ANNEXE AU CCAP SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

I. Définitions

Les définitions ci-après sont entendues au sens du 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*** »).

- « **Données à caractère personnel** » ou « **Données** » désigne toute information se rapportant à des personnes physiques identifiées ou identifiables (ci-après dénommées les « ***Personnes concernées*** ») ;

- « **Traitement »** ou **« Traitement de Données à caractère personnel** » désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des Données ou des ensembles de Données à caractère personnel ;

- « **Responsable du Traitement** » désigne la Partie qui détermine les finalités et les moyens du Traitement. Il s'agit du pouvoir adjudicateur identifié au présent marché public, c'est-à-dire l'EFS ;

- « **Sous-traitant** » : désigne la Partie qui traite des Données pour le compte, sur instruction et sous l'autorité du Responsable de Traitement. Il s'agit du titulaire du présent marché public.

II. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le Sous-traitant (le titulaire du marché public) s'engage à effectuer pour le compte du Responsable du Traitement (le pouvoir adjudicateur, l'EFS) les opérations de Traitement de Données à caractère personnel définies ci-après pour la réalisation des services tels que décrits dans les pièces du présent marché public.

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 européen sur la protection des données.

III. Description du Traitement faisant l'objet de la sous-traitance

- **Le Sous-traitant est autorisé à traiter pour le compte du Responsable du Traitement les Données à caractère personnel nécessaires pour fournir le service suivant** : le service tel que décrit dans les pièces du marché.

- **La nature des opérations réalisées sur les Données et des données d'activité dans le cadre de la prestation est** : la réception, l'enregistrement des références, le classement, la conservation matérielle, le transport, l'inventaire et le récolement, la recherche et la consultation nécessaires à une demande autorisée, la mise à disposition, le retour, la restitution et la destruction expressément autorisée. La numérisation ou la transmission de copies n'est permise que si elle est prévue au marché et demandée par l'EFS. Aucune extraction du contenu ni constitution de base secondaire n'est autorisée pour les besoins propres du Sous-traitant.
-

- **Les Données à caractère personnel traitées sont** :
- les références et descriptions documentaires nécessaires à la gestion des fonds, les informations contenues dans les documents effectivement confiés, ainsi que les identifiants professionnels, coordonnées et traces d'action des agents habilités à demander ou gérer les prestations. La liste exacte des catégories documentaires et des données, notamment données de santé, est contenue dans l'inventaire transmis. Les inventaires doivent éviter les données nominatives ou médicales inutiles à la localisation des archives.

- **Les catégories de Personnes concernées sont notamment** : salariés, donneurs, receveurs,fournisseurs, candidats à l'emploi, stagiaires et intérimaires, alternants

- Pour l'exécution de la prestation, le Responsable du Traitement met à la disposition du Sous-traitant les informations nécessaires sur les Personnes concernées.

- **Les Données à caractère personnel seront conservées pour** : la durée du marché public telle que définie dans le CCAP puis seront rendues par le Sous-traitant à l'EFS tel que prévu à l'article XI.

IV. Obligations du Sous-traitant vis-à-vis du Responsable du 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. Traiter les Données **conformément aux instructions documentées** du Responsable du Traitement. 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 du 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 contrat ;
4. Veiller à ce que les **personnes 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**

Le Sous-traitant peut désigner un Sous-traitant (ci-après un « Sous-traitant ultérieur ») pour traiter les Données :

- Sous réserve du consentement écrit préalable du Responsable du Traitement après que le Sous-traitant lui a fourni l'ensemble des informations concernant d'une part l'identité de ce Sous-traitant ultérieur et d'autre part les activités de Traitement qu'il effectuera ;

- A condition que le Sous-traitant ait conclu un contrat avec ledit Sous-traitant ultérieur avant que ce dernier ne transfère ou n'accède à des Données, et que ce contrat avec le Sous-traitant ultérieur contienne des obligations relatives au Traitement qui sont les mêmes que celles énoncées dans la présente Convention ; et

- A condition que le Sous-traitant veille à ce que le Sous-traitant ultérieur respecte les obligations en matière de protection des Données et de confidentialité, énoncées dans le présent article.

VI. Droit d'information des Personnes concernées

Il appartient au Responsable du Traitement / ou au Sous-traitant de fournir l'information aux Personnes concernées par les opérations de Traitement au moment de la collecte des Données.

VII. Exercice des droits des Personnes concernées

Dans la mesure du possible, le Sous-traitant doit aider le Responsable du 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) et droit d'introduire une réclamation auprès de l'autorité de contrôle (la CNIL).

Dans le cas où la requête est reçue par le Responsable des Traitements, le Sous-traitant s'engage à mettre en œuvre les moyens permettant de répondre à la demande dans les délais exigés par la réglementation en vigueur sur le périmètre des opérations de Traitement sous-traitées.

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 l'adresse suivante : Efs.Dpo@efs.sante.fr

Le Sous-traitant s'engage à aider le Responsable des Traitements lors du Traitement d'une réclamation d'une personne concernée et s'engage à mettre en œuvre les moyens permettant de traiter les demandes dans le délai de 1 mois imposé par le Règlement Général de Protection des Données.

Dans le cas où le Sous-traitant ne serait pas en capacité de fournir les éléments permettant au Responsable des Traitements de respecter le délai de 1 mois, il s'engage à fournir les justificatifs permettant au Responsable des Traitements d'informer le demandeur sur les difficultés rencontrées et il s'engage à mettre en œuvre les moyens pour traiter les demandes dans un délai maximum de 50 jours après la première sollicitation.

