**Règlement de la Consultation**

**ANNEXE 3 – Traitement des données à caractère personnelles**

# Terminologie utilisée dans le Règlement Européen

**Une donnée à caractère personnel** est toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

**Le responsable de traitement** est celui « qui détermine les finalités et les moyens d’un traitement » (article 4 du règlement européen). En matière de marché public, c’est l’organisme de Sécurité sociale.

**Le sous-traitant** est celui qui traite des données personnelles pour le compte, sur instruction et sous l’autorité d’un responsable de traitement. En matière de marché public, c’est le titulaire du marché (y compris le sous-traitant du titulaire).

# Traitement des données dans le cadre d’un marché public

## Propriété intellectuelle

Le titulaire déclare détenir l’intégralité des droits de propriété intellectuelle portant sur l’application et /ou être régulièrement titulaire des droits d’utilisation et d’exploitation portant sur les logiciels et progiciels tiers nécessaires à son fonctionnement.

Il concède à l’UIOSS de la Marne des licences personnelles, non exclusives, non transmissibles et non cessibles d’utilisation de la solution. Chaque licence est consentie pour la durée du marché et les besoins propres de l’UIOSS de la Marne.

L’UIOSS de laMarne s’interdit de céder et de transmettre de quelque manière que ce soit, même à titre gratuit, le droit d’utilisation concédé dans ce marché.

## Sécurité et protection des données.

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 »).

Pour l’exécution du service, objet du présent contrat, le titulaire s'engage à :

1. Traiter les données uniquement pour les finalités de la prestation qui font l’objet du contrat

2. Traiter les données conformément à ce qui est établis dans le contrat. Si l’une ou l’autre des parties 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 l’autre. 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 l’UIOSS de la Marne 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

6. Demander l’autorisation à l’UIOSS de la Marne pour faire appel à un sous-traitant pour mener des activités de traitement spécifiques. Il doit informer préalablement et par écrit le représentant de l’UIOSS de la Marne de tout changement envisagé concernant l’ajout ou le remplacement d’autres sous-traitants.

La déclaration de sous-traitance doit se faire dans les conditions énoncées dans l’article dédié du CCAP. En aucun cas le titulaire ne devra sous-traiter une partie de ses activités sans l’obtention de l’acceptation du sous-traitant par l’UIOSS de la Marne se traduisant par un acte spécial signé des deux parties.

**En tout état de cause le titulaire demeure responsable de ses sous-traitants.**

7. Droits d’informations des personnes concernées :

Le titulaire, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l’information relative aux traitements de données qu’il réalise. La formulation et le format de l’information doit être convenue avec l’UIOSS de la Marne avant la collecte de données.

8. Exercice des droits des personnes :

Dans la mesure du possible, le titulaire doit aider l’UIOSS de la Marneà 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 de l’UIOSS de la Marneet 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 des prestations prévues par le présent contrat.

9. Notification des violations de données à caractère personnel :

Le titulaire notifie à l’UIOSS de la Marne toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance et par tout moyen permettant une traçabilité à l’adresse [uioss.cpam-marne@assurance-maladie.fr](mailto:uioss.cpam-marne@assurance-maladie.fr)

Cette notification est accompagnée de toute documentation utile afin de permettre à l’UIOSS de la Marne, si nécessaire, de notifier cette violation à l’autorité de contrôle compétente.

Après accord de l’UIOSS de la Marne, le titulaire notifie à l’autorité de contrôle compétente (la CNIL), au nom et pour le compte de l’UIOSS de la Marne, 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.

Lorsque la notification à l’autorité de contrôle n’a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

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 l’UIOSS de la Marne 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.

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 de l’UIOSS de la Marne, le titulaire communique, au nom et pour le compte de l’UIOSS de la Marne, 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 l’UIOSS de la Marne 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.

10. Aide du titulaire dans le cadre du respect par l’UIOSS de la Marne de ses obligations :

Le titulaire aide l’UIOSS de la Marnepour la réalisation d’analyses d’impact relative à la protection des données ainsi que pour la réalisation de la consultation préalable de l’autorité de contrôle.

11. Mesures de sécurité :

Le titulaire s’engage à mettre en œuvre les mesures de sécurité techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, y compris, entre autres :

* 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 mettre en œuvre les mesures de sécurité prévues par le code de conduite élaborée par l’organisation représentative du secteur d’activité du titulaire et approuvé par le Commission européenne.

12. Désignation d’un DPO :

Le titulaire s’engage à communiquer à l’UIOSS de la Marne le nom et les coordonnées du délégué à la protection des données, s’il en a désigné conformément à l’article 37 du règlement européen.

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 responsable de traitement comprenant :

* le nom et les coordonnées du responsable de traitement de l’organisme contractant pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données de l’UIOSS de la Marne,
* les catégories de traitements effectués pour le compte du responsable du traitement

14. Documentation :

Le titulaire 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 du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

15. Sort des données :

Au terme du contrat, le titulaire s’engage à renvoyer toutes les données à caractère personnel au représentant de l’UIOSS de la Marne*.*

Le renvoi doit s’accompagner de la destruction de toutes les copies existantes dans les systèmes d’information du titulaire. Le titulaire doit justifier par écrit de la destruction.