CAHIER DES CLAUSES ADMINISTRATIVES PARTICULIERES

ANNEXE 2 – CLAUSES RELATIVES A LA PROTECTION DES DONNEES

Etabli en application des articles L2123-1 2°, R2123-1 3°, R2123-4 à R2123-7 (Marchés de services sociaux et autres services spécifiques passés selon une procédure adaptée), L2125-1, R2161-1 à R2162-6, R2162-13 et R2162-14 (Accord-cadre à bons de commande) du Code de la commande publique

Etablissement partie bénéficiaire :

Centre hospitalier de Belle-Ile-en-Mer

Objet du marché public :

REALISATION D'EXAMENS DE BIOLOGIE MEDICALE

PREAMBULE. DEFINITIONS

Données à caractère personnel :	toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement, pseudonymisée ou non.
Données sensibles :	toute information qui révèle la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique.
Traitement :	toute opération ou tout ensemble d'opérations effectué à l'aide de procédés automatisés ou non et appliqué à des données ou des ensembles de données à caractère personnel, pseudonymisée ou non telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.
Responsable du Traitement :	le représentant de l'Etablissement partie concerné
Sous-Traitant :	le Titulaire du marché public qui traite des Données à caractère personnel pour le compte du Responsable du traitement.
Sous-traitant ultérieur :	tout opérateur économique auquel le Sous-traitant fait appel pour traiter des Données à caractère personnel dans le cadre de l'exécution du marché public. Le Sous-Traitant s'assure que ses Sous-traitants ultérieurs respectent les clauses prévues.

Tout partenaire du Responsable du Traitement entrant dans le champ d'application des présentes définitions est ainsi amené à se voir appliquer les clauses suivantes. Ceci inclut *de facto* les opérations de maintenance effectuées par des tiers pour le compte du Responsable du Traitement, le mainteneur étant amené à réaliser un Traitement de Données à caractère personnel au sens des précédentes définitions.

Les présentes clauses ont également vocation à s'appliquer aux prestations d'hébergement de données de santé. A ce titre, et conformément à l'article L. 1111-8 du Code de la santé publique, tout Sous-Traitant (ou Sous-traitant ultérieur) hébergeant des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de l'Etablissement partie concerné doit avoir obtenu la certification Hébergeur de données de santé.

ARTICLE 1. 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 du 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*** » ou « ***le RGPD*** »).

ARTICLE 2. 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 ou les service(s) objet du marché public.

Les opérations réalisées sur les données sont conformes aux stipulations suivantes :

- La finalité du Traitement, les Données à caractère personnel traitées et les catégories de personnes concernées sont conformes à l'objet du contrat.

- Pour l'exécution du service objet du présent contrat, le Responsable du Traitement met à la disposition du Sous-Traitant les informations nécessaires.

ARTICLE 3. OBLIGATIONS DU SOUS-TRAITANT VIS-A-VIS DU RESPONSABLE DU TRAITEMENT

Le Sous-Traitant s'engage à :

1. Traiter les données uniquement pour la seule finalité qui fait/font l'objet de la sous-traitance.

2. Traiter les données conformément aux mesures de sécurité décrites au paragraphe 12 du présent article.

   Si le Sous-Traitant considère qu'une instruction constitue une violation du RGPD 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. Le Responsable du Traitement dispose d'un délai minimum d'un mois et maximum deux mois à compter de la date de réception de cette information pour présenter ses objections.

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

4. S'interdire de :

   - Traiter et/ou consulter les Données à caractère personnel à d'autres fins que l'exécution des prestations qu'il effectue pour le Responsable du Traitement au titre du marché public (même si l'accès à ces données est techniquement possible) ;
   - Divulguer, sous quelque forme que ce soit, tout ou partie des Données à caractère personnel traitées, anonymisées ou non ;
   - Prendre copie ou stocker, quelles qu'en soient la forme et la finalité, tout ou partie des informations ou Données à caractère personnel contenues sur les supports ou documents qui lui ont été confiés ou qu'il a recueillis en cours d'exécution du Contrat, en dehors des cas couverts par les présentes.

5. Veiller à ce que les personnes autorisées à traiter les Données à caractère personnel en vertu du présent marché public :

   - 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.

6. 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.

7. Sous-traitance ultérieure :

   Le Sous-Traitant peut faire appel à un autre Sous-Traitant pour mener des activités de Traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le Responsable du 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 du Traitement dispose d'un délai maximum de deux (2) mois à compter de la date de réception de cette information pour présenter ses objections.

   Le Sous-Traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du Responsable du 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 du Traitement de l'exécution par l'autre Sous-Traitant de ses obligations.

8. Droit d'information des personnes concernées :

   Il appartient au Responsable du Traitement de fournir l'information aux personnes concernées par les opérations de Traitement au moment de la collecte des données si le traitement le requiert.

9. Exercice du droit des personnes concernées :

   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 conformément à la loi relative aux droits des malades et à la qualité du système de santé 2002 n°2002-303 4 mars 2002, 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 au délégué à la protection des données du Responsable du Traitement par mail à dpo@ghba.fr avant d'y donner suite.

10. Notification des violations de Données à caractère personnel :

    Le Sous-Traitant notifie au délégué à la protection des données du Responsable du Traitement toute violation de Données à caractère personnel dans les plus brefs délais (maximum de 72 heures) après en avoir pris connaissance et par tout moyen permettant de donner date certaine. 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 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.

