**Marché N°2025-13**

**OBJET DU MARCHE**

**PRESTATIONS DE MEDECINE DU TRAVAIL (GROUPEMENT DE COMMANDES HAUTE AUTORITE DE SANTE, ETABLISSEMENT FRANÇAIS DU SANG-SIÈGE ET AGENCE DE BIOMEDECINE)**

**ANNEXE 1 AU CAHIER DES CLAUSES ADMINISTRATIVES PARTICULIÈRES**

**Clauses contractuelles prises en application du règlement européen sur la protection des données (RGPD)**

La présente annexe comprend 6 pages numérotées de 1 à 6.

Entre

**La Haute Autorité de santé (HAS)**

5, Avenue du Stade de France – Immeuble Green Corner - 93218 Saint-Denis La Plaine Cedex

représentée par Monsieur le Professeur Lionel COLLET, son Président,

**L’Agence de la Biomédecine (ABM)**

1 avenue du Stade de France - 93212 Saint-Denis La plaine

Représentée par Madame Marine JEANTET, sa directrice générale,

**L’Etablissement Français du Sang (EFS)** **- Siège**

20 avenue du Stade de France - 93218 SAINT DENIS Cedex

Représenté par Monsieur Frédéric PACOUD, son Président,

Ci-après dénommés« le pouvoir adjudicateur »,

D’une part,

Et

**La société XXXX**

Située

Représentée par

Ci-après « le Responsable de traitement »

D’autre part,

1. ***Définitions***

Les termes utilisés sont entendus au sens du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

1. ***Objet***

Le Titulaire, en sa qualité de service de santé au travail, agit en tant que **Responsable de traitement** au sens du Règlement (UE) 2016/679 (ci-après, « ***le règlement européen sur la protection des données*** ») pour les données à caractère personnel qu’il collecte et traite dans le cadre de l’exécution du présent marché.

Le pouvoir adjudicateur n’a pas accès aux données de santé des agents et n’intervient pas dans la détermination des finalités ou des moyens du traitement.

Cette annexe définit les conditions dans lesquelles le Titulaire s'engage à traiter les données à caractère personnel des agents ou salariés du pouvoir adjudicateur dans le cadre de la réalisation des prestations de santé au travail.

1. ***Description des données à caractère personnel concernées par le marché***

Les données à caractère personnel traitées dans le cadre du présent marché sont : les données d’identification (nom, prénom, date de naissance, numéro de sécurité sociale, numéro de téléphone, adresses email personnel et professionnel, etc.), les données de santé (antécédents médicaux, résultats de visites médicales et d'examens, diagnostics, traitements, etc.), les données professionnelles (poste occupé, conditions de travail, expositions à des risques professionnels, etc.).

1. ***Description du traitement mis en œuvre dans le cadre des prestations***

Dans le cadre des prestations, le Titulaire met en œuvre un traitement de données à caractère personnel en conformité avec la règlementation applicable, selon ses propres modalités.

1. ***Finalités du traitement envisagé***

La ou les finalité(s) du traitement faisant l’objet du présent marché sont les suivants : l’organisation et le suivi des visites médicales obligatoires (embauche, périodiques, de reprise, etc.), la réalisation des examens médicaux et des évaluations de santé des collaborateurs, la surveillance de la santé des collaborateurs et la prévention des risques professionnels, la gestion des dossiers médicaux et des historiques de santé des collaborateurs.

Les finalités peuvent être précisées par le Titulaire dans son offre.

1. ***Durée du traitement***

Les données à caractère personnel seront traitées pour la durée nécessaire à la réalisation des prestations de médecine du travail, conformément aux obligations légales et réglementaires applicables. À la fin des prestations, les données seront supprimées, sauf si leur conservation est imposée en vertu du droit de l’Union ou du droit national, il doit informer le pouvoir adjudicateur de cette obligation juridique avant le début des prestations.

1. ***Obligations du Titulaire***

Le Titulaire s’engage à :

1. Fournir des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles de sécurité telles que requises par le règlement européen sur la protection des données .
2. Informer immédiatement le pouvoir adjudicateur en cas de violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l’Union ou du droit national relatif à la protection des données. Le pouvoir adjudicateur se tient à disposition pour accompagner le Titulaire dans la communication aux personnes concernées, en cas de violation de données à caractère personnel. En outre, si le Titulaire 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 pouvoir adjudicateur 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 marché.

Le Titulaire s'engage à garantir la confidentialité des données de santé des collaborateurs. Les données collectées et traitées dans le cadre des prestations de médecine du travail sont soumises au secret médical et ne peuvent être communiquées à des tiers sans le consentement des personnes concernées, sauf obligation légale.

1. Veiller à ce que les **personnes autorisées 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 ;

1. Mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris 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 au sens du code de la commande publique :

Si le Titulaire souhaite recruter un sous-traitant dans les conditions des articles L. 2193-1 et suivants du code de la commande publique pour l’exécution d’une partie des prestations du marché impliquant un traitement des données à caractère personnel décrites à l’article 2, tel que décrit à l’article 3, il devra au préalable recueillir l’autorisation écrite du représentant du pouvoir adjudicateur. En amont de cette autorisation, le Titulaire indiquera clairement au pouvoir adjudicateur les activités de traitement qui seraient sous-traitées, l’identité et les coordonnées du sous-traitant et la durée envisagée pour la sous-traitance.

Dans ce cas, le sous-traitant du Titulaire sera soumis aux mêmes obligations que le Titulaire en matière de protection de données, en particulier pour ce qui est de présenter des 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 RGPD.

Dans l’hypothèse où le sous-traitant du Titulaire ne remplissait pas ses obligations en matière de protection des données, le Titulaire demeurerait pleinement responsable auprès du pouvoir adjudicateur de l’exécution des missions qui lui sont attribuées dans le cadre du présent marché.