VIII. Notification des violations de Données à caractère personnel

Le Sous-traitant notifie au Responsable du Traitement toute violation de Données à caractère personnel dans un délai maximum de quarante-huit (48) heures après en avoir pris connaissance et par mail à l'adresse suivante : Efs.Dpo@efs.sante.fr.

Cette notification est accompagnée de toute documentation utile afin de permettre au Responsable du Traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

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.

IX. Aide du Sous-traitant dans le cadre du respect par le Responsable du Traitement de ses obligations

Le Sous-traitant s'engage à conseiller le Responsable des Traitements sur l'application du règlement européen sur la protection des Données dès lors qu'il considère qu'une non-conformité peut avoir un impact sur la vie privée des Personnes concernées.

Le Sous-traitant aide le Responsable des Traitements pour la réalisation d'analyses d'impact relatives à la protection des Données rendues obligatoires lorsqu'un type de Traitement est susceptible de présenter un risque élevé pour les droits et libertés des Personnes concernées.

Le Sous-traitant aide le Responsable des Traitements pour la réalisation de la consultation préalable de l'autorité de contrôle lorsque l'analyse d'impact susmentionnée indique que le Traitement pourrait présenter un risque élevé si le responsable des Traitements ne prend pas de mesures nécessaires pour atténuer ce risque.

X. Mesures de sécurité

Le Sous-traitant aide le Responsable des Traitements à garantir ses obligations en matière de sécurité des Données à caractère personnel.

Si la prestation concerne les systèmes d'information de l'EFS, le Sous-traitant s'engage à mettre en œuvre les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque telles que détaillées dans les exigences de Sécurité des Systèmes d'Information (SSI) de l'EFS.

A défaut, le Sous-traitant s'engage à mettre en œuvre les mesures techniques et organisationnelles suivantes garantissant un niveau de sécurité adapté au risque telles que détaillées dans l'offre du titulaire.

A titre d'exemple :

- *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.*

XI. Sort des Données à l'issue du contrat

Au terme du marché public, le Sous-traitant s'engage à envoyer toutes les Données au Responsable des 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.

XII. Délégué à la protection des Données

Pour toute demande concernant les Traitements des Données personnelles, le Responsable de Traitement peut adresser une demande par email au Délégué à la Protection des Données (Data Protection Officer) adresse du DPO du prestataire :

……

Le caractère confidentiel des informations transmises à l'EFS par les candidats à la présente consultation, quelles qu'en soient la nature et la forme, sera strictement préservé. Seules les personnes de l'EFS habilitées à les traiter dans le cadre de la procédure de marché public en cours en auront connaissance. L'EFS s'engage à n'utiliser les informations qu'en vue de l'analyse de la candidature et de l'offre soumises et s'engage à ne pas les divulguer, à ne pas les communiquer à des tiers, à l'exception de ses autorités de contrôle, à ne pas les publier, ni à les rendre publiques de quelque manière que ce soit, sauf pour satisfaire l'obligation d'information posée par les articles R.2181-1 et suivants qui s'exerce conformément aux modalités rappelées par l'article L.2132-1 du code de la commande publique.

Il est toutefois précisé que, en ce qui concerne le marché public qui sera signé, celui-ci et les pièces s'y rapportant deviendront des documents administratifs communicables sur le fondement du code des relations entre le public et l'administration, le droit de communication des tiers s'exerçant cependant dans le respect du secret des affaires conformément au code précité.

Les données à caractère personnel des candidats et des soumissionnaires font l'objet de traitements par l'EFS, en tant que responsable de traitement, et dont le siège se situe 20 avenue du Stade France, 93218 La Plaine Saint-Denis Cedex. Ces traitements sont destinés à permettre l'analyse des candidatures et des offres, ainsi que le contact des candidats pendant la passation du marché public.

Les données personnelles sont conservées pendant une durée maximale de dix ans à compter de la signature du marché public. Seules les personnes autorisées dans le cadre de l'exercice de leurs fonctions ont accès aux données collectées.

Conformément aux lois et règlements en vigueur en matière de protection des données, et à condition de justifier de leur identité, les candidats et les soumissionnaires bénéficient d'un droit d'accès, de rectification, d'effacement, de limitation, ainsi que du droit à la portabilité de leurs données. Enfin, les candidats et les soumissionnaires disposent du droit d'introduire une réclamation auprès de Commission Nationale Informatique et Libertés (CNIL).

Ils peuvent exercer leurs droits auprès de l'EFS en s'adressant à stde.marches.publics@efs.sante.fr

L'EFS a désigné un délégué à la protection des données ou DPO - que les candidats et les soumissionnaires peuvent contacter en envoyant un message à l'adresse suivante : efs.dpo@efs.sante.fr

Si l'EFS est dans l'impossibilité de faire droit à leur demande, il motivera sa décision et les informera dans les meilleurs délais.

XIII. Registre des catégories d'activités de Traitement

Le Sous-traitant déclare **tenir par écrit et communiquer au Responsable du Traitement sur demande, un registre** de toutes les catégories d'activités de Traitement effectuées pour le compte du Responsable du Traitement comprenant :

- Le nom et les coordonnées du Responsable du Traitement pour le compte duquel il agit, des éventuels Sous-traitants ultérieurs et, le cas échéant, du délégué à la protection des Données du Sous-traitant ;
- 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 qui seront à fournir par le Sous-traitant et joints au présent contrat ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles telles que définies au point X ci-avant.

XIV. Documentation

Le Sous-traitant met à la disposition du Responsable du 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.

XV. Obligations du Responsable du Traitement vis-à-vis du Sous-traitant

Le Responsable du Traitement s'engage à :

1. Fournir au Sous-traitant les Données visées au III des présentes clauses ;
2. Documenter par écrit les instructions essentielles 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.