Annexe Protection des Données

L'Hôpital Novo, situé 6 avenue de l'Ile de France BP79, à Pontoise (95303)

et représenté par Monsieur Alexandre AUBERT

(ci-après désigné, « ***l'Acheteur*** »)

d'une part,

Et

…….., société située à ……, ……

et représentée par ……

(ci-après désignée, « ***le Titulaire du marché***»)

d'autre part,

Le Titulaire du marché et l'Acheteur sont conjointement dénommés « Les Parties »

I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles l'Acheteur et le Titulaire du marché s'engagent à assurer la conformité et la sécurité des opérations de Traitement(s) 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 aux Traitements de Données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ainsi que la loi n°78-17 du 6 janvier 1978 modifiée (ci-après, « *la Réglementation* »).

Au sein de la présente annexe, les termes de « Traitement », « Responsable de traitement », « Sous-traitant », « Violation de Données », « Données à caractère personnel » et « Personne concernée » auront les mêmes définitions que dans la Réglementation.

En cas de contradiction entre le marché et la présente annexe, en matière de Protection des données, l'annexe prévaudra.

II. Description des Traitements et responsabilités

Les Parties seront considérées comme Responsables de traitements distincts pour le(s) traitement(s) suivant(s) :

Finalité n°1: Assurer la signature du présent marché et son suivi administratif

Fondement : Exécution d'un contrat (Article 6.1.B du RGPD)

Personnes concernées : Représentants du titulaire du Marché et de l'Acheteur, signataires du contrat. Catégories de Données : Données d'identification (nom, prénom, fonction, signature). Durées de conservation : 10 ans après la fin du marché

Finalité n°2 : Mise en œuvre d'une assurance dommages aux biens avec risques annexes et flotte automobile. L'Acheteur est responsable des finalités du traitement et le Titulaire est responsable des moyens concourant à la mise en œuvre des prestations objets du marché.

Fondement : Exécution d'un contrat (RGPD Article 6.1.B), Exercice et défense des droits (RGPD Article 9.2.F)

Personnes concernées : Agents, patients Catégories de Données : Identité, situation familiale, économique ou financière, données bancaires, données sensibles concernant la santé

III. Durée de l'Annexe

La présente Annexe entre en vigueur à compter de la signature du marché et restera en vigueur jusqu'à complète destruction des Données dont elle encadre les Traitements.

IV. Obligations du Sous-traitant vis-à-vis du Responsable de traitement(s)

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. Ne pas transférer ou autoriser le transfert de Données hors de l'union européenne, sans accord écrit préalable du Responsable de traitements.

3. Garantir la confidentialité des Données à caractère personnel traitées dans le cadre du présent marché

4. Veiller à ce que les personnels autorisés à traiter les Données à caractère personnel en vertu du présent marché

- s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité,
- reçoivent la formation nécessaire en matière de protection des Données à caractère personnel.

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 ultérieure**

Le Sous-traitant peut faire appel à un autre Sous-traitant (ci-après, « *le Sous-traitant ultérieur* ») pour mener des

activités de Traitements spécifiques. Dans ce cas, il informe préalablement et par écrit le Responsable de traitements 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 ultérieur et les dates du contrat de délégation de gestion de sous-traitance. Le Responsable de traitements dispose d'un délai minium de 1 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 traitements n'a pas émis d'objection pendant le délai convenu.

Le Sous-traitant ultérieur est tenu de respecter les obligations du marché et de la présente annexe, conclues entre les Parties. 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 de la Réglementation. 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 traitements de l'exécution par l'autre Sous-traitant de ses obligations.

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

Il appartient au Responsable de traitements de fournir l'information aux Personnes concernées par les opérations de Traitements au moment de la collecte des Données.

8. **Exercice des droits des personnes**

Dans la mesure du possible, le Sous-traitant doit aider le Responsable de traitements 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@ght-novo.fr

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

Le Sous-traitant notifie au Responsable de traitements toute Violation de Données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance, par courrier électronique à dpo@ght-novo.fr. Cette notification est accompagnée de toute documentation utile afin de permettre au Responsable de traitements, si nécessaire, de notifier cette Violation à la CNIL et aux Personnes concernées.

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 Sous-traitant 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.

