

Les obligations des parties vis-à-vis de la sécurité informatique et du règlement européen sur la protection des données

I. OBLIGATIONS DU TITULAIRE VIS-A-VIS DES ETABLISSEMENTS DU GHT SLS

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le titulaire s'engage à effectuer pour le compte des établissements du GHT SLS 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 »).

Le titulaire du marché s'engage à :

1. Traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet du marché ;
2. Traiter les données conformément aux instructions documentées des établissements du GHT SLS, afin de fournir les services et remplir ces obligations. Si le titulaire du marché 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 les établissements concernés du GHT SLS, le Délégué à la Protection des Données (DPO), le Responsable de la Sécurité des Systèmes d'Information (RSSI) et le Responsable Système de Management de la Sécurité de l'Information (RSMSI) du GHT Somme Littoral Sud. 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 les établissements concernés du GHT SLS, ainsi que le DPO, le RSSI et le RSMSI du GHT 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 sécurité et la confidentialité** des données à caractère personnel traitées dans le cadre du présent contrat notamment par la mise en oeuvre de mesures techniques et organisationnelles permettant d'assurer la protection des données personnels. Le niveau de sécurisation peut toutefois varier en fonction de la nature des données, en particulière si le titulaire du marché est amené à faire transiter et à stocker des données sensibles ;
4. Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent marché :
 - a. S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
 - b. 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 titulaire est autorisé à faire appel à un « sous-traitant ». Le titulaire devra dans la déclaration de sous-traitance décrire les activités de traitement sous traitées. Le titulaire doit recueillir l'autorisation écrite, préalable et spécifique du GHT SLS.
Le sous-traitant est tenu de respecter les obligations du présent marché pour le compte et selon les instructions des établissements du GHT SLS. Il appartient au titulaire du marché de s'assurer que le sous-traitant présente les mêmes garanties suffisantes quant à la mise en oeuvre 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 ne remplit pas ses obligations en matière de protection des données, le titulaire du marché demeure pleinement responsable devant le GHT SLS.

7. **Exercice des droits des personnes** : Dans la mesure du possible, le titulaire doit aider le GHT SLS 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 exclusivement fondée sur un traitement automatisé, y compris le profilage.
Notamment lorsque les personnes concernées exercent auprès du titulaire du marché des demandes d'exercice de leur droit, le titulaire s'engage à communiquer les coordonnées du DPO et/ou DIM dans les plus brefs délais à la personne qui en a fait la demande. Dans le cadre de la bonne gestion des droits des personnes, le titulaire s'engage concomitamment à informer dans les plus brefs délais le DPO de toutes demandes (concernant les articles 15 à 22 du RGPD) qui seraient directement exercées auprès de lui.
8. **Notification des incidents de sécurité** : Le titulaire du marché s'engage à alerter les établissements concernés, le DPO, le RSSI et le RSMSI du GHT SLS de tout incident de sécurité dès que possible et dans un délai maximum de 24 heures après en avoir pris connaissance et par le moyen suivant : téléphone 03.22.08.80.00 ou mail dpo@chu-amiens.fr. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cet incident à l'autorité de contrôle compétente.
9. **Notification des violations de données à caractère personnel** : Le titulaire du marché notifie aux établissements concernés, le DPO, le RSSI et le RSMSI du GHT SLS de toute violation de données à caractère personnel dès que possible et dans un délai maximum de 24 heures après en avoir pris connaissance et par le moyen suivant : téléphone 03.22.08.80.00 ou mail dpo@chu-amiens.fr. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Pour information, la notification auprès de l'autorité de contrôle relevant de la responsabilité du responsable de traitement 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 DPO 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 les établissements du GHT SLS proposent 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.

Lorsque la violation est susceptible d'engendrer un risque concernant les droits et libertés d'une personne physique, l'établissement concerné, le DPO, le RSSI et le RSMSI communiquent la violation de données à caractère personnel dans les plus brefs délais.

Pour information, la communication à la personne concernée, relevant de la responsabilité du responsable de traitement, décrit en des termes clairs et simples, la nature de la violation de données à caractère personnel et 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 DPO 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 les établissements du GHT SLS proposent 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.

10. Aide et coopération du titulaire dans le cadre du respect par le GHT SLS de ses obligations :

La coopération portera sur :

- La détermination des données utiles au titulaire pour l'exécution de ses prestations ;
- La tenue et la mise à jour de leurs registres respectifs ;
- L'élaboration de réponses à fournir à l'autorité de contrôle qui ferait un contrôle ou demanderait des informations sur les mesures techniques et organisationnelles mises en place pour éviter les atteintes aux droits et libertés individuelles ;
- Faire cesser tout trouble en cas de détection d'une violation de données à caractère personnel ;
- La gestion d'une procédure judiciaire ;
- Effectuer des analyses d'impact, le cas échéant.

