|  |
| --- |
| CONTRAT DE TRAITEMENT DE 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 sous-traitant »,

D’une part

**ET**

**LE CENTRE HOSPITALIER UNIVERSITAIRE DE BREST,**

Etablissement Public de Santé

Dont le siège social se trouve 2, avenue Foch – 29609 BREST cedex

Représenté par Madame Florence FAVREL FEUILLADE, Directrice Générale.

Agissant en qualité de Responsable de traitement et de Client ;

Ci-après désigné par « le CHU de Brest » ou « le Client »,

D’autre part

**XXX** et **le CHU de Brest** sont individuellement désignés par la « Partie » et conjointement désignés par les « Parties ».

**ETANT PREALABLEMENT expose QUE :**

Les sous-traitants qui traitent des données personnelles pour le compte de leurs clients ont de nouvelles responsabilités au regard du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (« *RGPD* »).

Le RGPD impose des obligations spécifiques aux sous-traitants dont la responsabilité sera susceptible d’être engagée en cas de manquement.  Ces obligations concernent **tous les organismes qui traitent des données personnelles pour le compte d’un autre organisme, dans le cadre d’un service ou d’une prestation.**

Désormais, les sous-traitants sont tenus de respecter des obligations spécifiques en matière de sécurité, de confidentialité et de documentation de leur activité. Ils doivent prendre en compte la protection des données dès la conception du service ou du produit et par défaut et mettre en place des mesures permettant de garantir une protection optimale des données.

Les sous-traitants ont notamment une obligation de conseil auprès des clients pour le compte desquels ils traitent des données. Ils doivent les aider dans la mise en œuvre de certaines obligations du règlement (étude d’impact sur la vie privée, notification de violation de données, sécurité, contribution aux audits).

Le présent contrat a également vocation à s’appliquer aux prestations d’hébergement de données de santé. A ce titre, et conformément à l’article L. 1111-8 du Code de la santé publique, tout sous-traitant hébergeant des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte du CHU de Brest devra avoir obtenu la certification hébergeur de données de santé.

Les sous-traitants devront tenir un registre des activités de traitement effectuées pour le compte de leurs clients.

Dans certains cas, ils devront désigner un délégué à la protection des données (DPD) dans les mêmes conditions qu’un responsable de traitement.

A cet effet, le CHU agissant en qualité de responsable de traitement souhaite s’assurer que le sous-traitant présente bien les garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement, objet de la présente convention, réponde aux exigences du présent règlement et garantisse la protection des droits des personnes concernées. (Article 28 du règlement européen).

Le préambule fait partie intégrante de la présente Convention.

**EN CONSEQUENCE, Il a été convenu ce qui suit :**

**ARTICLE 1 – OBJET**

1.1. Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s’engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

1.2. Les termes « données à caractère personnel », « traiter/traitement », « responsable de traitement », « sous-traitant », « personne concernée » et « violation de données à caractère personnel » auront la même signification que dans le Règlement Général Européen sur la Protection des Données.

1.3. Ce Contrat de Traitement de Données complète et précise les dispositions du contrat régissant les prestations fournies par [Nom de la société] (Ci-après désigné « Contrat de sous-traitance »). En cas de contradiction entre les dispositions du Contrat de sous-traitance  et celles du Contrat de Traitement de Données, les dispositions du Contrat de Traitement de Données prévaudront.

**ARTICLE 2 – DESCRIPTION DU TRAITEMENT**

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) : [...].

|  |  |
| --- | --- |
| **N° de contrat** |  |
| **Nature des opérations réalisées sur les données** |  |
| **Finalité du traitement** |  |
| **Catégories de données traitées** |  |
| **Catégorie de personnes concernées** |  |
| **Durée de conservation** |  |
| **Informations transmises par le CHU de Brest au sous-traitant pour l’exécution du contrat** |  |

**ARTICLE 3 – INSTRUCTIONS RELATIVES AU TRAITEMENT**

3.1. 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 dans le cadre du Contrat de Traitement de Données.

3.2. [Nom du sous-traitant], en qualité de sous-traitant, s’engage à traiter les Données **conformément aux instructions documentées** du Client dans le cadre de l’exécution des Services. Le sous-traitant s’engage en outre à ne pas (i) traiter et utiliser les Données à des fins autres que celles visées dans le Contrat de sous-traitance ou dans le Contrat de Traitement de Données ou (ii) divulguer ces Données à des tiers à moins qu’une disposition légale ou réglementaire n’en dispose autrement.

Si le sous-traitant 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**. 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

3.3. Le sous-traitant met en œuvre des mesures techniques et organisationnelles afin de protéger les Données contre tout(e) destruction accidentelle ou frauduleuse, perte accidentelle, modification, divulgation ou accès non autorisé(e). Le sous-traitant restreindra l'accès aux Données à ses salariés et prestataires de services liés par des obligations de confidentialité et ayant besoin d'y accéder afin de fournir les Services. Les mesures techniques et organisationnelles sont détaillées à l’Annexe 1.

3.4. Le sous-traitant apportera une assistance raisonnable pour garantir la conformité du Client quant aux obligations lui incombant en vertu des lois applicables relatives aux droits d’accès des personnes concernées ainsi qu’à leur droit de rectification et de suppression des Données. Le sous-traitant avisera dans les meilleurs délais le Client de toute demande reçue d’une personne concernée en lien avec ses droits d’accès, de modification ou de correction de Données et ne donnera suite à cette demande que conformément aux instructions du Client.

