



Conditions Générales

Annexe RGPD

Accord-cadre n°AC.2024.1992

Service d'envoi et d'archivage de lettre recommandées

Préambule

La présente **Annexe RGPD** a pour objet de définir les conditions dans lesquelles le **Prestataire** effectue pour le compte des **Organismes bénéficiaires** les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de l'accord-cadre n°**AC.2024.1992** :

- Les **Organismes bénéficiaires** agissent en tant que **co-responsable du traitement** au sens du RGPD ;
 - Le **Prestataire** agit en tant que **sous-traitant** des **Organismes bénéficiaires** au sens du RGPD.
-

ARTICLE 1. DESCRIPTION DU TRAITEMENT FAISANT OBJET DE LA SOUS-TRAITANCE

1.1 GENERALITES

Le **Prestataire** est autorisé à traiter pour le compte des **Organismes bénéficiaires**, les données à caractère personnel nécessaires pour fournir les **Service d'envoi et d'archivage de lettre recommandées**, objet de l'accord-cadre n°AC.2024.1992.

1.2 CATEGORIE DES PERSONNES CONCERNEES PAR LE TRAITEMENT

Les catégories de personnes concernées par le traitement sont les suivants : les assurés, les employeurs, les professionnels de santé et autres destinataires des courriers.

1.3 LISTE DES DONNEES A CARACTERE PERSONNEL CONCERNEES PAR LE TRAITEMENT

Dans le cadre de l'accord-cadre n°AC.2024.1992, les données à caractère personnel pouvant faire l'objet d'un traitement sont les suivantes :

- L'identité (nom, prénom, genre) des destinataires des courriers;
- La profession des destinataires des courriers ;
- Les coordonnées (mail, adresse postale, numéro de téléphone) des destinataires des courriers.

1.4 NATURE DES OPERATIONS DE TRAITEMENT

La nature des opérations réalisées sur les données à caractère personnel est le recueil, la consultation, le traitement, l'adressage, le classement, l'organisation, l'archivage, le suivi et toute opération nécessaire à l'exécution des prestations constituant le **Service d'envoi et d'archivage de lettre recommandées**, objet de l'accord-cadre n°AC.2024.1992.

1.5 FINALITES DU TRAITEMENT

Le **Prestataire** est autorisé à traiter, dans le sens large du terme, pour le compte des **Organismes bénéficiaires**, les données à caractère personnel nécessaires à l'organisation et la tenue des prestations constituant le **Service d'envoi et d'archivage de lettre recommandées**, objet de l'accord-cadre n°AC.2024.1992.

Tout traitement de données à caractère personnel non strictement nécessaire à la finalité susmentionnée est expressément proscrit.

La finalité du traitement est exclusivement liée à l'exécution des prestations constituant le **Service d'envoi et d'archivage de lettre recommandées**.

A ces occasions, le **Prestataire** peut être notamment amené à :

- Confectionner une base de données ou registre sous forme d'annuaire listant l'identité (nom, prénom, genre, qualité), les adresses et coordonnées des destinataires des courriers à envoyer en lettre recommandée dans le cadre de l'accord-cadre n°AC.2024.1992 ;
- Consulter l'identité (nom, prénom, genre, qualité), les adresses et coordonnées des destinataires des courriers à envoyer en lettre recommandée dans le cadre de l'accord-cadre n°AC.2024.1992 ;
- Reproduire sur une étiquette, une enveloppe ou autre les adresses, les noms, le genre et la qualité des destinataires des courriers à envoyer en lettre recommandée dans le cadre de l'accord-cadre n°AC.2024.1992 ;

- Communiquer aux services postaux les adresses, les noms, le genre et la qualité des destinataires des courriers à envoyer en lettre recommandée dans le cadre de l'accord-cadre n°AC.2024.1992.

1.6 DUREE DU TRAITEMENT

Le **Prestataire** effectue pour le compte des **Organismes bénéficiaires** les opérations de traitement de données à caractère personnel mentionnées ci-avant et ce pendant toute la durée de l'accord-cadre n°AC.2024.1992.

ARTICLE 2. OBLIGATIONS DES PARTIES

2.1 OBLIGATIONS DU PRESTATAIRE

En application du RGPD et tant que sous-traitant, le **Prestataire** est notamment soumis aux obligations suivantes (article 28 et s. RGPD) :

