



Conditions Générales

Annexe RGPD

Marché n°2025-019

Gestion déléguée « retraite / invalidité décès » in

Préambule

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

Dans le cadre du marché n°**2025-019** :

- La **CPRN** agit en tant que **responsable du traitement** au sens du RGPD ;
 - Le **Prestataire** agit en tant que **sous-traitant** de la **CPRN** au sens du RGPD.
-

Conformément au 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 » ou « le RGPD »), le **Prestataire** s'engage à :

1. **Traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la sous-traitance tel que mentionnée ci-avant ;**
2. **Traiter les données conformément aux instructions documentées du responsable de traitement.**

Si le **Prestataire** 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 **CPRN**. En outre, si le **Prestataire** 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 **CPRN** de cette obligation juridique avant le traitement.

3. **Assurer la sécurité et la confidentialité des données à caractère personnel traitées dans le cadre du marché n°2025-019**
4. **Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du marché n°2025-019, 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. **Respecter les éléments suivants s'il compte faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques.**

Dans ce cas, il informe préalablement et par écrit le responsable de traitement 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 responsable de traitement dispose d'un délai de deux mois à compter de la date de réception de cette information pour présenter ses objections.

Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Tout sous-traitant ultérieur sera tenu de respecter les obligations du présent document et notamment les instructions du responsable de traitement.

Le sous-traitant doit s'assurer que le sous-traitant ultérieur choisi, 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 RGPD.

Si le sous-traitant ultérieur ne remplit pas les obligations en matière de protection des données, le sous-traitant demeure pleinement responsable de l'exécution par l'autre sous-traitant de ses obligations.

Le sous-traitant sera tenu responsable en cas de manquement exclusivement imputable à lui et/ou à ses sous-traitants ultérieurs à leurs obligations en vertu du présent contrat, du RGPD et de la Loi Informatique et Libertés.

7. Fournir, au moment de la collecte des données, 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 responsable de traitement avant la collecte de données.

8. Contribuer à l'exercice des droits des personnes.

Dans la mesure du possible, le **Prestataire** doit aider la **CPRN** responsable de traitement 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 **Prestataire** doit répondre, au nom et pour le compte de la **CPRN** responsable de traitement 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 de la sous-traitance prévue par le marché n°2025-019.

9. Notifier les violations de données à caractère personnel.

Après accord du responsable de traitement, le **Prestataire** notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte de la **CPRN** 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.

Cette notification devra se faire par courrier électronique à l'adresse suivante : ContactDPO@cprn.fr.

Cette notification contient au moins les informations suivantes :

- La description de l'incident de sécurité : nature, portée, catégories et nombre approximatif d'enregistrements de données personnelles concernées, catégories et nombre approximatif de personnes concernées, temporalité, conséquences ;
- Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel les informations supplémentaires peuvent être obtenues ;
- La description des mesures prises, engagées ou proposées pour remédier à l'incident de sécurité, y compris, le cas échéant les mesures pour atténuer les éventuels effets négatifs pour les personnes concernées.

S'il n'est pas possible de fournir toutes ces informations en même temps, le sous-traitant peut les communiquer de manière échelonnée.

Le sous-traitant s'engage à coopérer pleinement, à ses frais, avec le responsable de traitement afin de l'aider dans la gestion de cette situation et notamment en :

- L'aidant à la conduite des investigations sur l'incident de sécurité ;
- Fournissant au responsable de traitement ou au tiers indépendant qu'il a désigné, un accès physique aux installations et opérations concernées ;

- Organisant des entretiens entre le personnel du responsable de traitement et son propre personnel ;
- Fournissant tous les registres, journaux, dossiers, communications de données et autres documents pertinents nécessaires pour se conformer à la réglementation en vigueur et, le cas échéant, aux codes de conduite auxquels il aurait adhéré.

Le sous-traitant reconnaît que le responsable de traitement est seul habilité :

- A déterminer si l'incident de sécurité constitue ou non une violation de données à caractère personnel ;
- A décider si cette violation doit ou non être notifiée à l'autorité de contrôle, voire communiquée aux personnes concernées ;
- A formaliser le contenu de ladite notification ;
- A réaliser la notification proprement dite à la CNIL.

Lorsque le responsable de traitement est dans l'obligation de communiquer la violation de données à caractère personnel aux personnes concernées, le sous-traitant prend en charge les frais liés à cette communication si la violation est survenue à cause d'un manquement du sous-traitant aux obligations prévues par le présent document et au RGPD.

Suite à une éventuelle violation de données, le sous-traitant assiste le responsable de traitement pour répondre à toute enquête ou demande émanant d'une autorité de contrôle, voire à toute plainte formulée par une personne concernée.

Le sous-traitant tient et met à disposition du responsable de traitement un registre des incidents de sécurité qui ont impacté les données confiées et y documente, au minimum, toute information pertinente concernant les circonstances de ces incidents de sécurité, ses effets et les mesures prises à ses frais pour y remédier et éviter qu'ils ne se reproduisent.

