

Numéro et objet du marché : Marché n°2024PRA01 : Marché mutualisé de Prestations de Contrôle Technique et de Coordination en matière de Sécurité et de Protection de la Santé pour le compte des Caisses Primaires d'Assurance Maladie de la Région Auvergne Rhône-Alpes

Objet : Prise en compte du Règlement général sur la protection des données (RGPD) par les sous-traitants

Madame, Monsieur,

L'attribution d'un marché public confère à l'entreprise attributaire la qualité de titulaire de marché public. Cette qualité peut vous placer dans une situation de sous-traitance vis-à-vis des CPAM de la Région Auvergne Rhône-Alpes au sens de la réglementation dite « informatique et libertés ».

En effet, est qualifiée de sous-traitant « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données pour le compte du responsable du traitement¹* »

Or, le nouveau Règlement Européen de Protection des Données Personnelles (RGPD), entré en vigueur le 25 mai 2018, est venu fixer de nouvelles obligations pour les sous-traitants et notamment² :

- Prendre les mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD (exemple : niveau de sécurité adapté, afin de garantir l'intégrité ou la confidentialité des données³) et garantisse la protection des droits des personnes ;
- Ne traiter les informations que conformément aux instructions des CPAM de la Région Auvergne Rhône-Alpes, y compris en ce qui concerne les transferts de données en dehors de l'Union Européenne ;
- Veiller, à ce que votre personnel traitant les données soit tenu à la confidentialité ou soit soumis à une obligation légale appropriée de confidentialité ;
- Apporter votre aide aux CPAM de la Région Auvergne Rhône-Alpes, en fonction de la nature du traitement, pour qu'elles s'acquittent de l'ensemble

¹ Article 4 RGPD

² Articles 28 et s. RGPD

³ Article 32 RGPD

de leurs obligations (obligations vis-à-vis des droits des personnes concernées, de la sécurité du traitement, etc.⁴) ;

- Mettre à disposition des CPAM de la Région Auvergne Rhône-Alpes toutes les informations nécessaires pour démontrer le respect de leurs obligations et pour permettre la réalisation d'audits, y compris des inspections et contribuer à ces audits ;
- Informer les CPAM de la Région Auvergne Rhône-Alpes de toute instruction qui pourrait constituer, selon vous, une violation des dispositions du RGPD et de la loi dite « informatique et libertés » modifiée⁵ ;
- Notifier aux CPAM de la Région Auvergne Rhône-Alpes toute violation de données que vous traitez pour son compte dans les meilleurs délais après en avoir pris connaissance afin qu'elle puisse respecter leurs obligations⁶ ;
- Tenir un registre de toutes les catégories d'activité de traitement effectuées pour le compte des CPAM de la Région Auvergne Rhône-Alpes⁷.

Dans l'hypothèse où vous avez vous-même recours à de la sous-traitance pour une ou diverses missions que les CPAM de la Région Auvergne Rhône-Alpes vous ont confiées, et sous réserve qu'elles l'aient préalablement et formellement autorisée, nous vous rappelons que lesdits sous-traitants sont tenus aux mêmes obligations précitées. Vous demeurez cependant pleinement responsable de l'inexécution de leurs obligations. Ces règles sont naturellement valables pour toute nouvelle sous-traitance.

Ces dispositions ne remettent aucunement en cause l'ensemble des obligations contractuelles spécifiées au sein du marché qui vous lie aux CPAM de la Région Auvergne Rhône-Alpes et notamment celles relatives :

- au sort des données que vous traitez pour le compte des CPAM de la Région Auvergne Rhône-Alpes (suppression, destruction, retransmission de ces données) ;
- aux règles relatives à la confidentialité ;
- aux conditions de sécurité précisées au sein d'un éventuel plan d'assurance sécurité (PAS).

L'ensemble de ces obligations vous sont directement opposables pour les contrats en cours même si leur signature est antérieure à la date d'entrée en vigueur du RGPD.

⁴ Chap III RGPD, articles 32 à 36 RGPD

⁵ Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés telle que modifiée par la loi n°2018-493 du 20 juin 2018

⁶ Art. 33 RGPD

⁷ Art. 30.2 RGPD

Enfin, je vous prie de nous fournir l'avancée de vos mesures mises en place afin de vous conformer à cette réglementation ainsi que les coordonnées de votre délégué à la protection des données (DPO) si vous êtes soumis à l'obligation d'en désigner un⁸.

Je vous remercie de votre collaboration et vous prie de croire, Madame, Monsieur, l'expression de mes salutations distinguées.

Le Responsable Pôle Achat

⁸ Art. 37 RGPD