MODELE 1

ANNEXE au CCAP RELATIF A L'OBLIGATION DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Étude ciblée sur les facteurs d'attractivité et de fidélisation des professionnels médicaux et paramédicaux dans les hôpitaux de montagne

1 Glossaire

Titulaire : désigne la notion de sous-traitant au sens du Règlement Général sur la Protection des Données 2016/679 du 27 avril 2016 soit "*la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du pouvoir adjudicateur*".

Sous-traitant : désigne la notion de sous-traitant ultérieur au sens du Règlement Général sur la Protection des Données 2016/679 du 27 avril 2016.

Pouvoir adjudicateur : désigne la notion de responsable de traitement au sens du Règlement Général sur la Protection des Données 2016/679 du 27 avril 2016 soit "la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre".

L'établissement bénéficiaire n'étant pas le pouvoir adjudicateur du marché concerné et étant en charge de l'exécution administrative, technique et financière du présent marché, il pourra être substitué au pouvoir adjudicateur dans les droits et obligations ci-après, notamment dans les cas où ceux-ci relèvent de l'exécution du marché.

2 Objet des clauses relatives à la protection des données

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le titulaire s'engage à effectuer pour le compte du pouvoir adjudicateur 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* »).

3. Description du traitement faisant l'objet de la prestation

Le titulaire est autorisé à traiter pour le compte du pouvoir adjudicateur les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) : Étude ciblée sur les facteurs d'attractivité et de fidélisation des professionnels médicaux et paramédicaux dans les hôpitaux de montagne

La nature des opérations réalisées sur les données est : recueil, traitement y compris statistique, interprétation.

La ou les finalité(s) du traitement sont : restitution de statistiques, analyses et de conseils liés à l'objet du marché.

Les données à caractère personnel traitées sont :

Les catégories de personnes concernées sont : agents des établissements concernés par l'étude

Pour l'exécution du service objet du présent contrat, le pouvoir adjudicateur met à la disposition du titulaire les informations nécessaires suivantes : données personnelles nominatives, d'état civil, données professionnelles, de carrière.

4. Obligations du titulaire vis-à-vis du pouvoir adjudicateur

Le titulaire s'engage à :
1. traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la prestation.
2. traiter les données conformément aux instructions documentées du pouvoir adjudicateur figurant en annexe du présent contrat. Si le titulaire 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 pouvoir adjudicateur. En outre, si le titulaire est tenu de procéder à un transfert de données vers un pays tiers autorisé par la CNIL 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 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.

5. Sous-traitance des données à caractère personnel

Le titulaire peut faire appel à un sous-traitant (ci-après, « *le sous-traitant*») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le pouvoir adjudicateur 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 pouvoir adjudicateur dispose d'un délai minimum de 21 jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le pouvoir adjudicateur n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du pouvoir adjudicateur. Il appartient au titulaire de s'assurer que le sous-traitant 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 ne remplit pas ses obligations en matière de protection des données, le titulaire demeure pleinement responsable devant le pouvoir adjudicateur de l'exécution par le sous-traitant de ses obligations.

6. Droit d'information des personnes concernées

Il appartient au pouvoir adjudicateur de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données, sauf lorsque ce dernier revêt la qualité de sous-traitant au sens du règlement européen sur la protection des données.

7. Exercice des droits des personnes

Dans la mesure du possible, le titulaire doit aider le pouvoir adjudicateur 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).

Le titulaire doit répondre, au nom et pour le compte du pouvoir adjudicateur et dans les délais prévus par le règlement européen sur la protection des données, aux demandes des personnes concernées en cas d'exercice de leurs droits, s'agissant des données faisant l'objet du présent contrat.

8. Notification des violations de données à caractère personnel

Le titulaire notifie au pouvoir adjudicateur toute violation de données à caractère personnel dans les meilleurs délais et, si possible, dans un délai maximum de 72 heures après en avoir pris connaissance et par le moyen suivant [Mail : dpo@ch-alpes-leman.fr]. Lorsque la notification n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard. Cette notification est accompagnée de toute documentation utile afin de permettre au pouvoir adjudicateur, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Après accord du responsable de traitement, le sous-traitant notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte du responsable de traitement, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

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 responsable du traitement 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.

