

ANNEXE RGPD Convention n° 2023-INT-

Entre :

La collectivité, ci-après désignée par « **le responsable de traitement** » qui désigne la notion de responsable de traitement au sens du Règlement Général sur la Protection des Données, d'une part,

Et :

Le CDG74, ci-après désigné par « **le sous-traitant** » qui désigne la notion de sous-traitant au sens du Règlement Général sur la Protection des Données, d'autre part,

I. **Objet**

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

Les présentes clauses s'appliquent aux prestations de traitement de données à caractère personnel effectuées par le sous-traitant dans le cadre de l'exécution de la convention à laquelle elles sont annexées.

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** »).

II. **Description du traitement faisant l'objet de la sous-traitance**

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) :

- Le suivi médical réglementaire des agents, et la réalisation d'actions sur le milieu du travail
- Des interventions en psychologie du travail
- La mission d'inspection (ACFI) auprès de la collectivité
- La mission d'information et de conseil en matière d'hygiène et de sécurité au travail
- L'animation d'un réseau d'assistants et de conseillers de prévention
- L'aide à l'élaboration d'un DUERP
- La mise en œuvre d'une démarche de prévention des RPS
- L'accompagnement à la mise en œuvre d'un système de management de la santé et sécurité au travail

La nature des opérations réalisées sur les données est :

- La constitution et conservation du dossier médical de santé au travail de l'agent sur support informatique et/ou sur support papier
- La constitution et conservation des rapports d'inspection de la collectivité
- La mise en œuvre d'actions spécifiques en hygiène et sécurité au sein des collectivités ou sur le territoire départemental
- La collecte de données au vu de la bonne exécution des différentes prestations prévues par la convention
- La sauvegarde et archivage de données (sur supports informatiques pluriels)
- La consultation par requête informatique nécessaire au suivi des situations individuelles ou collectives

La ou les finalité(s) du traitement sont :

- assurer la préservation de la santé au travail des agents, et leur maintien dans l'emploi
- garantir le suivi médical efficace de ces derniers
- assurer efficacement la mission d'inspection
- garantir la conformité des bâtiments, équipements et matériels aux normes techniques et réglementaires, et proposer l'ensemble des mesures correctives utiles et adaptées aux circonstances
- tracer l'ensemble des expositions professionnelles
- Suivre et analyser les causes et conséquences des AT et MP, et proposer les mesures correctives utiles
- participer utilement aux instances paritaires et représentatives intéressant la santé au travail
- prévenir les situations à risques
- participer à l'amélioration des conditions de travail
- contribuer à la bonne ergonomie des moyens mis à la disposition des agents, et le cas échéant à l'aménagement de leurs postes de travail
- apporter aux collectivités l'assistance utile à la résolution de problématiques individuelles ou collectives en lien avec le contexte professionnel

Les données à caractère personnel traitées sont :

- données administratives des agents (état civil, situation familiale, adresse, coordonnées téléphoniques/mail, situation administrative, fonction, lieu d'exercice des missions, absences, éléments d'ordre pécuniaire ou assurantiel...)
- données à caractère médical des agents dans le cadre de la constitution et la conservation de leurs dossiers médicaux
- données administratives des collectivités (organigrammes hiérarchiques ou fonctionnels, projets de service, projets d'aménagements/de construction de locaux, notes, comptes-rendus et rapports d'activité ou opérationnels...)
- Données médicales des agents victimes d'accident du travail ou de maladie professionnelle nécessaires à l'analyse de ceux-ci

Les catégories de personnes concernées sont :

- Pour la médecine/psychologie : les agents titulaires et contractuels de la collectivité adhérente, quel que soit leur statut ou temps de travail
- Pour la prévention des risques professionnels : Agents titulaires et contractuels de droit public de la collectivité adhérente, en charge des missions de prévention des risques (assistants et conseillers de prévention) et agents victimes d'accident du travail ou de maladie professionnelle

Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes :

- données administratives des agents (état civil, situation familiale, adresse, coordonnées téléphoniques/mail, situation administrative, absences...)
- Données médicales des agents, sous réserve de transmission de médecin à médecin
- Données médicales des agents victimes d'accident du travail ou de maladie professionnelle nécessaires à l'analyse de ceux-ci

III. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/ont l'objet de la sous-traitance
2. traiter les données **conformément aux instructions spécifiques documentées** du responsable de traitement figurant en annexe de la présente convention. Si le sous-traitant 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** le responsable de traitement. En outre, si le sous-traitant 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 le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

En l'absence d'instructions spécifiques documentées du responsable de traitement, les instructions figurant dans le *II. « Description du traitement faisant l'objet de la sous-traitance »* de la présente annexe seront appliquées dans le respect de la politique de protection des données du CDG74 accessible sur son site Internet.

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. **Sous-traitance**

Le sous-traitant est autorisé à faire appel à l'entité **GIP informatique des centres de gestion** (ci-après, le « *sous-traitant ultérieur* ») pour mener les activités de traitement

suivantes : gestion des données administratives et statutaires pour transfert sur le logiciel métier pour les activités médicales et de psychologie.

En cas de recrutement d'autres sous-traitants ultérieurs, le sous-traitant doit recueillir l'autorisation écrite, préalable et spécifique du responsable de traitement.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur 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 règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

7. **Droit d'information des personnes concernées**

Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

8. **Exercice des droits des personnes**

Dans la mesure du possible, le sous-traitant doit aider le 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).

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à@.....
(indiquer un contact au sein du responsable de traitement) ou par courrier postal à l'adresse indiquée en préambule de la convention en l'absence d'adresse électronique.

9. **Notification des violations de données à caractère personnel**

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 72 heures après en avoir pris connaissance et par le moyen suivant : message électronique ou courrier en l'absence d'adresse de messagerie indiquée au point 8. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

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

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 le responsable du traitement 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 du responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, 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 le responsable du traitement 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 sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations**

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relatives à la protection des données.

Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

11. **Mesures de sécurité**

Le sous-traitant s'engage à prendre toutes les précautions utiles afin de préserver la sécurité des données et notamment de les protéger contre toute destruction accidentelle ou illicite,

perte accidentelle ou illicite, altération, diffusion ou accès non autorisés, ainsi que contre toute autre forme de traitement illicite ou communication à des personnes non autorisées.

Le sous-traitant s'engage notamment à mettre en œuvre :

- 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,
- les mesures de sécurité prévues par la politique de protection des données du CDG74.

Le sous-traitant s'engage à transmettre au responsable de traitement, à sa demande, la liste des mesures de sécurité mises en œuvre.

12. **Sort des données**

Au terme de la prestation de services relative au traitement de ces données, le sous-traitant s'engage à :

Au choix des parties :

- détruire toutes les données à caractère personnel ou
- à renvoyer toutes les données à caractère personnel au responsable de traitement ou
- à renvoyer les données à caractère personnel au sous-traitant 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 sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

13. **Délégué à la protection des données**

Le sous-traitant communique 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.

Pour le CDG74, il s'agit de

David GONCALVES, société Groupe Si2A – dpo@cdg74.fr

14. **Registre des catégories d'activités de traitement**

Le sous-traitant 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 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 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées;

- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
 - o la pseudonymisation et le chiffrement des données à caractère personnel;
 - o des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
 - des 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.

15. **Documentation**

Le sous-traitant 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.

V. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s'engage à :

1. fournir au sous-traitant les données visées au II des présentes clauses
2. documenter par écrit toute instruction concernant le traitement des données par le sous-traitant
3. veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant
4. superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant

Fait en 2 exemplaires,

Pour le responsable de traitement,

Le Maire / Président

Mr / Mme

Pour le sous-traitant,

Le Président du CDG74

M. Antoine de MENTHON