

|  |
| --- |
| Règlement Général de la Protection des Données |
| Clause relative à la protection des données à destination des marchés impliquant un traitement des données personnelles  Responsable de traitement – Sous-traitant |
| **Direction des Affaires Juridiques** |
| Version document : 22/12/2021 |

CLAUSE DE PROTECTION DES DONNÉES

RESPONSABLE DE TRAITEMENT – SOUS TRAITANT

**ENTRE**

**[Nom de la société]**

[Type de société] au capital social de [montant du CS] euros

Dont le siège social se situe [Adresse siège social]

Enregistrée au Registre du Commerce et des Sociétés de [Ville] sous le numéro : [XXX XXX XXX]

Représentée par [Nom du Dirigeant].

Agissant en qualité de sous-traitant et de fournisseur de produits et services

Ci-après désigné par«**XXX** » ou « le titulaire »,

D’une part

**ET**

**LE CENTRE HOSPITALIER UNIVERSITAIRE DE ROUEN,**

Etablissement Public de Santé

Dont le siège social se trouve 1, Rue de Germont – 76031 Rouen cedex

Représenté par Madame Véronique Desjardins, Directrice Générale.

Agissant en qualité de Responsable de traitement et de Client ;

Ci-après désigné par « le CHU de Rouen » ou « l’acheteur »,

D’autre part

**Nom de la société** et **le CHU de Rouen** sont individuellement désignés par la « Partie » et conjointement désignés par les « Parties ».

Préambule

Les présentes clauses trouvent à s’appliquer pour tout traitement de données à caractère personnel par un sous-traitant (le titulaire) pour le compte du responsable du traitement (CHU de Rouen) dans le cadre d’un marché public.

On entend par :

- **Données à caractère personnel** : toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement.

- **Personne physique identifiable** : une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

- **Traitement** : toute opération ou tout ensemble d'opérations effectuées à l'aide de procédés automatisés ou non et appliqué 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 du traitement** : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

- **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 du responsable du traitement.

Tout partenaire du CHU de Rouen entrant dans le champ d’application des présentes définitions est ainsi amené à se voir appliquer les clauses suivantes. Ceci inclut *de facto* les opérations de maintenance effectuées par des tiers pour le compte du CHU de Rouen le mainteneur étant amené à réaliser un traitement de données à caractère personnel au sens des précédentes définitions.

1. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le titulaire, sous-traitant au sens de l’article 28 du Règlement européen sur la protection des données (ci-après, « le règlement européen sur la protection des données »), s’engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies dans le cadre de l’objet principal du contrat.

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 européen sur la protection des données »)et les règles subsidiaires du droit national français.

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

Le client, en qualité de Responsable de traitement, détient seul et de manière exclusive le pouvoir de déterminer les finalités et les moyens du traitement de données.

Le sous-traitant est autorisé à traiter pour le compte du Responsable de Traitement les données à caractère personnel nécessaires pour fournir le(s) service(s) attendus, objet du présent marché.

Le traitement, dont certaines opérations sont confiées au titulaire, possède les caractéristiques définies en annexe.

1. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le titulaire 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.

Le titulaire s’engage en outre à ne pas utiliser les données à des fins autres que celles visées dans ce présent marché

1. Traiter les données conformément aux instructions documentées du CHU de Rouen. Si le titulaire considère qu’une instruction constitue une violation du règlement européen sur la protection des données 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.
2. Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent marché et s’engager à ne pas les divulguer à un tiers

A ce titre, toute donnée dont le titulaire a connaissance à l’occasion de l’exécution du présent marché est strictement couverte par le secret professionnel en application de l’article 226-13 du Code pénal.

Ne constituent pas des informations confidentielles les informations qui :

• Sont déjà connues du titulaire qui les reçoit préalablement à la date de leur divulgation par le CHU de Rouen.

• Sont disponibles dans le domaine public lors de leur divulgation ou tombent ultérieurement dans le domaine public, sans manquement aux stipulations du marché.

