





**CONTRAT DE SOUS-TRAITANCE DE DONNEES A CARACTERE PERSONNEL**

**Ght\_PRES\_2025-181 Audit Du Service Cardiologie**

***Notice explicative***

*L’article 28 du Règlement Général sur la Protection des Données (RGPD) impose aux Responsables de traitements de faire appel à des sous-traitants présentant des garanties suffisantes pour la protection des données à caractère personnel. Ce présent contrat permet le respect de cette obligation et établit les responsabilités de chacune des parties.*

*Dans le cadre des marchés publics et au sens du RGPD, le « responsable du traitement » est en principe l’acheteur public. Le terme « sous-traitant », qui désigne au sens du RGPD « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement », correspond en marché public au titulaire du contrat, ainsi qu’à tout sous-traitant (au sens commande publique) à qui il serait confié le traitement de données.* [*https://www.justifit.fr/b/guides/rgpd/*](https://www.justifit.fr/b/guides/rgpd/)

***Si vous ne collectez que des données relatives à l’exécution contractuelle (coordonnées agents) ou si vous agissez en tant que Responsable de traitements, vous n’êtes pas concernés par ce contrat. Dans ce cas, veuillez l’indiquer. Le cas échéant, aucune autre donnée ne vous sera transferée.***

Conformément à la réglementation en vigueur et au regard des traitements mis en œuvre dans le cadre du marché, le CHU de Saint-Etienne, en tant qu’établissement support du GHT Loire, agit en tant que Responsable de Traitement et le(s) titulaire(s) en tant que Sous-Traitant au sens du Règlement Général sur la Protection des Données à caractère personnel (RGPD), individuellement dénommées « Partie » et ensemble dénommées « Parties ».

**Il a été exposé préalablement ce qui suit :**

**EXPOSE PREALABLE**

Le présent contrat définit les engagements des Parties concernant la protection de la vie privée et des droits fondamentaux des personnes lors de l’accès ou de l’utilisation par le(s) titulaire(s), dans le cadre de l’exécution de sa mission, des données à caractère personnel qui sont sous la responsabilité du Responsable de Traitement (le CHU Saint-Etienne).

**Ceci exposé, les Parties conviennent et arrêtent ce qui suit :**

**1. Définitions**

Au sens des présentes clauses du contrat :

a) « données à caractère personnel », « catégories particulières de données », « traiter/traitement », « responsable du traitement », « sous-traitant », « personne concernée », « destinataire », « tiers », « fichier » ont la même signification que dans 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.

b) le « Responsable de Traitement » désigne l’entité pour le compte de laquelle des données à caractère personnel sont traitées. En l’espèce le CHU de Saint-Etienne.

c) le « Sous-Traitant » désigne l’organisme, le titulaire du marché public, qui traite pour le compte et sous instructions du Responsable de Traitement, des données à caractère personnel.

d) le « Contrat » désigne le contrat de prestation qui lie le Responsable de Traitement et le Sous-Traitant et qui porte sur le(s) traitement(s) des données à caractère personnel pour le compte du Responsable de Traitement.

d) le « tiers autorisé » désigne un organisme qui peut accéder à certaines données contenues dans des fichiers publics ou privés parce qu'une loi l'y autorise expressément.

**2. Objet**

Le titulaire du marché assure, pour le compte de son client, le CHU Saint-Etienne, les opérations décrites dans le présent contrat de sous-traitance.

En tant que Responsable de traitement, le CHU de Saint-Etienne est tenu de faire uniquement appel à des titulaires de marché qui présentent des **garanties suffisantes** quant à la mise en œuvre des règles de sécurité et de confidentialité et de s’assurer, notamment par voie contractuelle, que des mesures adéquates ont été prises par les sous-traitants (le titulaire du marché) afin que le traitement réponde aux exigences règlementaires en matière de protection de données à caractère personnel.

