**Dispositions Protection des données personnelles – Marchés Publics**

**Définitions**

Aux fins des présentes dispositions, il convient d’entendre les mots suivants “opération de traitement”, “données personnelles”, “données personnelles de santé”, “personne concernée”, “Responsable de Traitement”, “sous-traitant”, “information”, “finalité”, “registre des activités de traitement de données”, “analyse d’impact sur la vie privée”, “violation de données personnelles” et “autorité de contrôle” au sens des définitions visées à l’article 4 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 (ci-après le “RGPD”).

**1.1 Dispositions générales.** 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 »).

A cet égard, le Titulaire en qualité de Sous-traitant est informé que l’exécution des prestations qui lui sont confiées au titre du présent accord-cadre par Sant& Numérique Hauts-de-France peut impliquer une ou plusieurs opérations de traitement de données à caractère personnel pour lequel Sant& Numérique Hauts-de-France est Responsable de Traitement au sens des législations précitées.

La présente clause précise et définit les conditions dans lesquelles le Titulaire, en application des articles 57 à 61 de la loi Informatique et Libertés et de l’article 28 du Règlement européen sur la Protection des Données, s’engage à effectuer pour le compte de Sant& Numérique Hauts-de-France les opérations de traitement de données à caractère personnel définies à l’accord-cadre.

**1.2 Qualification des parties.** Sant& Numérique Hauts-de-France considéré comme « Responsable de Traitement » et le Titulaire du marché est considéré comme « sous-traitant » de Sant& Numérique Hauts-de-France conformément aux dispositions du Règlement général relatif à la protection des données personnelles (« RGPD ») du 27 avril 2016.

**1.3 Traitements opérés par le Sous-traitant.** Le sous-traitant est autorisé à traiter pour le compte du Responsable de Traitement les données à caractère personnel nécessaires pour fournir des prestations d’installation de l’outil, d’accompagnement technique, de développement, de maintenance et d’infogérance pour l’outil d’authentification – Keycloak , dans le cadre du projet de mise en service d’un outil sécurisant les services régionaux porté par le GRADeS Inéa – Sant& Numérique.

Les opérations réalisées par le sous-traitant sur les données sont :

● La collecte, l'accès, l'enregistrement, la consultation, l’utilisation, et l’effacement des données.

Les traitements potentiellement concernés ont pour finalité la prestations des services décrits au CCTP, en particulier l’exploitation et le maintien en conditions opérationnelles de l’outil et le support.

Les catégories de personnes concernées sont :

* Les professionnels de santé habilités à accéder aux services régionaux (leurs données d’exercice telles qu’identifiant, nom, prénom, métier et coordonnées ainsi que leurs traces d'utilisation seront visibles dans l’outil).
* Le personnel d’Inéa -Sant& Numérique ayant un compte sur Keycloak(nom, prénom, profession et coordonnées ainsi que leurs traces d’utilisation seront visibles dans l’outil) .
* D’autres utilisateurs habilités le cas échéant.

Les données à caractère personnel des personnes concernées traitées sont :

* Données d’identité professionnelle (par exemple: nom, prénom, fonction, organisme, coordonnées professionnelles).
* Données d’authentification (par exemple identifiant, hash de mot de passe)
* Métadonnées des flux (horodatage, service utilisé, actions réalisées, log de connexion)
* Données liées au support (par exemple tickets, notes).

**1.4 Obligation du Prestataire en qualité de sous-traitant.** Le sous-traitant s'engage à :

(i) traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l’objet de la sous-traitance ;

(ii) traiter les données conformément aux instructions documentées du Responsable de Traitement figurant en annexe du présent contrat. 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 États membres relative à la protection des données, il en informe immédiatement le Responsable de 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’État membre auquel il est soumis, il doit informer le Responsable de Traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;

(iii) alerter le Responsable de Traitement de toute instruction non conforme à la loi et à la réglementation par écrit à l’adresse email suivante : dpo@esante-hdf.fr ;

(iv) garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat ;

(v) 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

(vi) 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.

**1.5 Obligations de Sant& Numérique Hauts-de-France en tant que Responsable de Traitement.**  Le Responsable de Traitement est tenu de s’acquitter des obligations qui lui reviennent en application du RGPD, notamment en ce qui concerne l’obligation d’informer les personnes concernées par les opérations de traitement au moment de la collecte des données personnelles, la tenue du registre des traitements mis en œuvre, et plus généralement, du respect des principes issus du RGPD.