• Sont communiquées par un tiers à titre non confidentiel au titulaire, dès lors que ce tiers n'est pas lié à l'autre partie par une quelconque obligation de confidentialité.

• Sont développées de manière indépendante par le titulaire qui les reçoit, en dehors de tout manquement aux stipulations au marché.

1. Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent marché :

* 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
2. Sécurité

Le titulaire s’engage à respecter la sécurité et la confidentialité des données et des accès informatiques du CHU de Rouen conformément aux lois et régimes applicables, et notamment conformément à la règlementation relative à la protection des données, et aux dispositions du Code pénal en vigueur.

A ce titre, le titulaire s’engage :

* A ne pas divulguer à des tiers, à titre gratuit ou onéreux, et sous quelque forme que ce soit, les informations et documents communiqués par le CHU de Rouen à l’occasion de l’exécution du marché ;
* A prendre toutes les mesures pour que lesdites données ne puissent être accessibles à d’autres personnes que les personnels attachés à leur traitement et à leur analyse. Ces derniers seront sensibilisés au caractère stratégique des informations et documents confiés et liés au titulaire par un engagement de confidentialité ;
* A ne pas procéder à des copies, utilisations ou diffusion de partie ou totalité d’un fichier et/ou d’une donnée, détenus par le CHU de Rouen à l’exception des copies, utilisations ou diffusion nécessaires à l’exécution d’une prestation prévue au marché, auquel cas l’accord préalable et explicite du CHU de Rouen est nécessaire ;
* A ne pas sortir des locaux du CHU de Rouen des configurations, des supports numériques ou d’autres, d’éléments ou sous-ensembles d’une configuration, d’un matériel, ou d’une documentation, détenus par le CHU de Rouen sans l’autorisation préalable et écrite de celui-ci ;
* A informer le CHU de Rouen de toute réception par lui d’une mise en demeure, réquisition ou requête judiciaire, de toute enquête ou toute autre notification relative à la réalisation des prestations ;
* A assurer le chiffrement des informations présentes sur ses équipements utilisés ou transportés hors de ses locaux, comportant des informations nominatives, avec un logiciel de chiffrement à l’état de l’art.

Le titulaire est responsable vis-à-vis du CHU de Rouen de la perte de documents remis sous quelque forme que ce soit, ou de la divulgation volontaire ou involontaire d’informations communiquées.

En cas de non-respect des dispositions précitées, la responsabilité du titulaire peut également être engagée sur la base des dispositions des articles 226-5 et 226-17 du code pénal.

Au cas où le titulaire serait en position d’accéder à des données nominatives de santé, il est rappelé que les dispositions juridiques en vigueur imposent pour l’accès à ces données d’un moyen d’authentification forte validé par l’Agence du Numérique en Santé (Cf. : PGSSI-S : Politique générale de sécurité des systèmes d’information de santé - Référentiel d’authentification des acteurs de santé).

En particulier, le titulaire devra porter un soin particulier à l’accès à ces données nominatives de santé lors d’opérations de télémaintenance. Le titulaire devra prendre toutes les dispositions nécessaires pour qu’en aucun cas les données nominatives de santé ne soient transférées en dehors du système d’information du CHU de Rouen.

Le titulaire s’engage à mettre en œuvre les mesures de sécurité prévues aux clauses contractuelles particulières et à respecter strictement les dispositions décrites dans la Politique de Sécurité du Système d’Information du CHU de Rouen annexée au présent marché (Cf : Clauses de Sécurité, de Protection des données personnelles et de Confidentialité).

1. 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 de données à caractère personnel spécifiques. Dans ce cas, il informe préalablement et par écrit le CHU de Rouen de tout changement envisagé concernant l’ajout ou le remplacement d’autres sous-traitants. 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 CHU de Rouen, responsable de traitement, dispose d’un délai conforme à la règlementation de la commande publique ou de 2 mois pour tous les autres types de contrat 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 mêmes obligations demandées au titulaire et exposées au présent marché pour le compte et selon les instructions du CHU de Rouen.