En vue de la réalisation des prestations, le Sous-traitant (le titulaire du marché) pourrait être amené à prendre connaissance, que ce soit de manière fortuite ou suite à communication de la part du Responsable de traitement (CHU Saint-Etienne), d’informations et notamment de données nominatives dont le traitement est soumis à la mise en œuvre des mesures techniques et organisationnelles appropriées et effectives en vertu de la **loi 78-17 du 6 janvier 1978** modifiée relative à l'informatique, aux fichiers et aux libertés et, à compter du 25 mai 2018, du Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des données à caractère personnel (**RGPD**), ci-après dénommé le « Règlement ».

Le présent engagement s’applique à toutes les données à caractère personnel :

* Transmises par le Responsable de traitement au Sous-traitant dans le cadre de la mission effectuée pour le compte du Responsable de traitement ;
* Accessibles au Sous-traitant dans le cadre de la mission effectuée pour le compte du Responsable de traitement ;
* Reçues par le Sous-traitant d’un tiers dans le cadre de la mission effectuée pour le compte du Responsable de traitement.

**3. Description du traitement**

1. **Finalités (objectifs poursuivis par le traitement)**

Dans le cadre de la mission effectuée pour le compte du CHU Saint-Etienne, le titulaire du marché est amené à effectuer un traitement des données à caractère personnel conformément aux finalités prévues, à savoir :

[Préciser les finalités du traitement de données à caractère personnel/profesionnel mis en œuvre, cocher les cases :]

*Paiement des factures*  *gestion administrative*  *organisation pour l’exécution du marché public*  *planification des interventions sur site*  *S.A.V*  *rédaction de rapports*

Autre, à préciser :

1. **Nature des opérations**

La nature des opérations réalisées par le Sous-traitant sur les données à caractère personnel est :

Collecte  Enregistrement  Hébergement  Stockage  Adaptation  Modification

Consultation Extraction

Communication par transmission ou diffusion ou toute autre forme de mise à disposition

Autre à préciser :

1. **Données concernées**

Les données à caractère personnel/professionnel faisant l’objet d’un traitement dans le cadre de la mission effectuée pour le compte du Responsable de traitement sont les suivantes :

[Préciser de manière exhaustive les données personnelles/profesionnelles concernées, cocher les cases :]

Données d’identification (préciser lesquelles ; *exemple : nom/prénom, , coordonnées téléphoniques et électroniques etc.*)

Données de santé (préciser lesquelles ; *exemple : matricule, âge, antécédents médicaux, imagerie médicale, IMC etc.*)

Données économiques/financières (préciser lesquelles ; *exemple : RIB, revenus/salaire, avis d’imposition etc.*)

Données de connexion (préciser lesquelles ; *exemple : adresse IP, date et heure de connexion etc.*)

Données de situation familiale (préciser lesquelles ; *exemple : célibataire, marié, pacsé, veuve/veuf, enfants etc.*)

Autre à préciser :

1. **Catégories de personnes concernées**

Les catégories de personnes concernées par le traitement sont les suivantes :

Données patient  Données des professionnels du CHU St Etienne

Autre à préciser :

1. **Personnes ayant accès aux données**

Les personnes ayant accès aux données sont les suivantes :

[Indiquer les services/départements/sous-traitants ultérieurs pouvant accéder aux données]

1. **Mesures de sécurité mises en place par le Sous-traitant**

Les mesures de sécurité mises en place par le Sous-traitant sont les suivantes :

[Lister les mesures techniques et organisationnelles mises en place par le Sous-traitant afin de sécuriser les données]

*Exemples : désignature d’un DPO, mesures de cyber-sécurité, formations, mots de passe complexes, serveur sécurisés, etc.*

**4. Obligations à la charge du Sous-Traitant (le titulaire du marché)**

Les informations mises à disposition du Sous-traitant ou accessibles par le Sous-traitant ne peuvent faire l’objet d’une opération de traitement que sur **instruction documentée** du Responsable de traitement. Ainsi, ces informations **ne peuvent faire l’objet d’un traitement ne correspondant pas aux finalités susvisées**.