Lorsque la notification n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

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.

Après accord du responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée 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 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 responsable du traitement 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.

9. Aide du titulaire dans le cadre du respect par le pouvoir adjudicateur de ses obligations

Le titulaire aide le pouvoir adjudicateur pour la réalisation d'analyses d'impact relatives à la protection des données, en cas de risque élevé pour les droits et libertés des personnes physiques et préalablement au traitement.
Le titulaire aide le pouvoir adjudicateur pour la réalisation de la consultation préalable de l'autorité de contrôle, en cas de risque élevé pour les droits et libertés des personnes physiques et préalablement au traitement.

10. Mesures de sécurité

Le titulaire s'engage à mettre en œuvre les mesures de sécurité prévues par toute règlementation, code de conduite ou de déontologie, certification dont il serait détenteur.

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*

10.1 - Mesures concernant le contrôle des entrées

Pour protéger les bâtiments dans lesquels le traitement a lieu contre toute entrée non autorisée, le titulaire prend les mesures suivantes :
- Gestion détaillée des autorisations d'entrée,
- Dispositifs de verrouillage spéciaux et contrôle électronique des entrées (par exemple carte d'accès, etc.),
- Contrôle des entrées à la réception,
- Vidéosurveillance,
- Portes antieffraction,
- Système d'alarme et
- Détecteurs de mouvement

Pour protéger les locaux/bureaux dans lesquels le traitement a lieu contre toute entrée non autorisée, le titulaire prend les mesures suivantes :
- Bureaux avec des serrures spécifiques ne permettant l'entrée que des personnes autorisées,
- Gestion détaillée des autorisations d'entrée dans les locaux,
- Concept de zones protégées en fonction du risque pour les autorisations d'entrée,
- Limitation du groupe de personnes titulaires d'une autorisation d'entrée aux seules personnes qui en ont besoin,
- Systèmes spéciaux de verrouillage,
- Contrôle électronique de l'entrée (par exemple carte d'accès, etc.),
- Vidéosurveillance,
- Portes antieffraction,
- Système d'alarme et
- Détecteurs de mouvement.

Pour protéger le matériel (hardware)/les installations de stockage physique des données contre toute utilisation abusive, le titulaire prend les mesures suivantes:
- Serveur rack spécialement sécurisé,
- Instructions pour utiliser les appareils mobiles de manière responsable,
- Cryptage complet à la pointe de la technologie et conforme aux normes internationales, et
- Formation concernant la protection des données sensibles indépendamment de la désignation de la zone géographique.

L'adéquation de toutes les mesures de contrôle d'entrée susmentionnées est évaluée sur la base de :
- Vérifications périodiques (au moins une fois par an) des autorisations d'entrée,
- L'inspection et l'approbation régulières de la norme par des tiers et
- La revue régulière et la confirmation de la norme par le délégué à la protection des données.

10.2 - Mesures de contrôle des comptes

10.2.1 Administration des utilisateurs

Pour contrôler l'attribution des comptes utilisateurs, le titulaire prend les mesures suivantes :

- Mise en place d'un organisme central d'administration des utilisateurs,
- Concept d'affectation claire (procédure standardisée pour demander l'autorisation/la création/la modification/la suppression etc. d'un compte),
- Attribution limitée d'identifiants utilisateurs (limitée aux seules personnes qui en ont besoin) et
- Octroi limité de droits et de permissions/différenciation des droits et des permissions pour les utilisateurs respectifs (par exemple droits et permissions d'administrateur).

Pour contrôler la validité des comptes d'utilisateurs, le titulaire prend les mesures suivantes :

- Contrôles aléatoires et réguliers des comptes et
- Prise en compte des changements standard (par exemple déménagement, congé, congé parental, etc.) dans le concept de l'utilisateur.

Le titulaire documente l'accès aux comptes utilisateurs. Pour documenter les processus de connexion et d'autorisation, les procédures d'approbation et la procédure de modification, les mesures suivantes sont prises :

- Documentation générée automatiquement par le système (par exemple système d'enregistrement, gestion des flux de travail, etc.) et
- Administration des utilisateurs par l'organisme central en charge de cette administration (contrôleur).