Il appartient au titulaire 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 du règlement européen sur la protection des données.

Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le titulaire demeure pleinement responsable devant le CHU de Rouen de l’exécution par le sous-traitant ultérieur de ses obligations.

1. Transfert de données à caractère personnel hors UE

Le titulaire s’engage à ce que les données à caractère personnel dont le traitement lui est confié dans le cadre du présent marché ne soient pas transférées en dehors de l’Union Européenne sauf avec l’accord exprès, écrit et préalable du CHU de Rouen et sous réserve de prévoir l’encadrement juridique et matériel approprié (l’existence d’une décision d’adéquation de la Commission Européenne,  la mise en place de clauses contractuelles types,  l’existence de BCR,  les exceptions au principe d’interdiction d’un transfert hors UE).

1. Droit d’information des personnes concernées

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. Le titulaire s’engage à transmettre préalablement tous les éléments relatifs aux opérations de traitements nécessaires à cette information.

1. Exercice des droits des personnes

Dans la mesure du possible, le titulaire doit aider le responsable de traitement à s’acquitter de son obligation de donner suite aux demandes d’exercice des droits des personnes concernées et fournir tous les moyens nécessaires à la gestion de ces demandes : 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).

Lorsque les personnes concernées exercent auprès du titulaire des demandes d’exercice de leurs droits, le titulaire doit adresser ces demandes dès réception par courrier électronique à l’adresse email : [dpd@chu-rouen.fr](mailto:dpd@chu-rouen.fr).

1. Notification des violations de données à caractère personnel

Le titulaire s’engage à aviser le CHU de Rouen de toute disparition, ainsi que de tout incident de sécurité et de toute violation de données à caractère personnel qu’il aurait constaté dans un délai maximum de 48 heures après en avoir pris connaissance par écrit électronique à l’adresse email : [dpd@chu-rouen.fr](mailto:dpd@chu-rouen.fr).

Cette notification doit être accompagnée de toute documentation utile afin de permettre au CHU de Rouen, si nécessaire, de notifier l’incident ou la violation de données aux autorités compétentes voire aux personnes concernées.

Les données à communiquer seront les suivantes : la nature de la violation de données à caractère personnel, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données ainsi que les mesures prises pour atténuer les effets préjudiciables de la violation.

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

Le titulaire aide le responsable de traitement pour la réalisation d’analyses d’impact relative à la protection des données en fournissant tous les éléments relatifs à la sécurité et aux conditions d’utilisation des données à caractère personnel traités pour le compte du CHU de Rouen.

Le cas échéant, le titulaire aide le responsable de traitement pour la réalisation de la consultation préalable de l’autorité de contrôle en fournissant au CHU de Rouen tous les éléments relatifs à la sécurité et aux conditions d’utilisation des données à caractère personnel traités pour le compte du CHU de Rouen.

Le titulaire s’engage à fournir les éléments nécessaires à l’homologation de sécurité (intervenant au plus tard en phase de Vérification d’Aptitude (VA)) des téléservices entrant dans le champ de l’ordonnance 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives (Cf. Décret 2010-112 du 2 février 2010 et l’arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité) et à procéder le cas échéant aux adaptations nécessaires pour s’y conformer.

1. Délégué à la protection des données

Le titulaire 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 européen sur la protection des données. Le CHU de Rouen en fait de même.

|  |  |
| --- | --- |
| **Délégué à la Protection des Données (DPO)**  **du CHU de Rouen :**  Nom : PRETERRE  Prénom : Séverine   : dpd@chu-rouen.fr   : 02.32.88.05.86 | **Délégué à la Protection des Données (DPO)**  **du titulaire :**  Nom : Cliquez ou appuyez ici pour entrer du texte.  Prénom : Cliquez ou appuyez ici pour entrer du texte.   : Cliquez ou appuyez ici pour entrer du texte.   : Cliquez ou appuyez ici pour entrer du texte.  Le titulaire déclare ne pas avoir nommé de DPO à ce jour et ce sous son entière responsabilité. |

1. Registre des catégories d’activités de traitement

Le titulaire déclare tenir par écrit un registre de toutes les catégories d’activités de traitement effectuées pour le compte du CHU de Rouen conformément aux obligations prévues par le règlement européen sur la protection des données et qu’il tient à la disposition du CHU de Rouen.