Le Sous-traitant s’engage à considérer comme confidentielles et entrant dans le champ d’application du secret professionnel auquel il est tenu, les informations de toute nature, écrites ou orales, qu’il serait amené à connaître durant l’exécution du contrat. L’**obligation de confidentialité** du Sous-traitant continuera après expiration des présentes, aussi longtemps que lesdites informations n’auront pas été rendues publiques par le Responsable de traitement. Pour ces motifs, le Sous-traitant fait signer une clause de confidentialité par toutes les personnes l’assistant dans l’exécution du contrat.

Le Sous-traitant met en œuvre les **mesures techniques et organisationnelles** appropriées liées à la sécurité avant de traiter les données à caractère personnel qui lui sont confiées et use de tous les moyens nécessaires, eu égard aux risques liés au traitement, à la nature des données à protéger et au coût de mise en œuvre, afin de protéger les données à caractère personnel contre toute perte fortuite, altération, divulgation à des **tiers non autorisés ou accès non autorisé** aux données précitées. Les mesures de sécurité mises en œuvre sont les suivantes :

*Description des mesures de sécurité techniques et organisationnelles mises en œuvre par le ou les sous-traitants (y compris toute certification pertinente) visant à garantir un niveau de sécurité approprié, compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des risques pour les droits et libertés des personnes physiques. Mesures possibles :*

Mesures de pseudonymisation et de chiffrement des données à caractère personnel;

Mesures visant à garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

Mesures assurant de disposer de 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;

Procédures visant à tester, à analyser et à évaluer régulièrement l’efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement;

Mesures d’identification et d’autorisation de l’utilisateur;

Mesures de protection des données pendant la transmission;

Mesures de protection des données pendant le stockage;

Mesures visant à garantir la sécurité physique des sites où les données à caractère personnel sont traitées;

Mesures visant à garantir l’enregistrement des événements;

Autre à préciser :

Le Sous-traitant s’engage à traiter rapidement et comme il se doit toute **demande d’informations du Responsable de traitement**, permettant de garantir le respect et l’effectivité des obligations de sécurité et de confidentialité résultant du contrat. Il s’oblige à ce que ces informations soient mises à jour régulièrement ou sur demande du Responsable de traitement.

Le Sous-traitant traite les données à caractère personnel **pour le compte exclusif du Responsable de traitement**, conformément aux instructions de ce dernier et aux présentes clauses. S’il est dans l’incapacité de s’y conformer pour quelque raison que ce soit, il accepte d’informer dans les meilleurs délais le Responsable de traitement de son incapacité.

Le Sous-traitant prend 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**.

Le Sous-traitant tient un **registre de toutes les catégories d’activités de traitement** effectuées pour le compte du Responsable de traitement et s’engage à coopérer avec l’autorité de contrôle compétente. Sur sa demande, il met à sa disposition le registre précité.

Le Sous-traitant s’engage à obtenir l’accord écrit du Responsable de traitement avant tout **transfert de données à caractère personnel vers un pays tiers** situé hors de l’Union Européenne et à respecter les obligations légales et réglementaires incombant à tout transfert effectué hors de l’Union Européenne. En cas d’accord exprès du CHU, le sous-traitant prendra des mesures afin d’assurer une protection adéquate des données envoyées hors de l’Espace Economique Européen et l’ensemble des transferts sera couvert par un mécanisme de transfert approuvé par les autorités de l’Union Européenne.

Le Sous-traitant communique dans les meilleurs délais et avec une célérité permettant au Responsable de traitement de s’acquitter de ses obligations légales toute demande contraignante de transmission de données à caractère personnel **émanant d’un tiers autorisé** sauf disposition contraire, telle qu’une interdiction de caractère pénal visant à préserver le secret d’une enquête policière.