    Cette notification est a adressée au minimum aux adresses suivantes :

    - dpo@ghba.fr
    - rssi@ghba.fr

11. Aide du Sous-Traitant dans le cadre du respect par le Responsable du Traitement de ses obligations :

    Le Sous-Traitant aide le Responsable du Traitement pour la réalisation d'analyses d'impact (AIPD / PIA) relative à la protection des données.

    Le Sous-Traitant aide le Responsable du Traitement pour la réalisation de la consultation préalable de l'autorité de contrôle si cela est requis.

12. Hébergement des données :

    Le sous-traitant s'engage à héberger les données de santé concernées par la présente consultation conformément à la réglementation, chez un hébergeur de données de santé (HDS) certifié ou agréé.

    Le sous-traitant fournira avant la mise en œuvre du traitement de la preuve de la certification HDS du serveur sur lequel les données seront stockées.

13. Mesures de sécurité :

Le Sous-Traitant s'engage à mettre en œuvre les mesures de sécurité décrites infra et conformément aux principes de base suivants :

- La pseudonymisation et le chiffrement des Données à caractère personnel selon la criticité des données convenue avec le Responsable du Traitement ;
- 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 périmètre de responsabilité du Sous-Traitant intègre tous les composants et services permettant la réalisation de l'objet du marché public
Le Sous-Traitant s'engage spécifiquement à respecter l'ensemble des obligations de sécurité (notamment imposées par l'article 32 du RGPD) dans le traitement des données personnelles opérées pour le compte du Responsable du Traitement.
Le Sous-Traitant s'engage à mettre en œuvre les mesures de sécurité recommandées par l'ANSSI :

Mesures de sécurité et sûreté physique :

- Contrôle d'accès physique aux locaux, sécurité des accès, sécurité électrique et système de climatisation, etc.).

Mesures nécessaires pour assurer l'intégrité et la confidentialité des données :

- Règlement pour la gestion des privilèges (attribution de droits, de droits spéciaux, révocation des autorisations, contrôles réguliers).
- Politique de mots de passe (mots de passe forts, renouvellement et contrôles réguliers).
- Authentification des utilisateurs distants (processus de chiffrement, identification des terminaux, solutions VPN).
- Chiffrement des données et procédés garantissant ainsi que le prestataire n'a pas accès aux données qui lui sont confiées.

Mesures nécessaires pour garantir la disponibilité et la résilience constantes des systèmes et des services de traitement :

- Politique de sauvegarde : sauvegardes régulières et Systèmes de protection des bases de données.
- Réplication des données.
- Traçabilité.

Mesures de sécurité logique :

- Protection du réseau (pare-feu, antivirus, détection d'intrusion, contrôle du cloisonnement).
- Gestion des mises à jour et sécurité des développements applicatifs.

Les mesures techniques et organisationnelles doivent être conformes à l'état de l'art et aux évolutions techniques. Le prestataire sous-traitant devra tenir à la disposition de l'Etablissement partie du GHBA concerné par le présent marché public le détail des mesures mises en place.

14. Sort des Données personnelles et réversibilité :

Au terme du contrat, le sous-traitant s'engage à détruire, dans les deux mois, toutes les données y compris celles qui seraient anonymisées ou pseudonymisées sauf réversibilité demandée par le Responsable du Traitement. A l'issue de la réversibilité, l'ensemble de données seront détruites.
Au terme du contrat, le sous-traitant s'engage à fournir les données nécessaires au Responsable du Traitement pour couvrir ses obligations légales (données, traces fonctionnelles…) dans un format interopérable et réutilisable.

15. Délégué à la protection des données :

    Le Sous-Traitant communique au Responsable du 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.
    Le délégué à la protection des données du Responsable des traitements peut être contacté à l'adresse : dpo@ghba.fr

16. Registre des catégories d'activités de Traitement :

    Le Sous-Traitant déclare tenir par écrit 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 et, le cas échéant, du délégué à la protection des données ;
    - 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 ;
    - 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.

17. Flux transfrontaliers de Données à caractères personnelles :

    En cas de transfert de Données à caractère personnel vers un pays tiers, n'appartenant pas à l'Union Européenne, ou vers une organisation internationale, le Sous-Traitant doit obtenir l'accord préalable écrit du Responsable du Traitement. Si cet accord est donné, le Sous-Traitant s'engage à coopérer avec le Responsable du Traitement afin d'assurer :

    - Le respect des procédures permettant de se conformer à la Loi, par exemple dans le cas où une autorisation de la part de la CNIL apparaîtrait nécessaire ;
    - Si besoin, la conclusion d'un ou plusieurs contrats permettant d'encadrer les flux transfrontaliers de Données à caractère personnel. Le Sous-Traitant s'engage en particulier, si nécessaire, à signer de tels contrats avec le Responsable du Traitement et/ou à obtenir la conclusion de tels contrats par ses Sous-Traitants Ultérieurs. Pour ce faire, il est convenu entre les Parties que les clauses contractuelles types publiées par la Commission Européenne seront utilisées pour encadrer les flux transfrontières de Données à caractère personnel.

18. Documentation et audit :

    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.

    Le Sous-Traitant fournit l'analyse d'impact (AIPD / PIA) concernant le dispositif si celle-ci est requise ou a minima les éléments pour permettre au Responsable du Traitement de réaliser celle-ci.

ARTICLE 4. OBLIGATIONS DU RESPONSABLE DE TRAITEMENT VIS-A-VIS DU SOUS-TRAITANT

Le Responsable du Traitement s'engage à :

1. Fournir au Sous-Traitant les données prévues dans le marché public ;
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.