1. Audits et contrôles

Sous réserve d’un préavis de quinze (15) jours ouvrés incluant notamment l’objet de sa mission et la durée envisagée, le CHU de Rouen se réserve le droit, à ses frais, de procéder à toute vérification qui lui paraîtrait utile pour constater le respect par le titulaire de ses obligations au titre du marché, notamment par le biais d’un audit ou d’une inspection de contrôle.

Le titulaire s’engage à répondre aux demandes d’audit et de contrôle du CHU de Rouen et effectuées par le CHU de Rouen lui-même ou par un tiers de confiance qu’il aura sélectionné, reconnu en tant qu’auditeur indépendant, c'est-à-dire indépendant du titulaire, ayant une qualification adéquate, et libre de fournir les détails de ses remarques et conclusion d’audit au CHU de Rouen.

Les audits doivent permettre une analyse du respect du présent marché et des dispositions relatives à la protection des données à caractère personnel, notamment : par la vérification de l’ensemble des mesures de sécurité mises en œuvre par le titulaire, par la vérification des journaux de localisation des données, de copie et de suppression des données, par l’analyse des mesures mises en place pour supprimer les données, pour prévenir toutes transmissions illégales de données à des juridictions non adéquates ou pour empêcher le transfert de données vers un pays non autorisé. L’audit doit enfin pouvoir permettre de s’assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées sans que cela ne soit détecté et notifié.

A ce titre, le titulaire met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations.

Il est entendu entre les parties que les demandes d’information, les opérations d’audit et d’inspections devront être effectuées pendant les heures normales d’ouverture du titulaire et ne devront pas perturber le bon fonctionnement des activités de ce dernier.

Il est également entendu qu’un tel audit ou toute autre forme de contrôle/vérification ne peut en aucun cas porter sur les documents financiers et/ou comptables du titulaire ou sur les documents relatifs aux membres du personnel du titulaire (sauf accord préalable et éclairé de ces derniers). Le CHU de Rouen s'engage à respecter les obligations de confidentialité qui lui incombent au titre des présentes ainsi que les règles d'accès et de sécurité en vigueur dans les locaux du titulaire et se porte fort du respect de ces règles par les membres de son personnel et/ou auditeur externe.

Un exemplaire du rapport d’audit sera remis gracieusement au titulaire. Les parties examineront de bonne foi ce rapport et identifieront, le cas échéant, les actions qui devront être engagées par l’un ou l’autre des parties.

1. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s’engage à :

1. Documenter par écrit toute instruction concernant le traitement des données par le titulaire
2. Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du titulaire
3. Superviser le traitement, y compris réaliser les audits et les inspections auprès du titulaire
4. Sort des données

Au terme de la prestation de services impliquant le traitement des données à caractère personnel pour le compte du CHU de Rouen, le titulaire s’engage à :

* [option A]  détruire toutes les données à caractère personnel ou
* [option B]  à renvoyer toutes les données à caractère personnel au responsable de traitement ou
* [option C]  à renvoyer les données à caractère personnel au titulaire désigné par le responsable de traitement

Le renvoi doit s’accompagner de la destruction immédiate de toutes les copies existantes dans les systèmes d’information du titulaire. Une fois détruites, le titulaire doit justifier par écrit auprès du CHU de Rouen de la destruction.

