**MODIFICATION (AVENANT) RGPD**

**AU CONTRAT**

**N° XXXXXXXXXXX et au marché n° XXXXXXXXX**

***Date :***

***Version :***

***ENTRE***

Société X

Raison sociale – Capital

RCS – SIRET

Adresse

Représentée par

Agissant en qualité de sous-traitant et de fournisseur de services d’hébergement

Ci-après désigné par « Société X», ou «le Sous-traitant» ou le «Titulaire»

D’une part

***ET***

CH

Raison sociale – Capital

RCS – SIRET

Adresse

Représentée par

Représenté par

Agissant en qualité de Responsable de traitement et de Client ;

Ci-après désigné par CHM (Centre Hospitalier du Mans), « client » ou « responsable de traitement ».

D’autre part

Société X et CH sont individuellement désignés par la « Partie » et conjointement désignés par les « Parties »

**SOMMAIRE**

[**I.** **Préambule** 2](#_Toc535397508)

[**II.** **Objet** 3](#_Toc535397509)

[**III.** **Description du traitement faisant l’objet de la sous-traitance** 3](#_Toc535397510)

[**IV.** **Obligations du sous-traitant vis-à-vis du responsable de traitement** 4](#_Toc535397511)

[**V.** **Obligations du responsable de traitement vis-à-vis du sous-traitant** 8](#_Toc535397512)

# Préambule

Les clauses énoncées dans ce document s’appliquent pour tout traitement de données à caractère personnel par un sous-traitant pour le compte du responsable du traitement.

On entend par :

* **Données à caractère personnel :** toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée"); est réputée être une "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 (définition générale) :** toute opération ou tout ensemble d'opérations effectuées à l'aide de procédés automatisés ou non et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.
* **Traitement de type 1 :** La prestation objet du marché (matériel, logiciel, prestation de services, etc.) est livrée sur le site de la Personne Publique et les données traitées et les traitements effectués sur ces données sont réalisés in situ par le CHM, qui est Responsable de Traitement.

Exemple : un logiciel ou un matériel hébergé dans les datacenters du CHM, une prestation de service réalisée dans les locaux du CHM, etc.

* **Traitement de type 2 :** La prestation objet du marché (matériel, logiciel, prestation de services, etc.) est livrée dans les locaux du sous-traitant avec une assistance technique ou organisationnelle du sous-traitant, mais les données traitées et les traitements effectués sur ces données sont réalisés par le CHM qui est Responsable de Traitement. La plupart du temps, le sous-traitant n’est pas en contact direct avec les personnes dont les données sont traitées.

Exemple : un logiciel en mode SaaS, une prestation d’analyse de biologie, etc.

* **Traitement de type 3 :** La prestation objet du marché (matériel, logiciel, prestation de services, etc.) est livrée dans les locaux du CHM ou ceux du Titulaire du marché, mais les données traitées et les traitements effectués sont réalisés par le Titulaire du marché, qui est Responsable du Traitement.

Exemple : une prestation de services de conciergerie livrée « clés en main » par le Titulaire du marché.

* **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 (article 4 du règlement européen).
* **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, sur instruction et sous l’autorité du responsable du traitement.
* **Consentement de la personne concernée :** toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.
* **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.

Tout partenaire du CHM 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 CHM, le mainteneur étant amené à réaliser un traitement de données à caractère personnel au sens des précédentes définitions.

Le préambule fait partie intégrante du présent document.

# Objet

Les présentes clauses complètent et précisent les dispositions du **CONTRAT XXXXXXXXXXXXXXXXXXXXXXXXXXX** régissant les prestations fournies par la société **XXXXXXXXXX** (Ci-après désigné **«le contrat »**). En cas de contradiction entre les dispositions du Contrat et les clauses du présent document, ce sont ces dernières qui prévaudront.

Les dispositions du présent document resteront en vigueur pendant toute la durée des opérations de traitement de données à caractère personnel relatives au Contrat de sous-traitance.

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 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.

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

**Traitement de type 1**

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) :

* Intervention de maintenance sur site ou à distance ;
* Opérations techniques nécessaires au maintien en condition opérationnelle, notamment supervision, remontée d’alertes techniques, etc.

1. La finalité du traitement est :

Traitement des données dans le cadre des prestations prévues au contrat de sous-traitance et dans le respect d’une part des exigences du *Référentiel sécurité des systèmes d’information du CHM* en annexe 1 du présent document, et d’autre part des règles édictées dans la charte de bon usage du SI à destination des prestataires du CHM dans le cas où le sous-traitant y est soumis.

