**Clauses contractuelles de sous-traitance conformes aux obligations des articles 28 et 30 du règlement européen sur la protection des données.**

Le **CHR Metz-Thionville**, situé à 1, allée du château - CS 45001 - 57085 Metz cedex 03 France et représenté par la Directrice Générale Mme Saillard Marie Odile

D’une part,

ET

[…………….…], situé à [………….…] et représenté par […………….] (ci-après, « ***le sous-traitant***»)

d’autre part,

**I. Objet**

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s’engage à effectuer pour le compte du **CHR Metz-Thionville** 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*** »).

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

Le sous-traitant est autorisé à traiter pour le compte du CHR Metz-Thionville les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) […*Décrire le(s) ou le(s) services fournis par le sous-traitant*...].

La nature des opérations réalisées sur les données est […*Décrire les opérations réalisées sur les données à caractère personnel sur le périmètre du(es) service(s) du présent contrat*…………].

La ou les finalité(s) du traitement sont […*Décrire la(es) finalité(s) du traitement au sens du RGPD*.].

Les données à caractère personnel traitées sont […*Faire la liste des catégories de données auxquelles le sous-traitant pourra avoir accès dans le cadre des opérations de traitements sous-traitées*……………].

Les catégories de personnes concernées sont […*Décrire la liste des personnes concernées par les opérations de traitements sous-traitées (patients, personnels de l’établissement, personnels de partenaires,* ………………].

Pour l’exécution du service objet du présent contrat, le **CHR Metz-Thionville** met à la disposition du sous-traitant les informations nécessaires suivantes […*Faire la liste des informations mis à la disposition du CHR pour le bon déroulement des opérations de traitement sous-traitées*………..…].

**III. Durée du contrat**

Le présent contrat entre en vigueur à compter du [……………] pour une durée de […………].

**IV. Obligations du sous-traitant vis-à-vis du CHR Metz-Thionville**

Le sous-traitant 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.

2. traiter les données **conformément aux instructions documentées** du **CHR Metz-Thionville** figurant en annexe du présent contrat. 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 Luxembourgeois relative à la protection des données, il en **informe immédiatement** le CHR Metz-Thionville. 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 **CHR Metz-Thionville** de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public. Recommandation : Interdire le transfert de données dans un pays tiers

3. garantir la **confidentialité** des données à caractère personnel traitées dans le cadre du présent contrat

4. veiller à ce que les **personnels autorisés à traiter les données à caractère personnel** en vertu du présent contrat :

* 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.

5. 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.**

6. **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 spécifiques. Dans ce cas, il informe préalablement et par écrit le **CHR Metz-Thionville** 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 **CHR Metz-Thionville** dispose d’un délai minimum 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 **CHR Metz-Thionville** n’a pas émis d'objection pendant le délai convenu.

***Autre option possible*** *(autorisation spécifique)*

Le sous-traitant est autorisé à faire appel à l’entité […………..…] (ci-après, le « ***sous-traitant ultérieur*** ») pour mener les activités de traitement suivantes : […*Liste des opérations de traitements sous-traitées par le sous-traitant*………..]

En cas de recrutement d’autres sous-traitants ultérieurs, le sous-traitant doit recueillir l’autorisation écrite, préalable et spécifique du **CHR Metz-Thionville**.

***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 **CHR Metz-Thionville**. Il appartient au sous-traitant initial de s’assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en oeuvre 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 **CHR Metz-Thionville** de l’exécution par l’autre sous-traitant de ses obligations.

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

Il appartient au **CHR Metz-Thionville** de fournir l’information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

***Autre Option possible***

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 **CHR Metz-Thionville** avant la collecte de données.

8. **Exercice des droits des personnes**

Dans la mesure du possible, le sous-traitant doit aider le **CHR Metz-Thionville** 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 à [dpo@chr-metz-thionville.fr](mailto:dpo@chr-metz-thionville.fr)

***Autre option relative à la procédure de traitement des demandes***

Le sous-traitant doit répondre, au nom et pour le compte du **CHR Metz-Thionville** 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.

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

Le sous-traitant notifie au **CHR Metz-Thionville** toute violation de données à caractère personnel dans un délai maximum de […*Proposition : 1h00*…..] heures après en avoir pris connaissance et par le moyen suivant […*Proposition  : Mail au contact du CHR et appel téléphonique*…]. Cette notification est accompagnée de toute documentation utile afin de permettre au **CHR Metz-Thionville**, si nécessaire, de notifier cette violation à la CNIL.

***Autre option possible***

Après accord du **CHR Metz-Thionville**, le sous-traitant notifie à la CNIL, au nom et pour le compte du **CHR Metz-Thionville**, 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.

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 il n’est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord du **CHR Metz-Thionville**, le sous-traitant communique, au nom et pour le compte du **CHR Metz-Thionville**, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et 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.

10. **Aide du sous-traitant dans le cadre du respect par le CHR Metz-Thionville de ses obligations**

Le sous-traitant aide le **CHR Metz-Thionville** pour la réalisation d’analyses d’impact relative à la protection des données (AIPD) en conformité avec les exigences de l’article 35 du règlement européen sur la protection des données. Le sous-traitant aide le **CHR Metz-Thionville** pour la réalisation de la consultation préalable de l’autorité de contrôle en conformité avec les exigences de l’article 36 du règlement européen.