**Les parties paraphent toutes les pages et signent ce document**

Fait en deux exemplaires originaux, à Rouen, le Cliquez ou appuyez ici pour entrer une date.

|  |  |
| --- | --- |
| **Pour le CHU de Rouen**  **Madame Stéphanie DECOOPMAN** | **Pour** Cliquez ou appuyez ici pour entrer du texte.  **Monsieur/Madame** Cliquez ou appuyez ici pour entrer du texte. |
| Directrice Générale | Cliquez ou appuyez ici pour entrer du texte. |
|  |  |

Annexe : Descriptif du traitement des données à caractère personnel et liste des sous-traitants :

1. **Description du traitement confié au titulaire comportant les caractéristiques suivantes :**

|  |  |
| --- | --- |
| Service(s) fourni(s) | Hébergement  Maintenance  Formation  Service de « Hotline »  Autre (à préciser) : […] |
| Durée du traitement | Durée du présent contrat  Autre (à préciser) : […] |
| Nature des opérations réalisées sur les données | Collecte  Enregistrement  Organisation  Structuration  Conservation  Adaptation  Modification  Extraction  Consultation  Utilisation  Communication pour transmission/ diffusion/ autre forme de mise disposition  Rapprochement ou interconnexion  Limitation/effacement/accès/rectification/opposition/portabilité (si la personne concernée fait usage de l’un de ses droits sur ses données personnelles)  Destruction  Autres traitements (à préciser) : […] |
| Finalité(s) du traitement | […] |
| Catégories de données à caractère personnel traitées  Catégories de données à caractère personnel traitées | Etat civil, identité, données d’identification **:**  Nom, prénom  Adresse postale  Adresse électronique  Identifiant  Photographie  Date et lieu de naissance  Autres (à préciser) : […] |
| Vie personnelle (habitudes de vie, situation familiale, …) :  Habitudes de vie  Situation familiale  Autres (à préciser) : […]. |
| Vie professionnelle (Curriculum Vitae, formations, …) :  Situation professionnelle  Scolarité, formation  CV  Formation professionnelle  Autres (à préciser) : […] |
| Informations d’ordre économique et financier (revenus, situation fiscale, …) :  Coordonnées bancaires  Revenus  Situation financière  Situation fiscale  Autres (à préciser) : […] |
| Données de connexion (adresse IP, logs, etc.) :  Identifiants de terminaux  Identifiants de connexion  Information d’horodatage  Adresse IP  Logs  Autres (à préciser) : […] |
| Données de localisation (déplacements, données, GPS, GSM, …) :  Par satellite (GPS)  Par téléphone mobile (GSM)  Déplacements  Autres (à préciser) : […] |
| Données sensibles :  Données de santé (pathologie, antécédents, …)  Appréciations sur les difficultés sociales de la personne  Décès des personnes  Données médico-administratives (Assurance maladie, PMSI, …)  Données génétiques  Données relatives à l’origine raciale ou ethnique  Données concernant la vie sexuelle ou l'orientation sexuelle  Données relatives aux convictions religieuses  Données relatives à l'appartenance syndicale  Données relatives aux opinions philosophiques  Données relatives aux opinions politiques  Données biométriques  Données particulières (autres) :  Infractions, condamnations, mesures de sûreté  Numéro d’identification national unique (NIR pour la France) |
| Autres données (à préciser) : […] |
| Catégories de personnes concernées | Patients  Usagers  Agents  Prestataires  Mineurs  Autres (à préciser) : […] |
| Transferts Hors UE et EEE | Oui  Non |
| Pour l’exécution du service objet du présent marché, le CHU de Rouen met à la disposition du sous-traitant les informations nécessaires suivantes | […] |

1. **Identification des sous-traitants ultérieur du titulaire**

Liste des sous-traitants susceptibles d’intervenir en fonction de la prestation réalisée à la date de signature du marché. Cette liste est susceptible d’évoluer selon les conditions prévues au point V de la clause « Protection des données ».

|  |  |  |  |
| --- | --- | --- | --- |
| **Société** | **Pays** | **Activités de traitement** | **Date de contrat** |
| […] | […] | […] | […] |
| […] | […] | […] | […] |

Le titulaire déclare ne pas avoir recours à des sous-traitants à la date de signature marché. Le cas échéant, le titulaire obtiendra l’accord du CHU de Rouen selon les conditions prévues au point V de la clause « Protection des données ».