1. Les données à caractère personnel traitées sont :

Données révélant l'origine raciale ou ethnique

Données révélant les opinions politiques

Données révélant les convictions religieuses ou philosophiques

Données révélant l'appartenance syndicale

Données génétiques

Données biométriques aux fins d'identifier une personne physique de manière unique

Données concernant la santé

Données concernant la vie sexuelle ou l'orientation sexuelle

Données relatives à des condamnations pénales ou infractions

Numéro d'identification national unique (NIR pour la France)

Etat civil, identité, données d'identification, images…

Vie personnelle (habitudes de vie, situation familiale, etc.)

Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.)

Données de connexion (adresse IP, logs, etc.)

Données de localisation (déplacements, données GPS, GSM, etc.)

1. Les catégories de personnes concernées sont :

Patients

Usagers

Agents

Prestataires

Mineurs

Autres (Préciser) : …………………………………………………….

1. Pour l’exécution du service objet du présent document, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes :

Informations techniques nécessaires à la réalisation du traitement. (informations de connexion, modalités de connexion, adresses IP cibles nécessaires à la réalisation du service).

**Traitement de type 2**

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) :

* Intervention de maintenance sur site ou à distance ;
* Opérations techniques nécessaires au maintien en condition opérationnelle, notamment supervision, remontée d’alertes techniques, etc. ;
* Sauvegardes de données, restaurations, etc. ;

1. La finalité du traitement est :

Traitement des données dans le cadre des prestations prévues au contrat de sous-traitance et dans le respect d’une part des exigences du *Référentiel sécurité des systèmes d’information du CHM* en annexe 1 du présent document, et d’autre part des règles édictées dans la charte de bon usage du SI à destination des prestataires du CHM dans le cas où le sous-traitant y est soumis.

1. Les données à caractère personnel traitées sont :

Données révélant l'origine raciale ou ethnique

Données révélant les opinions politiques

Données révélant les convictions religieuses ou philosophiques

Données révélant l'appartenance syndicale

Données génétiques

Données biométriques aux fins d'identifier une personne physique de manière unique

Données concernant la santé

Données concernant la vie sexuelle ou l'orientation sexuelle

Données relatives à des condamnations pénales ou infractions

Numéro d'identification national unique (NIR pour la France)

Etat civil, identité, données d'identification, images…

Vie personnelle (habitudes de vie, situation familiale, etc.)

Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.)

Données de connexion (adresse IP, logs, etc.)

Données de localisation (déplacements, données GPS, GSM, etc.)

1. Les catégories de personnes concernées sont :

Patients

Usagers

Agents

Prestataires

Mineurs

Autres (Préciser) : …………………………………………………….

1. Pour l’exécution du service objet du présent document, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes :

Informations techniques nécessaires à la réalisation du traitement. (informations de connexion, modalités de connexion, adresses IP cibles nécessaires à la réalisation du service).

**Traitement de type 3**

Le Titulaire doit décrire précisément :

1. Les données traitées ;
2. La nature des opérations réalisées sur ces données ;
3. La ou les finalité(s) du traitement ;

# Durée du contrat

La présente modification (avenant) entre en vigueur à compter de sa signature et jusqu’à la fin du Contrat.

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

Le sous-Traitant s’engage à :

1. traiter les données **uniquement pour la seule finalité** qui fait l’objet de la sous-traitance.
2. traiter les données **conformément aux instructions documentées** du responsable de traitement figurant à l’annexe 1 ***Référentiel sécurité des systèmes d’information du CHM*** du présent document. 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. **garantir la confidentialité** des données à caractère personnel traitées dans le cadre du présent document.
4. veiller à ce que les **personnes autorisées à traiter les données à caractère personnel**en vertu du présent document :

* 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. **Sous-traitance de rang(s) ultérieur(s)**

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 informe préalablement et par écrit le responsable de traitement des caractéristiques de cette sous-traitance selon les mêmes champs que ceux énumérés à l’article III a) à f). Il l’informe également de tout changement envisagé concernant l’ajout ou le remplacement de sous-traitants.

Cette information doit en outre indiquer clairement l’identité et les coordonnées du sous-traitant ainsi que les dates du contrat de sous-traitance. Le responsable de traitement dispose d’un délai de 2 mois 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.

A la date de signature du contrat de sous-traitance, le sous-traitant déclare qu’il fait d’ores et déjà appel au(x) sous-traitant(s) de rang ultérieur suivant :

**A compléter par la société en utilisant l’annexe 2 : Modèle de déclaration de sous-traitant(s) ultérieur(s).**

**Le sous-traitant renseignera autant de déclaration de sous-traitant ultérieur que nécessaire**

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

En conséquence 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.