11. **Mesures de sécurité**

Le sous-traitant s’engage à mettre en oeuvre les mesures de sécurité suivantes :

[…*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…].*

Le sous-traitant s’engage à mettre en oeuvre les mesures de sécurité prévues par [*code de conduite, certification*].

[*Dans la mesure où l’article 32 du règlement européen sur la protection des données prévoit que la mise en oeuvre des mesures de sécurité incombe au responsable du traitement et au sous-traitant, il est recommandé de déterminer précisément les responsabilités de chacune des parties au regard des mesures à mettre en oeuvre*]

12. **Sort des données**

Au terme de la prestation de services relatifs au traitement des 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 CHR Metz-Thionville ou
* à renvoyer les données à caractère personnel au sous-traitant désigné par le CHR Metz-Thionville

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.

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

Le sous-traitant communique au **CHR Metz-Thionville 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.

14. **Registre des catégories d’activités de traitement**

Conformément à l’article 30 du règlement européen sur la protection des données, le sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d’activités de traitement effectuées pour le compte du **CHR Metz-Thionville** comprenant :

* le nom et les coordonnées du **CHR Metz-Thionville** 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 **CHR Metz-Thionville**;
* 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.

15. **Documentation**

Le sous-traitant met à la disposition du **CHR Metz-Thionville** la **documentation nécessaire pour démontrer le respect de toutes ses obligations** et pour permettre la réalisation d'audits, y compris des inspections, par le **CHR Metz-Thionville** ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

*Options : Engagements complémentaires aux exigences du règlement européen*

16. **Obligation de conseil**

*Le sous-traitant s’engage à conseiller le CHR Metz-Thionville sur l’application du Règlement Général de Protection des Données dès lors qu’il considère qu’une non-conformité peut avoir un impact que le respect de clauses du présent contrat.*

### 17. ***Communication de données à des tiers autorisés***

*Le sous-traitant s’engage à informer sans délai le CHR Metz-Thionville en cas de requête provenant d’une autorité administrative ou judiciaire demandant à avoir communication de données à caractère personnel entrant dans le périmètre du présent contrat.*

*Dans le cas où la requête est reçue par le CHR Metz-Thionville, le sous-traitant s’engage à mettre en œuvre les moyens permettant de répondre à la demande dans les délais exigés sur le périmètre des opérations de traitement sous-traitées.*

### 18. ***Engagement relatif aux audits***

*Le sous-traitant s’engage à répondre aux demandes d’audit du CHR Metz-Thionville, effectuées par lui-même ou par un tiers de confiance qu’il aura sélectionné et s’engage à mettre en œuvre les moyens permettant à l’auditeur de réaliser sa mission dans les meilleures conditions.*

*Le CHR Metz-Thionville s’engage à fournir au sous-traitant une copie du rapport d’audit afin qu’il puisse prendre en compte rapidement les non-conformités constatées et les mesures correctives proposées.*

*Le sous-traitant s’engage à mettre en œuvre les mesures correctives nécessaires au traitement des non-conformités identifiées dans un délai et selon les conditions définies d’un commun accord.*

*Dans le cas ou des mesures correctives ne seraient pas applicables, le sous-traitant s’engage à justifier l’impossibilité de mettre en œuvre les mesures et s’engage à proposer des mesures palliatives pour réduire les risques encourus.*

### 19. ***Engagement du sous-traitant en tant que responsable de traitements***

*Le sous-traitant s’engage à respecter les obligations qui lui incombent en tant que responsable de traitements et à fournir au CHR Metz-Thionville des éléments de traçabilité permettant de le démontrer.*

*Le délégué à la protection des données du sous-traitant se tiendra à la disponibilité du CHR Metz-Thionville pour apporter les éléments justificatifs démontrant l’application du Règlement Général de Protection des Données.*

### 20. ***Devoir de coopération avec la CNIL***

*Le sous-traitant s’engagent à coopérer avec la CNIL, notamment en cas de demande d’information qui pourrait être adressée par cette dernière, ou en cas de contrôle sur site ou à distance des opérations de traitement sous-traitées.*

*Le sous-traitant s’engage à informer sans délai le CHR Metz-Thionville en cas de contrôle de la CNIL (sur site ou à distance) impactant le périmètre des opérations de traitement sous-traitées et à remettre le cas échéant une copie du rapport de la CNIL.*

### ***Obligation de confidentialité***

*Le sous-traitant s’engage à veiller à ce que les personnels autorisés à intervenir sur les moyens de traitement des données à caractère personnel respectent les consignes internes en matière de sécurité définies dans les documents de politique de sécurité interne.*

*Soumis à des obligations de discrétion professionnelle, ou le cas échéant soumis au secret professionnel, les personnels du sous-traitant sont régulièrement sensibilisés sur leurs rôles et responsabilités en matière de confidentialité et de sécurité des données.*

**V. Obligations du CHR Metz-Thionville vis-à-vis du sous-traitant**

Le **CHR Metz-Thionville** s’engage à :

1. fournir au sous-traitant les données visées au paragraphe II des présentes clauses ;

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.

ANNEXE I : Instructions du **CHR Metz-Thionville** relatives aux traitement des données

*A compléter : Le sous-traitant doit décrire les instructions qu’il a reçu du CHR Metz-Thionville concernant les opérations de traitements sous-traitées (exigence du RGPD article 28)*