En toute hypothèse, le Sous-traitant n'est pas autorisé à notifier directement des Violations de Données à l'autorité de contrôle et aux Personnes concernées, sans accord écrit préalable du Responsable de traitements.

10. **Aide du sous-traitant dans le cadre du respect par le Responsable de traitements de ses obligations**

Le Sous-traitant aide le Responsable de traitements pour la réalisation d'analyses d'impact relatives 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 Responsable de traitements pour la réalisation de la consultation préalable de l'autorité de contrôle en conformité avec les exigences de l'article 36 du règlement européen lorsque cela s'avère nécessaire.

11. **Mesures de sécurité**

Le Sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

- 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 Traitements ;
- 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 ;
- des tests et analyses permettant d'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité des Traitements.

- pour l'hébergement des Données de santé, l'obtention de la certification Hébergement de Données de santé.

12. **Sort des Données**

Au terme de la prestation de services relative aux Traitements des Données, le Sous-traitant s'engage à respecter la décision du Responsable de traitements s'agissant du sort des Données :

- à renvoyer toutes les Données à caractère personnel au Responsable de traitements ou
- à renvoyer les Données à caractère personnel au Sous-traitant désigné par le Responsable de traitements

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 Responsable de traitements 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.

Mail du DPO (ou assimilé) **du Titulaire du marché**

14. **Registre des catégories d'activités de traitement(s)**

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 Traitements effectuées pour le compte du Responsable de traitements comprenant :

- Le nom et les coordonnées du Responsable de traitements pour le compte duquel il agit, des éventuels Sous-traitants et,
- Les catégories de Traitements effectués pour le compte du Responsable de traitements;
- Le cas échéant, les transferts de Données à caractère personnel vers un pays tiers Européen, y compris l'identification de ce pays tiers et 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 Traitements;
  - 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 des Traitements.

15. **Obligation de conseil**

Le Sous-traitant s'engage à conseiller le Responsable de traitement sur l'application de la Réglementation, dès lors qu'il considère qu'une non-conformité peut avoir un impact sur le respect de clauses du marché et de son annexe.

16. **Communication de données à des tiers autorisés**

Le Sous-traitant s'engage à informer sans délai le Responsable de traitements 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 marché et de son annexe.

Le cas échéant, le Sous-traitant s'engage à remettre à son Responsable de Traitement(s), une copie du rapport d'audit de la CNIL.

Dans le cas où la requête est reçue par le Responsable de Traitements, 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.

17. **Engagements relatif aux audits**

Le Sous-traitant s'engage à répondre aux demandes d'audit du Responsable de traitements, 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 Responsable de traitement 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 de l'impossibilité de mettre en œuvre les mesures et s'engage à proposer des mesures palliatives pour réduire les risques encourus.

18. **Obligation de confidentialité**

Le Sous-traitant s'engage à veiller à ce que les personnels autorisés à intervenir sur les moyens de Traitement(s) 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 Responsable de traitements vis-à-vis du Sous-traitant

Le Responsable de traitements s'engage à :

1. fournir au Sous-traitant les Données visées au II des présentes clauses ;

2. documenter par écrit toute instruction concernant le(s) Traitement(s) des Données par le Sous-traitant ;

3. veiller, au préalable et pendant toute la durée du/des Traitement(s), au respect des obligations prévues par le règlement européen sur la protection des Données de la part du Sous-traitant ;

4. superviser le(s) Traitement(s), y compris réaliser les audits et les inspections auprès du Sous-traitant.

Pour le Titulaire du marché

_____

_____

Pour l'Etablissement

M. Alexandre AUBERT
Directeur du GHT NOVO

Fait à Pontoise,

Le ……

Sous-traitants ultérieurs

Tableau à remplir par le Titulaire du marché conformément au IV.6 de l'Annexe.

Nom du Sous-traitant ultérieur	SIREN du Sous-traitant ultérieur	Adresse du sous-traitant ultérieur (rue, ville, pays)	Nom, prénom du représentant du Sous-traitant ultérieur	Traitement sous-traité par le Titulaire du marché	Date de début de sous-traitance ultérieure envisagée	Date et référence du contrat signé entre le Titulaire du marché et le Sous-traitant ultérieur

Toutes les certifications déclarées (HDS, ISO…) devront être adressées à dpo@ght-novo.fr avant le début de la relation contractuelle.

Paraphe du représentant du Titulaire du marché et date ↓