Le titulaire s'assure que l'attribution de comptes administrateurs est limitée au nombre nécessaire. Le titulaire s'assure que les administrateurs ont les compétences techniques et personnelles nécessaires. Le titulaire s'assure que les administrateurs externes, le personnel de service ou de maintenance ont les compétences personnelles nécessaires.

10.2.2 Sécurité du mot de passe

Pour s'assurer que les mots de passe ne sont connus que de l'utilisateur concerné et non d'une personne non autorisée, le titulaire prend les mesures suivantes :

- Changement du mot de passe initial rendu techniquement obligatoire,
- Interdiction de partage des mots de passe,
- Instructions pour garder les mots de passe secrets,
- Instructions sur le transfert sécurisé des mots de passe,
- Interdiction de documenter les mots de passe de quelque manière que ce soit et
- Administration des utilisateurs par l'organisme central chargé de cette administration (contrôleur).

Pour augmenter les exigences de complexité relatives aux mots de passe, le titulaire prend les mesures suivantes :

- Politique interne relative aux mots de passe avec des spécifications concrètes et
- Paramètres par défaut n'autorisant que les mots de passe conformes à la politique.

Pour garantir que l'utilisateur puisse ou doive changer régulièrement son mot de passe, le titulaire prend les mesures suivantes :

- Renouvellement automatique obligatoire du mot de passe à certains intervalles (par exemple tous les mois),
- Obligation de renouveler le mot de passe,
- Obligation de changer immédiatement les mots de passe prédéfinis et
- Stockage de l'historique des mots de passe afin d'éviter les mots de passe identiques pendant une certaine période.

La gestion des mots de passe est assurée par une unité centrale. Les rôles et permissions ont été définis au sein de cette unité centrale.

En cas d'échec d'une tentative de connexion, le titulaire prend les mesures suivantes :

- Le compte utilisateur est bloqué automatiquement,
- Le contrôleur (administrateur/unité centrale) est automatiquement informé de l'échec de la tentative de connexion,
- Message à l'employé pour qu'il change immédiatement le mot de passe et
- Déblocage automatique après un certain temps.

Pour empêcher tout accès non autorisé aux données personnelles sur le poste de travail, le titulaire prend les précautions organisationnelles suivantes :

- Instructions régulières sur le traitement de divers matériels,

- Instructions régulières sur le traitement des documents,
- Authentification à deux facteurs (exemple : en plus du nom d'utilisateur et du mot de passe, une carte à puce/un jeton sécurisé est requis),
- Mesures garantissant que seules les clés USB d'entreprise cryptées peuvent être utilisées,
- Utilisation d'un logiciel spécial pour la perte de données,
- Utilisation d'un logiciel spécial de prévention des fuites de données,
- Introduction d'un processus de réponse aux violations de données et
- Introduction d'un système de réponse aux incidents.

10.3 Mesures de contrôle d'accès

Pour garantir que les rôles/autorisations d'accès seront attribués de manière à répondre aux exigences et à être limités dans le temps, le titulaire prend les mesures suivantes :

- Système de gestion des identités (IDMS) pour définir les rôles/permissions,
- Audit régulier des rôles/permissions existants, et
- Demande de droits/permissions via IDMS et validation par le supérieur.

Pour documenter les autorisations d'accès, le titulaire prend les mesures suivantes :

- Il existe un concept de permission obligatoire (différenciation par exemple entre admin local/admin groupe/utilisateurs standard).

Pour s'assurer que les utilisateurs n'abusent pas de leur autorisation d'accès, le titulaire prend les mesures suivantes :

- Suivi via IDMS,
- Utilisation de systèmes d'enregistrement et d'évaluation des logs et
- Utilisation d'un système permettant d'identifier les activités suspectes.