10. Aider le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données prévues à l'article 35 du RGPD.

Le **Prestataire** aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle (article 36 du RGPD).

11. Mettre en œuvre les mesures de sécurité nécessaires au respect du RGPD.

A savoir notamment :

- La pseudonymisation, le chiffrement des données à caractère personnel, le chiffrement des sauvegardes des données à caractère personnel, le chiffrement des données à caractère personnel en transit, le chiffrement des données à caractère personnel au sein des bases de données, un dispositif de détection des violations de données à caractère personnel et la mise à disposition des traces de connexion aux données traitées pour le compte du responsable de traitement pendant toute la durée de la mission.
- Ne pas chercher à lever le pseudonymat de données pseudonymes qui lui auraient été confiées par le responsable de traitement. Informer sans délai le responsable de traitement en cas de réidentification à partir de données insuffisamment anonymisées par le responsable de traitement ;
- 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.

Concernant la sécurité des données, le sous-traitant s'engage à mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté pour la protection des données à caractères personnel.

Ces mesures techniques et organisationnelles doivent tenir compte de la doctrine de la CNIL et du Référentiel Général de Sécurité (RGS) et sont conformes aux standards de sécurité en vigueur.

Le sous-traitant s'engage à communiquer au responsable de traitement, sur simple demande, tout document décrivant sa politique de sécurité des informations, les mesures de sécurité mises en œuvre, les certifications obtenues et les résultats synthétiques des audits de sécurité qu'il fait réaliser.

Ces documents sont considérés comme confidentiels.

Engagements de sécurité

Le sous-traitant s'engage expressément à :

- Prendre en compte les principes de protection des données par défaut et dès la conception de ses outils, produits, applications ou services (Security by Default & by Design) ;
- Assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité d'accès et d'usage des données qu'il traite pour le compte du responsable de traitement ;
- Tenir à jour une documentation écrite décrivant les mesures de sécurité techniques et organisationnelles mises en œuvre à cet effet ;
- Traiter avec diligence toute demande du responsable de traitement relative à la sécurité des données traitées dans le cadre du marché **n°2025-019**;
- Rétablir dans les meilleurs délais la disponibilité et l'accessibilité des données du responsable de traitement en cas d'incident de sécurité ;
- Assurer le stockage des données du responsable de traitement séparément de ses propres données ou des données d'autres clients ;
- Restreindre l'accès aux données faisant l'objet du traitement au seul personnel habilité et autorisé à cet effet, du fait de son travail et ses fonctions, en limitant l'accès aux données strictement nécessaires à l'accomplissement de leurs tâches ;
- Veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité et reçoivent une formation nécessaire en matière de protection des données à caractère personnel ;
- Ne prendre aucune copie des documents et supports d'information confiés par le responsable de traitement, sauf si ladite copie est indispensable à la réalisation de la prestation ;
- Ne pas utiliser, ni communiquer les documents et informations traités à des finalités autres que celles définies par le marché **n°2025-019** ;
- Prendre toutes les mesures permettant d'éviter une utilisation détournée ou frauduleuse des données en cours d'exécution du marché **n°2025-019**.

Toute modification importante des mesures de sécurité mises en place par le sous-traitant doit être documentée et présentée au responsable de traitement pour évaluation. Elles ne peuvent en aucun cas réduire le niveau de sécurité des données pendant l'exécution du marché **n°2025-019**.

12. Renvoyer, au terme du marché n°2025-019, toutes les données à caractère personnel au responsable de traitement ou renvoyer les données à caractère personnel au tiers 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 **Prestataire**. Une fois détruites, le **Prestataire** doit justifier par écrit de la destruction.

13. Communiquer au responsable de traitement le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

14. Tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement (article 30 du RGPD).

Ce registre comprend :

- L'identification des parties prenantes du traitement ;
- La finalité du traitement ;
- La conservation des données ;
- Le nom et les coordonnées du responsable de traitement 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 responsable du traitement;
- 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. Sur demande expresse et spécifique du responsable de traitement, le sous-traitant s'engage à traiter les données exclusivement sur le territoire d'un Etat membre de l'Union européenne ou assurant un niveau de protection adéquat au titre de l'article 45 du RGPD ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, celles prévues au point 11 ci-avant.

Cette liste est non exhaustive.

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

Le sous-traitant sera tenu responsable en cas de manquement exclusivement imputable à lui et/ou à ses sous-traitants ultérieurs à leurs obligations en vertu du présent accord, du RGPD et de la Loi Informatique et Libertés.

A ce titre, le sous-traitant s'engage à indemniser le responsable du traitement pour tout dommage direct subi par ce dernier.

Le sous-traitant est responsable du traitement des données personnelles pendant toute la durée de la mission.

En cas de non-respect par le **Prestataire** de la présente annexe, le marché **n°2025-019** pourra être résilié pour faute du **Prestataire** dans les conditions stipulées aux **Conditions Générales**.