Pour ce faire le sous-traitant prendra toutes les mesures nécessaires, notamment en répercutant toutes les exigences prévues aux présentes dans le contrat qu’il conclura avec le sous-traitant ultérieur.

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.

1. **Droit d’information des personnes concernées**

**Traitements de type 1 et 2 :**

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.

**Traitements de type 3 :**

Le Titulaire, 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 sont de la seule responsabilité du Titulaire.

1. **Exercice des droits des personnes**

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 notamment : droit d’accès, de rectification, d’effacement et d’opposition, droit à la limitation du traitement, droit à la portabilité des données conformément à la loi relative aux droits des malades et à la qualité du système de santé 2002 N°2002-303 4 mars 2002, 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 responsable de traitement via [DPO@ch-lemans.fr](mailto:DPO@ch-lemans.fr)

**Traitements de type 1 et 2 :**

Le Responsable du traitement est responsable de la prise en charge de l’exercice des droits des personnes. Le sous-traitant transmet toutes les données nécessaires dans un délai de 24h pour que le responsable du traitement puisse assurer cette conformité réglementaire.

**Traitements de type 3 :**

Le Titulaire doit répondre, 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 du présent document.

1. **Notification des violations de données à caractère personnel**

**Traitements de type 1 et 2 :**

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans le plus bref délai (maximum 24 heures) après en avoir pris connaissance et par le moyen suivant [DPO@ch-lemans.fr](mailto:DPO@ch-lemans.fr). 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 et aux personnes concernées.

**Traitements de type 3 :**

Le Titulaire notifie à l’autorité de contrôle compétente (la CNIL) les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d’engendrer un risque pour les droits et libertés des personnes physiques.

Dans tous les cas, les données à communiquer seront les suivantes :

* 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.

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

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

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

1. **Mesures de sécurité**

**Traitements de type 1 et 2 :**

Le sous-traitant s’engage à mettre en œuvre les mesures de sécurité prévues à l’annexe 1 ***Référentiel sécurité des systèmes d’information du CHM*** du présent document et conformes aux principes de base suivants :

* la pseudonymisation et le chiffrement des données à caractère personnel selon la criticité des données convenue avec le responsable de traitement
* 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

Le périmètre de responsabilité du sous-traitant intègre tous les composants et services permettant la réalisation de l’objet du contrat de sous-traitance.

Les mesures de sécurité à mettre en œuvre sont décrites à l’annexe 1 du présent document ***Référentiel sécurité des systèmes d’information du CHM.***

Le sous-traitant fournit son appréciation des risques formalisée telle qu’exigée dans le RGPD.

1. **Sort des données**

**Traitements de type 1 et 2 :**

Au terme de la prestation de services relatifs au traitement de ces données (expiration ou résiliation du Contrat de sous-traitance), le sous-traitant s’engage à :

* Ne pas utiliser les données à d’autres fins que celles prévues par le contrat de sous-traitance,
* Ne pas utiliser les données pour son compte ou celui d’un tiers,
* Ne pas transférer les données à un tiers sauf à un sous-traitant désigné par le responsable de traitement,
* N’utiliser les données que pendant la durée du contrat de sous-traitance,
* Restituer les données au terme du contrat de sous-traitance quelle qu’en soit la cause
* Détruire toutes les copies existantes des données dans le système d’information du sous-traitant et des sous-traitants ultérieurs et justifier par écrit de cette destruction auprès du responsable de traitement dans un délai d’un mois à compter de la fin du contrat de sous-traitance.
* Respecter les dispositions prévues à l’annexe 1 ***Référentiel sécurité des systèmes d’information du CHM*** du présent document en conformité avec les réglementations applicables au périmètre de données concernées par le contrat de sous-traitance.

**Traitements de type 3 :**

Le sort des données est de la seule responsabilité du Titulaire du marché.

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

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

Le délégué à la protection des données désigné par le sous-traitant est à minima francophone, ou au moins anglophone.

1. **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 ;
* 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.

Sans préjudice de ce qui précède le responsable de traitement pourra demander au sous-traitant toute information complémentaire nécessaire dans le cadre de l’exécution du présent document.

1. **Documentation et audit**

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

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

Le responsable de traitement s’engage à :

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

**La société et le client paraphe toutes les pages et signe ce document**

Fait (en deux exemplaires originaux) à ………………………………………..……………, le ….…/…./……..…

|  |  |  |
| --- | --- | --- |
| **Pour *le client* (Nom et qualité du signataire)** |  | **Pour *la société XXXXXXXXXXXXXXXXXX***  **(Nom, qualité du signataire et cachet de la société)** |