Table des matières

[1 Aide au remplissage de ce document 2](#_Toc83399159)

[1.1 document de référence CNIL 2](#_Toc83399160)

[1.2 Précisions pour renseigner ce document 2](#_Toc83399161)

[Définitions (extrait article 4 RGPD) 4](#_Toc83399162)

[Préambule 4](#_Toc83399163)

[CONVENTION 5](#_Toc83399164)

[**ARTICLE 1 – Objet** 5](#_Toc83399165)

[**ARTICLE 2 - Description du traitement faisant l’objet de la sous-traitance** 5](#_Toc83399166)

[**ARTICLE 3 – Instructions relatives au traitement** 6](#_Toc83399167)

[**ARTICLE 4 – Sous-traitants ultérieurs** 7](#_Toc83399168)

[**ARTICLE 5 – Exportation de données** 7](#_Toc83399169)

[**ARTICLE 6 – Droit d’information des personnes concernées** 8](#_Toc83399170)

[**ARTICLE 7 – Exercice des droits des personnes** 8](#_Toc83399171)

[**ARTICLE 8 – Notification des violations des données à caractère personnel** 8](#_Toc83399172)

[**ARTICLE 9 – Audit** 9](#_Toc83399173)

[**ARTICLE 10 – Durée et résiliation – Sort des données** 9](#_Toc83399174)

[**ARTICLE 11 - Délégué à la protection des données** 10](#_Toc83399175)

[**ARTICLE 12 - Registre des catégories d’activités de traitement** 10](#_Toc83399176)

[**ARTICLE 13 - Documentation** 11](#_Toc83399177)

[**ARTICLE 14 – Dispositions diverses** 11](#_Toc83399178)

[**ANNEXE 1 - Mesures techniques et organisationnelles** 12](#_Toc83399179)

[**ANNEXE 2 - Points de contact des deux parties** 13](#_Toc83399180)

Nom du document CHU : 4-Annexe - SSI - Contrat sous-traitance RGPD-V3.docx

Version 04 du 24 septembre 2021

# Aide au remplissage de ce document

## document de référence CNIL

* <https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-un-guide-pour-accompagner-les-sous-traitants>
* <https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses>

## Précisions pour renseigner ce document

Seules les phrases ou mots surlignés en jaune sont à modifier ou adapter.

A l’article 4 :

Si vous n'envisagez pas de sous-traitants ultérieurs mettre "Sans objet - pas de sous-traitance ultérieure" à l'option A (autorisation générale) et B (autorisation spécifique).

Aux Articles 6 et 7 :

Si le traitement ne concerne pas la collecte de données personnelles, indiquez que cet article est sans objet.

Si le traitement concerne la collecte de données personnelles, choisir réponse A.

A l’annexe 1 :

SI le traitement concerne la collecte de données de santé, merci de contacter le DPO de l’établissement pour préciser le contenu de l’annexe 1.

**CLAUSES CONTRACTUELLES de TRAITEMENT de données**

**responsable de traitement – sous traitant**

**ENTRE**

**Le Centre Hospitalier Universitaire d’Angers**,

Etablissement Public de Santé

Dont le siège social est situé : 4, rue Larrey 49933 Angers Cedex 9

Représenté par : Madame Cécile Jaglin-Grimonprez en sa qualité de Directrice Générale,

Agissant en qualité de Responsable de traitement et de client ;

Ci-après dénommé : « ***le responsable de traitement***»

**D’une part,**

**ET**

**[Nom de la société]**,

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

Dont le siège social est situé : [Adresse siège social]

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

Représenté par : [Nom du Dirigeant],

Agissant en qualité de sous-traitant et de fournisseur de produits et services référencés au marché n° [numéro de marché] en date du [date notification du marché] concernant la consultation [numéro de consultation] en date du [date de consultation] ;

Ci-après dénommé : « ***le sous-traitant***»

**D’autre part,**

**[Nom de la société]** et **le CHU d’Angers** sont individuellement désignés par la « Partie » et conjointement désignés par les « Parties ».

# Définitions (extrait article 4 RGPD)

Aux fins du **R**èglement **G**énéral de **P**rotection des **D**onnées du 27/04/2016, on entend par :

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

- **Personne concernée** : 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.

- **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. Cette définition intègre également le sous-traitant ultérieur à qui le sous-traitant peut faire appel.

- **Traiter/Traitement** : toute opération ou tout ensemble d'opérations effectué 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.

- **Violation de données à caractère personnel** : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

# Préambule

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 (consultation préalable de l’autorité de contrôle, étude d’impact sur la vie privée, notification de violation de données, sécurité, contribution aux audits).