10.4 Mesures de suivi du partage de données

Pour garantir l'intégrité et la confidentialité des données lors du partage des données personnelles, le titulaire prend les mesures suivantes :

- Classification des données en fonction de leur degré de confidentialité, pseudonymisation/anonymisation des données avant leur partage,
- Accords de confidentialité avec les prestataires de services/sous-traitants,
- Cryptage des courriels et autres communications électroniques,
- Utilisation de la protection par mot de passe/du cryptage pour les appareils mobiles,
- Règles organisationnelles/directives d'entreprise concernant la restriction de l'utilisation des appareils mobiles/dispositifs de stockage de données (par exemple interdiction des clés USB, interdiction d'utiliser des appareils mobiles personnels),
- Séparation technique des communications professionnelles et personnelles,
- Sélection minutieuse des moyens de transport et des coursiers lors du transport de dispositifs de stockage de données,
- Directives d'entreprise détaillant les mesures organisationnelles correspondantes,
- Processus de réponse aux violations de données et
- Système de réponse aux incidents.

Lors du partage des données personnelles, le titulaire utilise les systèmes de cryptage suivantes :

- Procédure Ipsec,
- Procédure SSH,
- Bitlocker pour crypter les ordinateurs portables,
- Cryptage TLS,
- Plateformes cryptées pour l'échange de données ainsi que
- Cryptage des courriels comprenant le cryptage de bout en bout et le cryptage du transport.

Pour documenter le partage des données personnelles, le titulaire prend les mesures suivantes :

- Création d'un concept de partage des données,
- Enregistrement des récupérations de données,
- Création d'une liste de destinataires et
- Sélection des prestataires de services selon une approche fondée sur le risque.

Pour limiter la dissémination non autorisée de données personnelles, le titulaire prend les mesures techniques suivantes :

- Obligation de protéger les dispositifs de stockage de données contre la perte, les dommages, etc. et
- Système de destruction sécurisée des dispositifs de stockage de données.

Le titulaire dispose d'un système de surveillance qui permet de détecter la dissémination non autorisée de données personnelles grâce à un enregistrement côté système, un processus d'évaluation régulier et l'utilisation d'un système permettant d'identifier les activités suspectes.

10.5 Mesures de contrôle des flux

Le titulaire prend des mesures pour permettre de visualiser les détails (heure, durée) de l'accès aux données. Les données de connexion et de déconnexion sont enregistrées.

Pour permettre de visualiser les activités réalisées dans les diverses applications, le titulaire prend les mesures suivantes :

- Enregistrement des processus de saisie, de modification et de suppression,
- Tenue de rapports et
- Utilisation d'un système permettant d'identifier les activités suspectes.

10.6 Mesures de contrôle du respect des instructions

Le titulaire prend les mesures suivantes pour garantir que le traitement des données personnelles par les employés chargés du traitement ne peut être effectué que conformément aux instructions du donneur d'ordres :

- Lignes directrices, consignes de travail relatives à la protection des données/la sécurité des données,
- Briefing des employés chargés de cette responsabilité,
- Contrôle d'accès (notamment différenciation entre les employés externes/internes),
- Confidentialité des données/obligation de protection des données applicable aux employés et
- Obligations de confidentialité particulières (par exemple informations protégées par le droit pénal).

Pour s'assurer que les sous-traitants ne mènent pas d'activités non autorisées avec les données fournies, le titulaire prend les mesures suivantes :

- Instructions concernant la sélection minutieuse des sous-traitants,
- Interdiction d'engager des sous-traitants dans des pays tiers ne disposant pas d'un niveau adéquat de protection des données,
- Application des obligations contractuelles pertinentes aux sous-traitants et
- Audit régulier des sous-traitants sur la base des normes ISO et/ou TISAX et documentation de l'audit.

Pour s'assurer que les données personnelles sont supprimées/verrouillées à la fin de la finalité justifiant le stockage, le titulaire a techniquement mis en œuvre les mesures suivantes :

- Consignes de travail/directives d'entreprise concernant la suppression/le verrouillage/la limitation du stockage, et
- Application des obligations contractuelles pertinentes aux sous-traitants.

10.7 Mesures de contrôle de la disponibilité des données

Le titulaire prend les mesures organisationnelles et techniques suivantes afin d'assurer la disponibilité des données et des systèmes le plus rapidement possible en cas de dommage :

- Plans d'urgence relatifs à la sauvegarde et à la récupération après sinistre,
- Directives d'entreprise relatives aux processus de sauvegarde,
- Mise en miroir physique synchrone et/ou asynchrone des disques durs dans des centres de données distincts dotés de capacités opérationnelles adéquates (alimentation électrique indépendante),
- Processus de réponse aux violations des données et
- Système de réponse aux incidents.