- 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 données ; article 32 RGPD) et garantisse la protection des droits des personnes ;
- Ne traiter les informations que conformément aux instructions des **Organisme bénéficiaires**, y compris en ce qui concerne les transferts de données en dehors de l'Union Européenne ;
- Veiller, à ce que le personnel traitant les données soit tenu à la confidentialité ou soit soumis à une obligation légale appropriée de confidentialité ;
- Fournir, le cas échéant, aux **Organisme bénéficiaires** ou toute autorité d'enregistrement désignée, la liste exhaustive du personnel accédant aux données ;
- Apporter l'aide aux **Organisme bénéficiaires**, en fonction de la nature du traitement, pour qu'ils s'acquittent de l'ensemble de leurs obligations (obligations vis-à-vis des droits des personnes concernées, de la sécurité du traitement, etc ; Chap III RGPD, articles 32 à 36 RGPD) ;
- Mettre à disposition des **Organisme bénéficiaires** 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 ;
- Permettre aux **Organisme bénéficiaires** de gérer toutes les obligations relatives à l'exercice des droits ;
- Informer les **Organisme bénéficiaires** de toute instruction qui pourrait constituer une violation des dispositions du RGPD et de la loi dite « informatique et libertés » modifiée (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) ;
- Notifier aux **Organisme bénéficiaires**, dans les meilleurs délais, toute suspicion de violation de données, accidentelle ou non, traitées pour leur compte dans les meilleurs délais après en avoir pris connaissance afin qu'elle puisse respecter ses obligations (article 33 RGPD) ¹ ;
- Tenir un registre de toutes les catégories d'activité de traitement effectuées pour le compte de la **Cnam** (article 30.2 RGPD).

Dans l'hypothèse où le **Prestataire** a lui-même recours à de la sous-traitance pour une ou diverses missions que les **Organisme bénéficiaires** lui ont confiées, et sous réserve qu'il ait été préalablement et formellement autorisé, les sous-traitants sont tenus aux mêmes obligations précitées.

¹ Il est convenu entre la **Cnam** et le **Titulaire** que toutes les interventions qui seront effectuées par ce dernier auront lieu sous couvert de l'anonymisation des données grâce à des scripts fournis par ledit Titulaire et que le pouvoir adjudicateur s'engage à utiliser.

Le **Prestataire** demeure cependant pleinement responsable de l'inexécution de obligations.

Ces dispositions ne remettent aucunement en cause l'ensemble des obligations contractuelles spécifiées au sein de l'accord-cadre n°AC.2024.1992 qui lie le **Prestataire** aux **Organisme bénéficiaires** et notamment celles relatives :

- Au sort des données que traite le **Prestataire** pour le compte de la **Cnam** (suppression, destruction, retransmission de ces données) ;
- Aux règles relatives à la confidentialité.

Sur demande des **Organisme bénéficiaires**, le **Prestataire** doit être en mesure de fournir l'avancée des mesures mises en place afin de se conformer à cette réglementation ainsi que les coordonnées du délégué à la protection des données (DPO) dans la mesure où le **Prestataire** est soumis à l'obligation d'en désigner un (article 37 RGPD).

Afin de contrôler le respect par le **Prestataire** de ses obligations, un audit RGPD (hors audit déclenché par une autorité de contrôle) peut être réalisé.

Au maximum, un (1) audit par an peut être conduit afin de vérifier que le **Prestataire** est en conformité avec les obligations du RGPD.

En cas de demande de la **Cnam** en tant que représentante des **Organismes bénéficiaires**, de réalisation d'un audit, le **Prestataire** est informé au minimum **quatorze (14) jours calendaires** avant sa réalisation.

Cet audit peut être assuré par la **Cnam** en tant que représentante des **Organismes bénéficiaires**, ou un auditeur tiers non concurrent du **Prestataire**.

Si un auditeur tiers a la charge de l'audit, il est conduit aux frais exclusifs de la **Cnam** en tant que représentante des **Organismes bénéficiaires**, et soumis à un engagement de confidentialité.

2.2 OBLIGATION DES ORGANISMES BENEFICIAIRES

De son côté, tout au long de l'accord-cadre n°AC.2024.1992, la **Cnam** s'engage au nom et pour le compte des **Organismes bénéficiaires** à :

- Transmettre ses instructions de manière documentée ;
- Sans préjudice du devoir de conseil du **Prestataire**, vérifier que chacune de ses instructions est licite au regard de la réglementation applicable à la protection des données à caractère personnel ;
- Répondre aux demandes du **Prestataire** et lui transmettre sans délai toute information ou document dont le **Prestataire** aurait besoin pour maintenir sa conformité à la réglementation applicable à la protection des données à caractère personnel ou répondre à toute requête provenant d'une autorité de contrôle ;
- Communiquer au **Prestataire**, dès la signature de l'accord-cadre n°AC.2024.1992, l'identité et les coordonnées de son délégué à la protection des données² ;
- Informer le **Prestataire**, immédiatement de toute requête, audit ou contrôle déclenché par une autorité de contrôle qui concernerait ou impliquerait, de quelque manière que ce soit, directement ou indirectement, le **Prestataire** ;
- Superviser le traitement, y compris réaliser les audits et inspections auprès du **Prestataire**, suivant les conditions prévues au présent article ;

² En cas de changement, la Cnam s'engage d'en informer le **Titulaire**, dans les meilleurs délais et lui transmettre la nouvelle identité et les nouvelles coordonnées du délégué à la protection des données

- Notifier à l'autorité de contrôle concernée toute violation de données à caractère personnel dans un délai de **soixante-douze (72) heures**, à compter de sa prise de connaissance d'un tel évènement, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernées ;
- Conduire une analyse d'impact sur la vie privée, pour tous les traitements de données à caractère personnel susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées, et pour les types d'opérations de traitement listés par l'autorité de contrôle conformément à l'article 35 du Règlement.