Le Titulaire pourra transférer les données à caractère personnel au sous-traitant du Titulaire pour les besoins de la fourniture des traitements, dans les conditions suivantes :

* Le Titulaire tient une liste à jour de ses sous-traitants au sens de la commande publique auxquels il transfère les données à caractère personnel et met en œuvre un mécanisme de notification des nouveaux sous-traitants au sens de la commande publique ;
* Le Titulaire garantit que chaque sous-traitant au sens de la commande publique amené à traiter des données à caractère personnel dans le cadre de l’exécution du marché :
  + fournisse des garanties suffisantes en matière de mesures techniques et organisationnelles exigées par la Réglementation sur la protection des données à caractère personnel ;
  + s'engage à une obligation de confidentialité dont le niveau de garantie ne pourrait être inférieur à celui des présentes ;
  + cesse immédiatement le traitement de ces données à caractère personnel si une telle garantie n’était plus assurée.

1. Droit d’information des personnes concernées :

Il appartient au Titulaire, responsable de traitement, d’informer les personnes dont les données à caractère personnel sont traitées dans le cadre du présent marché de leurs droits et cela, dès la collecte de ces données.

Les catégories de personnes concernées sont tous les agents permanents et les salariés de la HAS, de l’EFS et de l’ABM.

1. Droit des personnes concernées :

Le Titulaire doit 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.

Le Titulaire indique dans son offre les modalités d’exercice des droits (adresse courrier électronique, courrier postal).

1. Notification des incidents de sécurité :

Le Titulaire notifie au pouvoir adjudicateur tout incident de sécurité dans un délai de 48 heures après en avoir pris connaissance, par courrier électronique à :

* pour la HAS : [dpo@has-sante.fr](mailto:dpo@has-sante.fr) et [securiteSI@has-sante.fr](mailto:securiteSI@has-sante.fr)
* pour l’EFS : [efs.dpo@efs.sante.fr](mailto:efs.dpo@efs.sante.fr)
* pour l’ABM : [dpo@biomedecine.fr](mailto:dpo@biomedecine.fr) et [securiteSI@biomedecine.fr](mailto:securiteSI@biomedecine.fr)

La notification devra décrire : a) la nature et les conséquences de la violation de données à caractère personnel, b) les mesures prises ou que le Titulaire propose de prendre pour remédier à la violation de données à caractère personnel, c) toute personne auprès de qui des informations complémentaires pourront être obtenues, d) l’heure de la découverte de la violation de données à caractère personnel, e) tout autre information liée à la violation de données à caractère personnel raisonnablement demandée par le pouvoir adjudicateur, f) si possible les catégories et le nombre approximatif de personnes concernées et le nombre approximatif d'enregistrements de données à caractère personnel concernés.

Le Titulaire devra prendre, dans les meilleurs délais, toutes les mesures pour cesser ou contenir l’exposition des données à caractère personnel sur les équipements et/ou dans les locaux du Titulaire et tient le pouvoir adjudicateur informé de l’état de la violation de données à caractère personnel et de toutes autres questions connexes, sans préjudice des droits du pouvoir adjudicateur.

En tant que responsable du traitement des données, le Titulaire du marché procèdera à la notification CNIL de la violation de données à l’autorité de contrôle compétente et le cas échéant aux personnes concernées.

1. Mesures de sécurité :

Le Titulaire met en œuvre toutes les mesures techniques et organisationnelles nécessaires pour assurer la sécurité et la confidentialité des données, conformément aux dispositions du règlement européen sur la protection des données. Il décrit dans son offre les dispositions prises à cet égard, notamment pour les modalités d’authentification et pour les conditions d’hébergement des données.

Le Titulaire s’engage à :

* Prendre toutes mesures permettant d’éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d’exécution du contrat ;
* Mettre en œuvre les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
* Mettre en œuvre 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 ;
* Mettre en œuvre une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ;
* Mettre en œuvre les mesures de sécurité adaptées prévues par les documents du marché.
* Respecter les avis et les recommandations de la CNIL, notamment ceux qui concernent les règles de sécurité et de gestion applicables, en particulier, aux données archivées.

1. Délégué à la protection des données :

Le Titulaire communique au pouvoir adjudicateur **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.

1. Registre des catégories d’activités de traitement :

Le Titulaire déclare **tenir par écrit un registre** de toutes les catégories d’activités de traitement.

1. Documentation :

Le Titulaire met à la disposition du pouvoir adjudicateur la **documentation nécessaire pour démontrer le respect de toutes ses obligations**.

1. Données des salariés :

Dans le cadre de l'exécution du présent marché public, les parties peuvent également être amenées à traiter des données à caractère personnel de certaines catégories de personnes travaillant pour chacune d'elles ayant pour finalité la gestion de la relation et la communication que cette relation induit. Ce traitement est fondé sur l'intérêt légitime de chacune des parties, celui-ci étant nécessaire à la bonne exécution de la relation contractuelle. Les données sont conservées pendant la relation contractuelle augmentée du délai de prescription.

Les données sont destinées aux services compétents de chacune des parties, ainsi qu'aux éventuels sous-traitants auxquels elles pourraient avoir recours. Les collaborateurs de chacune des parties disposent d'un droit d'accès, de rectification, d'effacement ou de portabilité de leurs données, du droit de s'opposer ou de solliciter la limitation du traitement, dans les conditions et limites prévues par la réglementation. Pour exercer ces droits, ils peuvent contacter chacune des parties aux coordonnées figurant au contrat. Ils peuvent introduire une réclamation auprès de la CNIL. Il revient à chacune des parties d'informer ses collaborateurs en conséquence.