Le titulaire prend les mesures suivantes pour garantir la protection des dispositifs de stockage des données contre l'influence des éléments naturels (feu, eau, rayonnement électromagnétique, etc.):

- Détecteurs de fumée et d'incendie,
- Système d'arrosage,
- Portes coupe-feu,
- Équipement étanche,
- Blindage électromagnétique,
- Alimentation électrique de secours,
- Procédure standardisée pour des audits réguliers de l'adéquation des mesures de protection et
- Règlement intérieur n'autorisant l'accès qu'après formation/instruction ou avec accompagnement.

Le titulaire prend les mesures de protection suivantes pour lutter contre l'utilisation de logiciels malveillants :

- Logiciels anti-malware,
- Scanners de virus,

- Programmes anti-spyware,
- Scans complets réguliers et scans rapides de l'ensemble des inventaires informatiques,
- Pare-feu,
- Filtres anti-spam et
- Systèmes IDS/IPS.

Le titulaire prend les mesures suivantes pour s'assurer que les dispositifs de stockage de données qui ne sont plus utilisés ou qui sont défectueux sont éliminés de manière appropriée :
- Embauche et suivi d'entreprises spécialisées,
- Embauche exclusive d'entreprises respectant la norme DIN 66399,
- Garantie d'une élimination conforme aux instructions de travail et aux directives d'entreprise,
- Élimination conformément à la norme DIN 66399 et
- Utilisation exclusive de disques durs/SSD de serveurs avec une politique de "non-retour" (ne devant en aucun cas quitter les locaux).

10.8 Mesures de de surveillance de la séparation des données
Mesures de surveillance de la séparation des données
Le titulaire prend les mesures suivantes pour que la séparation obligatoire, notamment en ce qui concerne la finalité des données personnelles, soit assurée :
- Stockage séparé pour la pseudonymisation des données personnelles,
- Séparation des données de test et de production,
- Restriction technique d'accès,
- Cryptage des fichiers de données et
- Instructions de travail/directives d'entreprise sur la limitation des objectifs.

11. Sort des données à caractère personnel

Au terme de la prestation de services relatifs au traitement de ces données, le titulaire s'engage à :

- Détruire toutes les données à caractère personnel ou ;
- A renvoyer toutes les données à caractère personnel au responsable de traitement ou ;
- A renvoyer les données à caractère personnel au prestataire désigné par le responsable de traitement

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.

12. 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.

13. 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 du pouvoir adjudicateur comprenant :

- Le nom et les coordonnées du pouvoir adjudicateur 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 pouvoir adjudicateur ;
- 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.

Une copie du registre est envoyée au pouvoir adjudicateur à la mise en place du registre ainsi qu'à chaque modification de ce dernier.

14. Documentation

Le titulaire met à la disposition du pouvoir adjudicateur la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le pouvoir adjudicateur ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

15. Obligations du pouvoir adjudicateur vis-à-vis du titulaire

Le pouvoir adjudicateur s'engage à :

1. Fournir au titulaire les données visées au 3 des présentes clauses ;

2. Documenter par écrit toute instruction concernant le traitement des données par le titulaire ;

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.

16. Obligation de confidentialité

Le titulaire s'engage à veiller à ce que les personnels autorisés à intervenir sur les moyens de traitement des données à caractère personnel respectent les consignes internes en matière de sécurité définies dans les documents de politique de sécurité interne.

Soumis à des obligations de discrétion professionnelle, ou le cas échéant soumis au secret professionnel, les personnels du titulaire sont régulièrement sensibilisés sur leurs rôles et responsabilités en matière de confidentialité et de sécurité des données.

17. Communication de données à des tiers autorisés

Le titulaire s'engage à informer sans délai le pouvoir adjudicateur en cas de requête provenant d'une autorité administrative ou judiciaire demandant à avoir communication de données à caractère personnel entrant dans le périmètre du présent contrat.

