité de contrôle.

## Mesures de sécurité

Le sous-traitant s’engage à :

* mettre en œuvre et maintenir des mesures techniques et organisationnelles appropriées comprenant des traçabilités, afin de garantir un niveau de sécurité adapté au risque en préservant la confidentialité, l’intégrité et la sécurité des Données à Caractère Personnel, conformément à l’article 32 du RGPD ;
* Décrire les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, y compris, entre autres les moyens permettant de **garantir la confidentialité, l'intégrité, la disponibilité** et la résilience constantes des systèmes et des services de traitement;
* Apporter la preuve du respect des conformités exigées afin d’assurer la sécurité et la protection des données dans le cadre des projets soumis au cadre d’interopérabilité et de conformité de l’Agence du Numérique en Santé (ANS).

Le sous-traitant s’engage à mettre en œuvre les mesures de sécurité suivantes *à ajuster* et détailler par le sous-traitant :

* **La pseudonymisation et le chiffrement** des données à caractère personnel *(ex : https, mail sécurisé, accès VPN, etc)*
* ***L’hébergement*** *des données (ex : HDS si données sensibles)*
* ***Accès aux locaux******ou à l’application si télémaintenance*** *: badgés aux bâtiments et à certaines zones de bâtiments, Accès restreints au data center aux personnes habilités, et traçabilité de ces accès.*
* ***Sécurisation des postes de travail*** *(mdp individuel, verrouillage automatique etc)*
* ***Authentification forte****: mdp conforme aux recommandations de la CNIL, OTP…, Filtrage d’IP pour l’accès au service ;*
* ***Habilitation*** *restreinte, demande d’autorisation en cas de connexion, déconnexion obligatoire…et mise à jour*
* ***Traçabilité***
* ***Fourniture annuelle de nouvelles versions***
* Les moyens permettant **de rétablir la disponibilité** des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique; *ex****: sauvegarde logiciel****/applications et données sur deux sites physiques différents, PIA, plan de gestion des risques.*
* Les moyens de **détection des Violations de Données.** Une procédure visant **à tester, à analyser et à évaluer régulièrement l'efficacité** des mesures techniques et organisationnelles pour assurer la sécurité du traitement

Le Sous-traitant est en mesure d’apporter la preuve au Responsable de traitement, à tout moment, qu’il dispose de ces moyens organisationnels et techniques. Il informe régulièrement le Responsable de traitement des mises à jour de ces moyens et mesures.

## Sort des données

Au terme du Marché, le sous-traitant s’engage, selon le choix du responsable de traitement et sur instruction écrite de ce dernier :

* A détruire toutes les données à caractère personnel
* A renvoyer toutes les données à caractère personnel au responsable de traitement
* À renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement

Le renvoi doit s’accompagner de la destruction de toutes les copies existantes dans les systèmes d’information du sous-traitant. Une fois détruites, le sous-traitant fournit une attestation de destruction dans les trente (30) jours calendaires suivant l’échéance du Marché.

## Délégué à la protection des données

Le sous-traitant communique au responsable de traitement le nom et les coordonnées de son délégué à la protection des données, s’il en a désigné un conformément à l’article 37 du règlement général sur la protection des données.

## Registre des catégories d’activités de traitement

Le sous-traitant déclare tenir par écrit un registre de toutes les catégories d’activités de traitement effectuées pour le compte du responsable de traitement comprenant :

• le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données;

• les catégories de traitements effectués pour le compte du responsable du traitement;

• le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées; dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins:

* la pseudonymisation et le chiffrement des données à caractère personnel;
* des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
* des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
* une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement..

## AUDIT

Le sous-traitant met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

## RESPONSABILITE

Sous réserve de la réglementation en vigueur, en particulier l’article 28 du RGPD, la responsabilité du sous-traitant pourra être engagée en cas de manquement à ses obligations prévues au titre des présentes clauses.

# Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s’engage à :

1. Fournir au sous-traitant les données visées à l’article 4 des présentes clauses
2. Documenter par écrit toute instruction concernant le traitement des données par le sous-traitant
3. Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le RGPD de la part du sous-traitant
4. Superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant

# SIGNATURES

Fait à …………………………………….,

Le …./…./……..

En deux exemplaires originaux.

Chaque Partie déclarant en avoir reçu un exemplaire et avoir accepté les responsabilités chacun en ce qui le concerne.

|  |  |  |  |
| --- | --- | --- | --- |
| **L’ÉTABLISSEMENT** | | **LE PARTENAIRE** | |
| **NOM :** |  | **NOM :** |  |
| **Qualité :** |  | **Qualité :** |  |
| **Date :** |  | **Date :** |  |
| Signature + tampon | | Signature + tampon | |