Les présentes clauses contractuelles de traitements de données ont 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 d’Angers 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 conséquence, il a été convenu ce qui suit :

# CONVENTION

### **ARTICLE 1 – Objet**

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.

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*** »).

Ces Clauses Contractuelles 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 des Clauses Contractuelles de Traitement de Données, les dispositions des Clauses Contractuelles de Traitement de Données prévaudront pour le traitement des données à caractères personnel.

### **ARTICLE 2 - 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) [...].

La nature des opérations réalisées sur les données est […].

La ou les finalité(s) du traitement sont [...].

Les données à caractère personnel traitées sont […].

Les catégories de personnes concernées sont […].

Pour l’exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes […]

### **ARTICLE 3 – Instructions relatives au traitement**

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 sous-traitance.

[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 :

- traiter et utiliser les Données à des fins autres que celles visées dans le Contrat de sous-traitance

- 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 dans les plus brefs délais le responsable de traitement** dès la date de son constat.

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

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 sous réserve que l’hébergement des données à caractères personnelles et/ou des données de santé soit réalisé à l’extérieur de l’enceinte de l’établissement.

Le client, en qualité de responsable de traitement, fournira un accès distant au sous-traitant qui réponde aux exigences de la PGSSI-S – Guide ASIP-Santé « Règles pour les interventions à distance sur les systèmes d’information de santé ». Les clauses de sécurité et une charte pour les prestataires seront remis par le client et, préciseront les modalités d’accès aux données à caractères personnelles. Les accès aux données seront nominatifs et les ressources autorisées (base de production ou base de tests) seront spécifiées dans les demandes d’habilitations. Le sous-traitant devra informer le client de tout changement d’intervenant pour créer ou résilier les habilitations.

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.

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 ultérieurs**

*Choisir l’une des deux options*

***Option A*** *(autorisation générale)*

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « ***le sous-traitant*** ***ultérieur*** ») pour mener des activités de traitement spécifiques. Dans ce cas, il informepréalablement et par écrit le responsable de traitement de tout changement envisagé concernant l’ajout ou le remplacement d’autres sous-traitants dans un délai de un mois avant la mise en œuvre du traitement 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 minium de […] 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.

Les points de contacts des deux parties devront être identifiés en Annexe 2. Tout changement de coordonnées des personnes des deux parties à contacter devra faire l’objet d’une mise à jour de cette Annexe 2 et être validé par les deux parties.

***Option B*** *(autorisation spécifique) /!\ obligatoire si hébergement de données de santé*

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.

***Quelle que soit l’option*** *(autorisation générale ou spécifique)*

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement.

Conformément à l’article 33 du Règlement européen sur la protection des données, le sous-traitant ultérieur notifiera au responsable de traitement et, au sous-traitant initial, dans un délai maximum de 72 heures, toute violation de Données à caractère personnels dans les meilleurs délais à partir des premiers éléments constatés (cf.**ARTICLE 8** ).

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.

### **ARTICLE 5 – Exportation de données**

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.

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.

Dès que le sous-traitant annonce publiquement l’obtention de l’accord des autorités de protection des données de l’Union Européenne, les transferts de Données seront couverts par les règles internes d'entreprise ou Binding Corporate Rules (BCR) applicables aux sous-traitants.

### **ARTICLE 6 – 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.

### **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).

*Choisir l’une des deux options*

*[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 dpo@chu-angers.fr

*[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.

### **ARTICLE 8 – Notification des violations des données à caractère personnel**

Conformément à l’article 33 du Règlement européen sur la protection des données, le sous-traitant notifiera au Client, dans un délai maximum de 72 heures, toute violation de Données à caractère personnels dans les meilleurs délais à partir des premiers éléments constatés. Que ces dernières soient stockées :

* sur ses systèmes ou supports électroniques
* sur 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 décrit autant que possible, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

* 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 de la nature de la violation de données à caractère personnel
* 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.
* 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 ;

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 (suivant l’ordre de la liste ci-dessus) sans 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**

A la demande du Client, et conformément à l’article 28 §3 h) du RGPD, le sous-traitant fournira au Client les documentations raisonnablement exigibles et pertinentes démontrant sa conformité quant aux obligations lui incombant au titre des Clauses Contractuelles de Traitement de Données. Le Client ou l’un de ses mandataires peut auditer, dans la limite d’une fois par an, la conformité du sous-traitant au regard des dispositions des Clauses Contractuelles de Traitement de Données en cas de doute raisonnable relatif à un quelconque manquement auxdites dispositions.