En cas de **violation de données à caractère personnel** entraînant, de manière accidentelle ou illicite, l'accès ou divulgation non autorisé, la destruction, la perte, l'altération de données à caractère personnel transmises, conservées ou traitées d'une autre manière, le Sous-traitant s’engage à prendre toutes les mesures nécessaires pour atténuer tout risque immédiat et potentiel pour les personnes concernées et notifie **dans les plus brefs délais** la violation de données au Responsable de traitement. La notification doit décrire la nature de la violation, ses conséquences probables, les mesures prises par le Sous-traitant et tout élément permettant au Responsable de traitement de prendre des mesures proportionnées au risque identifié.

Le Sous-traitant met à la disposition du Responsable de traitement la **documentation nécessaire pour démontrer le respect de toutes ses obligations** et permettre la réalisation d’audits par le Responsable de traitement ou un autre auditeur. Le cas échéant, le Sous-traitant assiste le Responsable de traitement dans la réalisation des analyses d’impact relatifs à la mise en œuvre du/des traitement(s) concerné(s). À la demande du CHU, et conformément à l’article 28 du règlement européen sur la protection des données, le titulaire fournira au Client les informations raisonnablement exigibles et pertinentes démontrant sa conformité quant aux obligations lui incombant au titre du présent contrat. Ces informations permettront 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. Le responsable de traitement peut auditer, dans la limite d’une fois par an, la conformité du sous-traitant en cas de doute raisonnable relatif à un quelconque manquement à la présente clause. L’audit devra être réalisé au cours des heures normales d'ouverture sur le site concerné, il sera soumis aux règles internes du titulaire, et il ne devra pas perturber de manière excessive les activités de celui-ci. Les rapports d’audit sont considérés comme des informations confidentielles des Parties. Tous les frais associés aux audits sont à la charge du pouvoir adjudicateur.

Le Sous-Traitant fournira au délégué à la protection des données tous les éléments nécessaires à l'enregistrement des traitements dans le registre des traitements. Ces informations sont donc au minimum les suivantes : *identification des services opérationnels traitant les données, identification des catégories de données traitées, lieu où sont hébergées les données, durées de conservation des données, liste des mesures mises en œuvre pour minimiser les risques.*

**5. Obligations du Responsable de Traitement (le CHU Saint-Etienne)**

Le Responsable de traitement s’engage à :

* Fournir au Sous-traitant les données nécessaires à la réalisation de la prestation ;
* Documenter par écrit toute instruction concernant le traitement des données par le Sous-traitant et veille à respecter un délai raisonnable pour toute instruction complémentaire en vue de l’application des instructions ;
* Veiller au respect des obligations prévues par le Règlement de la part du Sous-traitant ;
* Superviser le traitement, y compris réaliser les audits et les inspections auprès du Sous-traitant.

**6. Obligations des parties**

Les Parties déclarent être en conformité avec les dispositions légales et réglementaires relatives à la protection des données à caractère personnel, et notamment le Règlement (UE) n° 2016/679.

De façon générale, les Parties s’engagent à coopérer afin de garantir le respect des dispositions légales et réglementaires relatives à la protection des données.

**7. Sous-traitance ultérieure**

Le(s) titulaire(s) ne peut(vent) faire appel à un sous-traitant pour mener des activités de traitement sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le(s) titulaire(s) informe(nt) le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'un sous-traitant, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

Cette information doit indiquer clairement les activités de traitement sous-traitées, l’identité et les coordonnées du sous-traitant ultérieur ainsi que les dates du contrat de sous-traitance. **Si le Responsable de traitement émet des objections, cette sous-traitance ne peut être effectuée.**

Le sous-traitant ultérieur est tenu de respecter les obligations décrites dans le présent document. Le Sous-traitant s’y assure au moyen d’un contrat qui impose au sous-traitant ultérieur les mêmes obligations en matière de protection des données que celles imposées au Sous-traitant en vertu des présentes clauses. À la demande du Responsable du traitement, le Sous-traitant lui fournit une copie de ce contrat conclu avec le sous-traitant ultérieur et de toute modification qui y est apportée ultérieurement.