Le Responsable de Traitement s’engage en outre à :

(i) fournir au sous-traitant les données personnelles visées dans les caractéristiques du traitement ;

(ii) documenter par écrit toute instruction concernant le traitement des données personnelles par le sous-traitant

(iii) 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

(iv) superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.

**1.6 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, celui-ci doit, sans y répondre, adresser ces demandes dès réception par courrier électronique à l’adresse suivante : dpo@esante-hdf.fr.

**1.7 Notification de violation 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 48 (quarante-huit) heures après en avoir pris connaissance et par email, à l’adresse email ci-après : dpo@esante-hdf.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.

La présente information doit comprendre a minima les éléments suivants :

* La nature de la violation de données ;

- Les catégories et le volume de données à caractère personnel concernées ;

- La catégorie et le nombre approximatif de personnes concernées ;

- Les conséquences existantes et probables de la violation ;

- L’estimation de la gravité du risque engendré par la violation ;

- Les mesures prises ou prévues pour remédier, limiter, atténuer la violation ;

- Le nom et les coordonnées de contact du délégué à la protection des données personnelles s’il a été désigné, le cas échéant le nom et les coordonnées de contact d’un référent.

Dans le cas d’une violation de données, le Titulaire prend toutes les mesures raisonnables et nécessaires pour limiter les conséquences et prévenir une nouvelle fuite.

Par ailleurs, le Titulaire fournit à Sant& Numérique Hauts-de-France, selon le périmètre des données concernées, toute l’assistance nécessaire pour évaluer l’ampleur et les conséquences de la violation de données et pour se conformer à l’obligation de déclaration concernant les atteintes à la protection des données et au devoir d’information des personnes concernées.

**1.8 Assistance du sous-traitant auprès du Responsable de Traitement.** Le sous-traitant aide le Responsable de Traitement, si nécessaire au regard des exigences des autorités de contrôle et notamment la Commission Nationale Informatique et Libertés (CNIL), pour la réalisation d’analyses d’impact relative à la protection des données et de la consultation préalable de l’autorité de contrôle, prévues par le RGPD.

**1.9 Mesures de sécurité.** Le sous-traitant s’engage à mettre en œuvre des mesures de sécurité adaptées, consistant notamment en :

● les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement utilisés ;

● les moyens permettant de rétablir la disponibilité des Données Personnelles 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.

Par ailleurs, le sous-traitant communique une liste précise des mesures de sécurité technique et organisationnelle mises en œuvre pour la fourniture des services en Annexe 5 - PAS..

**1.10 Sort des données à la fin du contrat.** Au terme des Prestations relatives au traitement des Données Personnelles, le sous-traitant s’engage à :

● à renvoyer toutes les données à caractère personnel au Responsable de Traitement ou le cas échéant au sous-traitant qui aura été désigné par le Responsable de Traitement, et ce sans appliquer de frais supplémentaires. Le Responsable de Traitement s’engage à fournir les informations nécessaires au sous-traitant afin de réaliser l’opération relative au sort des données.

Le renvoi doit s’accompagner de la destruction de toutes les copies existantes dans les systèmes d’information du sous-traitant, nonobstant les données nécessaires au sous-traitant dans le cadre de ses obligations légales. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction sur simple de demande du Responsable de Traitement dans un délai de 10 jours ouvrés à compter de ladite demande.

**1.10 Registre des traitements de données.** En cas de traitement de données sensibles, 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 elle 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 de Traitement ;

● le cas échéant, les transferts de Données Personnelles 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 RGPD, les documents attestant de l'existence de garanties appropriées;

● dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles.

**1.11 Délégué à la protection des données.** Chaque Partie s’engage à désigner un Délégué à la protection des données conformément aux dispositions de l’article 37 du RGPD, si cette désignation est obligatoire pour celle-ci.

