ANNEXE RGPD

Clauses contractuelles de sous-traitance

conformes aux obligations des articles 28 et 30 du règlement européen sur la protection des données.

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 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*** »).

II. 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) décrit dans le présent marché.

III. Durée du contrat

Le présent contrat entre en vigueur à compter de la signature de ce contrat et restera en vigueur aussi longtemps que les deux parties sont liées par le contrat de service ou marché cité à l'article 2.

IV. Obligations du sous-traitant vis-à-vis du responsable de traitement

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'Europe.

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

4. veiller à ce que les **personnels autorisées 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 **responsable de traitement** 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 **responsable de traitement** 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 traitement** n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du **responsable de traitement**. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le **responsable de traitement** de l'exécution par l'autre sous-traitant de ses obligations.

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

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.

8. **Exercice des droits des personnes**

Dans la mesure du possible, le sous-traitant doit aider le **responsable de traitement** à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à rgpd@ght-novo.fr

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

Le sous-traitant notifie au **responsable de traitement** toute violation de données à caractère personnel dans un délai maximum de 4 heures après en avoir pris connaissance et par courrier électronique à rgpd@ght-novo.fr. Cette notification est accompagnée de toute documentation utile afin de permettre au **responsable de traitement**, si nécessaire, de notifier cette violation à la CNIL.

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.

10. **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 (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 traitement** 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 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 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 ;
- des tests et analyses permettant d'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.
- 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 relatifs au traitement des données, le sous-traitant s'engage à respecter la décision du **responsable de traitement** qu'en au sort des données :

- 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.

13. **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.

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 **responsable de traitement** comprenant :

- le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et,
- les catégories de traitements effectués pour le compte du responsable de traitement;
- 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 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 **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 de traitement** ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

16. **Obligation de conseil**

Le sous-traitant s'engage à conseiller le responsable de traitement 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 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 présent contrat.

Dans le cas où la requête est reçue par le responsable de traitement, 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 responsable de traitement, 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

l'impossibilité de mettre en œuvre les mesures et s'engage à proposer des mesures palliatives pour réduire les risques encourus.

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

Le **responsable de traitement** s'engage à :

1. fournir au sous-traitant les données visées au 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.

Pour le Responsable de Traitement, au sein du GHT NOVO (Nord-Ouest Vexin Val-d'Oise)
M. Alexandre AUBERT
Directeur du GHT NOVO