PROTECTION DES DONNEES PERSONNELLES

MARCHE DE MAITRISE D'ŒUVRE

MAITRISE D'ŒUVRE POUR LA RENOVATION DU BÂTIMENT RENOIR

26M07-7110

CAISSE PRIMAIRE D'ASSURANCE MALADIE DES ALPES MARITIMES

48, Avenue Roi Robert Comte de Provence
06180 NICE CEDEX 2

1. 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 la Caisse Primaire d'Assurance Maladie (CPAM) des Alpes Maritimes 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 la CPAM.

La CPAM 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.

2. 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 aux instructions documentées de la CPAM 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 la CPAM des Alpes Maritimes. 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 la CPAM 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 la CPAM pour faire appel à un sous-traitant pour mener des activités de traitement spécifiques. Il doit informer préalablement et par écrit la CPAM 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. La CPAM dispose d'un délai minimum de 15 jours à compter de la date de réception de cette information pour présenter ses

objections. Cette sous-traitance ne peut être effectuée que si La CPAM n'a pas émis d'objection pendant le délai convenu.

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 le la CPAM avant la collecte de données.

8. Exercice des droits des personnes
Dans la mesure du possible, le titulaire doit aider le la CPAM 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 la CPAM 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 des prestations prévues par le présent contrat.

9. Notification des violations de données à caractère personnel
Le titulaire notifie à la CPAM toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance et par le moyen suivant : marches.cpam-alpes-maritimes@assurance-maladie.fr

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

Après accord de la CPAM, le titulaire notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte de la CPAM, 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 la CPAM 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 la CPAM le titulaire communique, au nom et pour le compte de la CPAM, 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 la CPAM 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 la CPAM de ses obligations.
Le titulaire aide la CPAM pour 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.

12. Désignation d'un DPO
Le titulaire s'engage à communiquer à « indiquer le nom de l'organisme » 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 la CPAM contractant pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données de la CPAM.
· 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 à la CPAM.
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.