3.5. Le sous-traitant s’engage à 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**.

**ARTICLE 4 – SOUS-TRAITANTS ULTERIEURS**

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat 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 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 sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l’exécution par l’autre sous-traitant de ses obligations.

Le responsable de traitement dispose d’un délai maximum de 15 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 est autorisé à faire appel à l’entité […] (ci-après, le « sous-traitant ultérieur ») pour mener les activités de traitement suivantes : […]

En cas de recrutement d’autres sous-traitants ultérieurs, le sous-traitant doit recueillir l’autorisation écrite, préalable et spécifique du responsable de traitement

**ARTICLE 5 – EXPORTATION DE DONNÉES**

5.1. Dans le cadre des Services, le sous-traitant ne pourra pas transférer les Données à des destinataires situés dans des pays hors de l’Espace Economique Européen, sans accord exprès du Client.

5.2. En cas d’accord exprès du Client, 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, conformément au chapitre V du Règlement européen sur la protection des données.

**ARTICLE 6 – DROIT D’INFORMATION DES PERSONNES CONCERNEES**

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.

**ARTICLE 7 – 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).

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 au délégué à la protection des données désigné par le CHU de Brest à l’adresse mail : [protection.donnees@chu-brest.fr](mailto:protection.donnees@chu-brest.fr)

**ARTICLE 8 – VIOLATION DES DONNÉES À CARACTÈRE PERSONNEL**

Conformément à l’article 33 du Règlement européen sur la protection des données, le sous-traitant notifiera dans les meilleurs délais au Client, toute violation de Données à caractère personnels stockées sur ses systèmes ou supports électroniques ou ceux de sous-traitants ultérieurs autorisés dont ce dernier aurait connaissance et qui serait susceptible de compromettre la disponibilité, la confidentialité ou l’intégrité de ces Données.

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, le sous-traitant ne peut fournir toutes les informations en même temps, les informations pourront être communiquées de manière échelonnée sans autre retard indu.

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.

**ARTICLE 9 – AUDIT**

9.1. À la demande du Client, et conformément à l’article 28 du RGPD, le sous-traitant fournira au Client les informations raisonnablement exigibles et pertinentes démontrant sa conformité quant aux obligations lui incombant au titre du Contrat de Traitement de Données. Le Client peut auditer, dans la limite d’une fois par an, la conformité du sous-traitant au regard des dispositions du Contrat de Traitement de Données en cas de doute raisonnable relatif à un quelconque manquement auxdites dispositions.

9.2. L’audit devra être réalisé au cours des heures normales d'ouverture sur le site concerné, il sera soumis aux règles internes du sous-traitant, 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 Client.

**ARTICLE 10 – DURÉE ET RÉSILIATION**

10.1. Le Contrat de Traitement de Données restera en vigueur pendant toute la durée des opérations de traitement de données à caractère personnel relatives au Contrat de sous-traitance.

10.2. À l’expiration ou en cas de résiliation du Contrat de sous-traitance entraînant résiliation du Contrat de Traitement de Données, le sous-traitant s’engage :

Au choix des parties :

* détruire toutes les données à caractère personnel ou
* à renvoyer toutes les données à caractère personnel au responsable de traitement ou
* 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 doit justifier par écrit de la destruction.

**ARTICLE 11 – DISPOSITIONS DIVERSES**

11.1. Aucune Partie ne pourra être tenue pour responsable envers l’autre Partie en cas de dommage, manque à gagner, perte d’économies anticipées, atteinte à la réputation, perte de clientèle, dommage accessoire ou consécutif résultant de :

* Un accès non autorisé au réseau ou à l’équipement en dépit des mesures de sécurité prises par l’une des Parties conformément à l’Annexe 1 ;
* Toute action coercitive intentée à l’encontre de l’autre Partie par toute autorité réglementaire en raison d’un manquement par l’une des Parties à ses obligations au titre de la législation applicable en matière de protection des données.

11.2. 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 européen sur la protection des données.

11.3. 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.

11.4. Le Contrat de Traitement de Données sera régi et interprété conformément aux lois applicables au contrat de sous-traitance et les Parties se soumettent irrévocablement à la compétence non exclusive des tribunaux stipulés dans les Contrats pour toute réclamation ou litige découlant du Contrat de Traitement de Données.

**EN FOI DE QUOI** les Parties ont demandé à leurs dirigeants ou représentants respectifs dûment autorisés de signer le Contrat de Traitement de Données.

# ARTICLE 12 – Annexes

Est annexé au présent Contrat :

Annexe 1 : **Mesures techniques et organisationnelles** mises en œuvre par le sous-traitant ;

Etant précisé entre les Parties que l’annexe fait partie intégrante du présent Contrat.

Le présent Contrat et son annexe constituent l’intégralité des accords relatifs à la collaboration entre le CHRU de Brest et le sous-traitant à ce jour.

\*\*\*\*\*\*\*\*\*\*\*

**Fait à Brest le jour mois 2025, en deux (2) exemplaires :**

**Pour le CHU de Brest Pour la société**

Nom : Florence FAVREL FEUILLADE Nom :

Titre : Directrice Générale Titre :

Signature : Signature :