Chaque Partie déclare avoir désigné, au jour de la signature des présentes, en qualité de délégué à la protection des données :

|  |  |  |
| --- | --- | --- |
|  | Le Responsable de Traitement | Le Sous-traitant |
| Contact email | dpo@esante-hdf.fr |  |

**1.11 Documentation et audit.** 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.

Dans le cadre de tels audits, le Responsable de Traitement ou l’auditeur mandaté par lui ne seront pas autorisés à accéder aux secrets d’affaires du sous-traitant, aux informations stratégiques de celle-ci ou aux informations que le sous-traitant s’est engagé à garder confidentielles. Le sous-traitant pourra s’opposer, par écrit et de façon motivée, à toute mesure de contrôle du Responsable de Traitement ou de l’auditeur mandaté par lui qui serait susceptible de leur donner accès à de telles données ou informations, sans que le Responsable de Traitement puisse effectuer la moindre réclamation à cet égard. Un tel refus par le sous-traitant ne doit pas entraver l’esprit du RGPD et des objectifs globaux du contrôle réalisé par le Responsable de Traitement. Le Responsable de Traitement veillera par ailleurs en tout état de cause à ce que l’auditeur et, plus généralement, le personnel procédant au contrôle soit soumis à des obligations de confidentialité appropriées, et n’exerce pas d’activité concurrente à celle du sous-traitant.

**1.12 Sous-traitants ultérieurs.** Le sous-traitant mettra à la disposition du Responsable de Traitement la liste existante des sous-traitants ultérieurs préalablement à l’attribution du marché pour les services identifiés. Le Responsable de Traitement dispose de la possibilité d’effectuer son choix en fonction des sous-traitants ultérieurs présentés.

Le sous-traitant doit informer le Responsable de Traitement de tout changement prévu dans l'ajout ou dans le remplacement de ses sous-traitants, donnant au Responsable de Traitement la possibilité d'émettre des objections à ces changements. Le sous-traitant effectue les formalités relatives à la Sous-traitance des marchés publics et indique en sus, les activités de traitement sous-traitées, l’identité et les coordonnées du Sous-sous-traitant et les dates de ce contrat telles que demandées dans le formulaire de désigné (DC4) :

<https://www.economie.gouv.fr/daj/formulaires-declaration-du-candidat>

Le sous-traitant reste entièrement responsable à l’égard du Responsable de Traitement pour l'exécution, de tout ou en partie, des obligations de ses sous-traitants régulièrement déclarés et acceptés par le Sant& Numérique Hauts-de-France.

**1.13 Transfert de données en dehors de l’Union européenne.** Le sous-traitant s’engage à ne pas transférer les données à caractère personnel dans un territoire situé hors de l’Espace Économique Européen excepté dans les cas suivants :

- Le transfert est réalisé à destination d’un pays ayant un niveau adéquat de protection de données à caractère personnel certifié par la Commission Européenne ;

- Le transfert est réalisé à destination d’une entreprise ayant adhéré à un dispositif spécifique reconnu par la Commission Européenne, ou à défaut par la CNIL ;

- Le transfert est couvert par des clauses contractuelles types (CCT) élaborées par la Commission Européenne.

Le sous-traitant s’engage à faire respecter ces obligations par ses affiliés et sous-traitants.

Le sous-traitant s’engage à informer le Responsable de Traitement de la localisation des lieux de traitements des données à caractère personnel de quelque nature qu’ils soient (hébergement, backup, maintenance, administration, helpdesk).

**1.14 Coopération avec l’autorité de contrôle.** En cas de besoin, les Parties s’engagent à coopérer de façon conjointe pour répondre aux demandes de l'autorité de contrôle.

**1.16 Droit à réparation et Responsabilité**

Les parties sont responsables des dommages résultant des violations des obligations légales d’une part, et de leurs obligations respectives décrites à l’accord-cadre.

Par ailleurs, à l’effet de l’article 82 du RGPD :

● Le Responsable de Traitement mis en cause aux fins d’indemnisation d’un dommage appelle en garantie le Titulaire pour la part de réparation correspondant à sa part de responsabilité dans le dommage ;

● Le Responsable de Traitement ayant supporté l’intégralité d’indemnisation d’un dommage est en droit de réclamer au Sous-traitant la part de réparation correspondant à sa part de responsabilité dans le dommage

En tout état de cause, le Titulaire est tenu d’apporter à première demande et sans frais toute l’aide et l’assistance nécessaire au responsable de traitement pour préserver ses droits.