Il appartient au Sous-traitant de s’assurer que le sous-traitant ultérieur présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du Règlement. **Le Sous-traitant demeure pleinement responsable devant le Responsable de traitement du défaut de conformité du sous-traitant ultérieur**.

**8. Informations et droits des personnes concernées**

Les personnes concernées désignent les personnes dont les données à caractère personnel sont traitées dans le cadre du présent marché.

1. **Information des personnes concernées**

Le Responsable de traitement, au moment de la collecte des données, fournit aux personnes concernées par les opérations de traitement l’information relative aux traitements de données qu’il réalise.

1. **Droits des personnes concernées**

Dans la mesure du possible, le Sous-traitant vient en aide au Responsable de traitement afin que ce dernier s’acquitte de son obligation de donner suite aux demandes d’exercice des droits des personnes concernées.

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 au Responsable de traitement. Le(s) titulaire(s) fournira(ont) donc à ce sujet, au délégué à la protection des données (DPD), les procédures permettant d'exercer les droits (dans un délai maximum de 2 mois) après la signature du contrat. Il doit aider le responsable du traitement à s’acquitter de son obligation de donner suite aux demandes d’exercice des droits des personnes concernées. Lorsque les personnes concernées exercent auprès du titulaire des demandes d’exercice de leurs droits, il doit adresser ces demandes dès réception et sans délai par courrier électronique au délégué à la protection des données du responsable du traitement à l’adresse [rgpd-dpd@chu-st-etienne.fr](mailto:rgpd-dpd@chu-st-etienne.fr).

**9. Responsabilité**

Le Sous-traitant reconnaît qu’en cas de non-respect des obligations susvisées :

* Sa responsabilité est susceptible d’être engagée sur la base des articles 226-13 et 226-17 du Code pénal ;
* Il sera tenu responsable envers le Responsable de traitement des conséquences dommageables causées par ce manquement, ainsi qu’au versement de réparations pour le préjudice subi ;
* Que le Responsable de traitement pourra prononcer la résiliation immédiate du contrat, sans indemnité à l’égard du Sous-traitant.

**10. Délégué à la protection des données**

Les Parties ont désigné des Délégués à la Protection de Données (Data protection Officer – DPO) qui seront les interlocuteurs privilégiés pour l’ensemble des process relatifs à la protection des données.

Les coordonnées des DPO sont les suivantes :

DPO du CHU de Saint-Etienne

* [rgpd-dpd@chu-st-etienne.fr](mailto:rgpd-dpd@chu-st-etienne.fr)

**11. Autres dispositions**

La clause de sous-traitance ne pourra faire l’objet d’aucune modification, cession, apport ou transfert, sous quelque forme que ce soit, notamment au profit d’un sous-traitant ultérieur, sauf à ce que ce dernier agisse sous la responsabilité et le contrôle du Sous-traitant, dans le cadre d’un contrat soumis à la validation préalable du Responsable de traitement et permettant d’assurer le respect des obligations souscrites par le Sous-traitant.

Les clauses sont régies par le droit français. Les dispositions du contrat initial concernant la juridiction compétente s’appliquent.

Les Parties conviennent qu’au terme des services de traitement de données, le Sous-traitant restituera au Responsable de traitement, et à la convenance de celui-ci, l’ensemble des données à caractère personnel transférées, ainsi que les copies, ou détruira l’ensemble de ces données et en apportera la preuve au Responsable de traitement, à moins que la législation imposée au Sous-traitant ne l’empêche de restituer ou de détruire la totalité ou une partie des données à caractère personnel transférées. Dans ce cas, le Sous-traitant garantit qu’il assurera la confidentialité des données à caractère personnel transférées et qu’il ne traitera plus activement les dites données pendant la durée de cette obligation légale, durée après laquelle les données sont détruites ou restituées au Responsable de traitement dans les mêmes conditions que celles décrites ci- dessus.

|  |  |
| --- | --- |
| Date | Signature du candidat |