Dans le cas où la requête est reçue par le pouvoir adjudicateur, le titulaire s'engage à mettre en œuvre les moyens permettant de répondre à la demande dans les délais exigés sur le périmètre des opérations de traitement confiées au titulaire.

18. Engagement relatif aux contrôles et aux audits

Le titulaire s'engage à répondre aux demandes d'audit du pouvoir adjudicateur, effectuées par lui-même ou par un tiers de confiance qu'il aura sélectionné et s'engage à mettre en œuvre les moyens permettant à l'auditeur de réaliser sa mission dans les meilleures conditions.

Le pouvoir adjudicateur s'engage à fournir au titulaire une copie du rapport d'audit afin qu'il puisse prendre en compte rapidement les non-conformités constatées et les mesures correctives proposées.

Le titulaire s'engage à mettre en œuvre les mesures correctives nécessaires au traitement des non-conformités identifiées dans un délai et selon les conditions définies d'un commun accord.

Dans le cas où des mesures correctives ne seraient pas applicables, le titulaire s'engage à justifier l'impossibilité de mettre en œuvre les mesures et s'engage à proposer des mesures palliatives pour réduire les risques encourus.

19. Engagement relatif au traitement des réclamations

Le titulaire s'engage à informer sans délai le pouvoir adjudicateur pour toute demande qu'il reçoit des personnes concernées par les opérations de traitement confiées.

Le titulaire s'engage à aider le pouvoir adjudicateur 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 titulaire ne serait pas en capacité de fournir les éléments permettant au pouvoir adjudicateur de respecter le délai de 1 mois, il s'engage à fournir les justificatifs permettant au pouvoir adjudicateur 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 60 jours après la première sollicitation.

20. Engagement du titulaire en tant que responsable de traitement

Le titulaire s'engage à respecter les obligations qui lui incombent en tant sous-traitant des données personnelles qu'il traite pour le compte du responsable de traitement et à fournir au pouvoir adjudicateur des éléments de traçabilité permettant de le démontrer.

Si désignation obligatoire, le Délégué à la Protection des Données du titulaire se tiendra à la disponibilité du pouvoir adjudicateur pour apporter les éléments justificatifs démontrant l'application du Règlement Général de Protection des Données.

21. Devoir de coopération avec l'autorité de contrôle (CNIL)

Le titulaire s'engage à coopérer avec l'autorité de contrôle compétente en matière de protection des données (CNIL), notamment en cas de demande d'information qui pourrait être adressée par cette dernière, ou en cas de contrôle sur site ou à distance des opérations de traitement confiées au titulaire.

Le titulaire s'engage à informer le pouvoir adjudicateur en cas de contrôle sur site ou à distance des opérations de traitement confiées au titulaire et à remettre le cas échéant une copie du rapport de l'autorité de contrôle.

22. Engagement en matière de sécurité des données

Le titulaire s'engage à prendre toutes précautions utiles afin de préserver la sécurité des données et notamment de les protéger contre toute destruction accidentelle ou illicite, perte accidentelle, altération, diffusion ou accès non autorisés, ainsi que contre toute autre forme de traitement illicite ou communication à des personnes non autorisées (conformément à l'article 32 du Règlement Général de Protection des Données).

Le titulaire s'engage notamment à mettre en œuvre :

- 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.

Le titulaire s'engage à respecter les bonnes pratiques en matière de sécurité émises par les autorités compétentes (ANSSI et CNIL notamment) et à mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. La cartographie des risques réalisée par le titulaire pourra être présentée sur demande au pouvoir adjudicateur.

Le pouvoir adjudicateur pourra à tout moment solliciter le Responsable de la Sécurité des Systèmes d'Information (RSSI) du titulaire pour s'assurer que la politique spécifique de sécurité mise en œuvre sur le périmètre du présent contrat est appliquée et respecte les bonnes pratiques reconnues dans le domaine ainsi que les exigences du Règlement Général de Protection des Données.

Il est expressément prévu que toute modification sur ce point entre dans le cadre de l'article R2194-1 du Code de la commande publique. La conclusion d'un avenant ne sera pas obligatoire : la modification pourra être intégrée automatiquement à l'accord-cadre (ou du marché) sur simple information d'une partie par la partie la plus diligente.