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.

Cet audit est notifié par le Client au Prestataire par lettre recommandée avec accusé de réception détaillant les documents demandés et, le cas échéant, le protocole qui sera déroulé, les méthodes utilisées et données auditées, trente (30) jours ouvrés avant la date projetée de sa mise en œuvre.

Il est expressément convenu entre les Parties qu’est privilégiée, dans la mesure du possible, la réalisation d’un audit sur pièces et qu’un audit sur place sera programmé si les éléments mis à la disposition par le Prestataire ne s’avéraient pas suffisant pour démontrer le respect de ses obligations au titre de la présente clause.

Dans ce second cas de figure, le Client assume les frais supplémentaires résultants, notamment, de la nécessité d’un renforcement des effectifs pour permettre la réalisation de l’audit et la continuité de l’activité du Prestataire.

L’audit est effectué par le Client ou par un tiers désigné par lui, à la triple condition que ce tiers ne soit pas un concurrent direct ou indirect du Prestataire, qu’il soit soumis au secret professionnel et qu’il ait conclu un accord de confidentialité.

Il est, par ailleurs, entendu que cette démarche d’audit exclut toute communication de documents de nature financière, comptable ou tenant aux relations du Prestataire avec d’autres clients.

Les résultats d’audit feront l’objet d’un débat contradictoire et d’une validation par les Parties. Les frais d'audit demeureront à la charge du Client, ainsi que les éventuels frais engagés et temps passé par le Prestataire.

### **ARTICLE 10 – Durée et résiliation – Sort des données**

Le présent contrat entre en vigueur à compter de la date de notification du marché et est applicable pendant la période d’exécution du marché.

Les Clauses Contractuelles de Traitement de Données resteront en vigueur pendant toute cette durée des opérations de traitement de données à caractère personnel relatives au Contrat de sous-traitance.

A l’expiration ou en cas de résiliation du Contrat de sous-traitance entraînant résiliation des Clauses Contractuelles de Traitement de Données, le sous-traitant s’engage à :

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 - 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 àl’article 37 du règlement européen sur la protection des données. Le responsable de traitement en fait de même.

|  |  |
| --- | --- |
| **DPO du Responsable de traitement**  Nom : POCQUET  Prénom : Pierre-Alain   : DPO@CHU-Angers.fr   : 02 41 35 49 29 | **DPO du Sous-traitant**  Nom : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Prénom : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_\_\_\_\_   : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

### **ARTICLE 12 - 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.

### **ARTICLE 13 - Documentation**

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’un audit sur pièces ou d’un audit sur place (cf. ARTICLE 9 – Audit §9.3, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

### **ARTICLE 14 – Dispositions diverses**

Le responsable de traitement s’engage à :

* fournir au sous-traitant les données visées à l’article 2 des présentes clauses
* documenter par écrit toute instruction concernant le traitement des données par le sous-traitant
* 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 sous-traitant
* superviser le traitement, y compris réaliser les audits sur pièces ou les audits sur place auprès du sous-traitant (cf. ARTICLE 9 – Audit §9.3 ).

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.

Les Clauses Contractuelles de Traitement de Données seront régies et interprétées 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 des Clauses du contrat de sous-traitance.

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

Fait en deux exemplaires originaux, à Angers, le [JJ].[MM].[AAAA].

|  |  |
| --- | --- |
| **Pour le CHU d’Angers**  **Madame Cécile JAGLIN-GRIMONPREZ** | **Pour XXX**  **Monsieur/Madame XXX** |
| Directrice Générale | XXX |
|  |  |

### **ANNEXE 1 - Mesures techniques et organisationnelles**

Le sous-traitant s’engage à mettre en œuvre les mesures de sécurité prévues à l’annexe Plan Assurance Sécurité du présent appel d’offres conformément aux principes de base suivants :

*Décrire les mesures techniques et organisationnelles garantissant un niveau de sécurité* *adapté au risque, y compris, entre autres :*

*La pseudonymisation et le chiffrement des données à caractère personnel*

*Les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;*

*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;*

*Une procédure visant à tester, à ’analyser et à ’évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement*]

### **ANNEXE 2 - Points de contact des deux parties**

Les points de contacts des deux parties devront être identifiés pour permettre la gestion et l’information des changements des acteurs, parties prenantes dans mise en œuvre de mesures techniques et organisationnelles appropriées au traitement faisant l’objet de la présente convention.

Tout changement de coordonnées des personnes des deux parties à contacter devra faire l’objet d’une mise à jour de cette Annexe 2 et être validé par les deux parties.