Les parties s'engagent à se communiquer toutes informations dont elles auraient connaissance et qui auraient un impact sur l'exécution des prestations objet du marché.

Les parties s'engagent à coopérer de façon loyale et constructive en vue de la résolution de toute difficulté liée aux données personnelles.

11. Audit : Le titulaire s'engage à se conformer aux demandes des établissements du GHT SLS ou des auditeurs qu'il aurait mandatés afin :

- D'accéder à ou d'inspecter les locaux, les systèmes d'information, les registres ainsi que tout document et information,
- D'interroger le personnel du prestataire, et ce afin de permettre aux établissements du GHT SLS d'auditer et de vérifier que le prestataire et ses sous-traitants ultérieurs respectent pleinement les dispositions du RGPD.

Les frais de l'audit sont à la charge de ou des établissement(s) demandeur(s) du GHT SLS.

Par exception à ce qui précède, si l'audit révèle des manquements du titulaire à ses obligations, le titulaire rembourse les établissements demandeurs du GHT SLS des frais de l'audit, sans préjudice de toute indemnisation qui pourra être réclamée par le ou les établissement(s) demandeur(s) du GHT SLS.

Le titulaire s'assure que le contrat conclu avec ses sous-traitants permet aux établissements du GHT SLS de procéder ou de faire procéder aux audits prévus au présent article, chez son titulaire du marché et ses propres sous-traitants.

12. Mesures de sécurité : Le titulaire s'engage à mettre en œuvre les mesures de sécurité suivantes :

- 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 ;

Le titulaire s'engage à respecter la Politique de Sécurité des Systèmes d'Informations (PSSI) du ou des établissements concerné(s).

13. **Sort des données** : Au terme de la prestation de services relatifs au traitement de ces données, le titulaire et ses sous-traitants s'engagent à renvoyer toutes les données à caractère personnel aux établissements concernés du GHT SLS.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du titulaire. Une fois détruites, le titulaire doit justifier par écrit de la destruction.

A noter qu'au terme de la prestation de services, le titulaire peut être tenu pénalement responsable à raison des prestations sous-traitées.

14. **Délégué à la protection des données** : Le titulaire communique 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.

15. **Registre des catégories d'activités de traitement** : Le titulaire déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte des établissements concernés du GHT SLS comprenant :

- Le nom et les coordonnées des établissements concernés du GHT SLS 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 des établissements du GHT SLS ;
- 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 46-1 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.

16. **Documentation** : Le titulaire met à la disposition des établissements du GHT SLS **la documentation nécessaire pour démontrer le respect de toutes ses obligations** et pour permettre la réalisation d'audits, y compris des inspections, par le GHT SLS ou un autre auditeur qu'il a mandaté, et s'engage à contribuer à ces audits.

17. **Sanctions** : En cas de violation du respect de la sécurité informatique et du RGPD par l'une des parties, les parties devront coopérer pour parvenir à une remise en conformité, en accord avec le responsable du traitement.

Si la violation perdure, elle pourra être caractérisée comme une faute du titulaire et entraîner la résiliation du marché. A ce titre l'établissement concerné pourra demander réparation des préjudices matériels et immatériels occasionnés par ladite violation.

II. OBLIGATIONS DES ETABLISSEMENTS DU GHT SLS VIS-A-VIS DU TITULAIRE DU MARCHE

Les établissements du GHT SLS s'engagent à :

1. Fournir au titulaire du marché les données visées dans la présente consultation.
2. Vérifier que le titulaire du marché se donne les moyens de respecter par des mesures techniques et organisationnelles la Politique Générale de Sécurité des Systèmes d'Information– Santé (PGSSI-S) à laquelle les établissements du GHT SLS sont soumis.
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 titulaire.
4. Superviser et contrôler le traitement, y compris réaliser les audits et les inspections auprès du titulaire.

Les coordonnées du DPO, du RSSI, du RSMSI et du DIM du GHT SLS :

Délégué à la Protection des Données (DPO) : dpo@chu-amiens.fr

Responsable de la Sécurité des Systèmes d'Information (RSSI) : rsi@chu-amiens.fr

Responsable Système de Management de la Sécurité de l'Information (RSMSI) : rsmsi@chu-amiens.fr

Responsable du Département d'Information Médicale (DIM) : dim.dossiersmedicaux@chu-amiens.fr