AGIR AVEC CEUX QUI FONT LE LOGEMENT SOCIAL

ANNEXE RGPD

A. Préambule

Une **Donnée à Caractère Personnel** désigne toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement.

Un **Traitement** est « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ».

Le **Responsable de Traitement** est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres (les responsables conjoints de traitement), détermine les finalités et les moyens du traitement (il s'agit en principe de l'acheteur).

Le **Sous-Traitant** est un organisme traitant des Données à Caractère Personnel pour le compte, sur instruction et sous l'autorité d'un responsable de traitement (il s'agit en principe du titulaire du marché).

B. 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.

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 (ci-après, « ***le règlement européen sur la protection des données*** ») ainsi que la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après la « ***loi informatique et libertés*** »).

C. Description du traitement de données à caractère personnel

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir les prestations objet du contrat.

La CGLLS s'engage à n'utiliser les informations contenues dans les offres du titulaire, ou recueillies par l'acheteur dans le cadre de l'exécution du marché, qu'en vue respectivement de l'analyse des candidatures et des offres soumises, et pour la finalité du traitement induit par l'objet du marché.

La CGLLS s'engage également à ne pas divulguer ces informations, à ne pas les communiquer à des tiers, à l'exception de ses autorités de contrôle, à ne pas les publier, ni à les rendre publiques de quelque manière que ce soit, sauf pour satisfaire l'obligation d'information posée par l'article R. 2181-1 du Code de la commande publique.

Les données à caractère personnel font l'objet d'un traitement informatisé destiné à l'usage exclusif des services de la CGLLS, que sont le pôle des achats et de la commande publique, le pôle RH, les personnes en charge de l'analyse des offres, ainsi que les autres personnes chargées de suivre les procédures des marchés, dans la limite de leurs compétences.

Il est toutefois précisé que, en ce qui concerne le marché public qui sera signé, celui-ci et les pièces s'y rapportant deviendront des documents administratifs communicables sur le fondement du livre III du code des relations entre le public et l'administration.

Toutefois, le droit de communication de ces pièces à toute personne non partie au marché s'exerce dans le respect du secret en matière industrielle et commerciale. Les données personnelles recueillies dans le cadre du présent marché font l'objet d'un traitement par la CGLLS en sa qualité de responsable de traitement.

Lorsque le traitement de donnée confié au sous-traitant est susceptible de porter sur d'autres données à caractère personnel, le sous-traitant doit formaliser la demande de communication de ces données auprès du responsable de traitement une fois le marché attribué.

Ces demandes devront respecter les principes du RGPD, notamment celui de minimisation des données collectées.

Toute demande fera l'objet de formalités de mise en conformité au RGPD au sein de la CGLLS.

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

Le sous-traitant s'engage à :

1. **Traiter les données uniquement pour les seules finalités qui font l'objet de la sous-traitance**
2. **Traiter les données conformément aux instructions documentées du responsable de traitement figurant dans le présent contrat.**

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.

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. **Renseigner la CGLLS sur la sous-traitance envers des tiers**

Le sous-traitant peut 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 (avec accusé réception) 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 maximum de 15 (quinze) jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ultérieure ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

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. Prendre en compte le droit d'information des personnes concernées

Le sous-traitant, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données à caractère personnel concernés. La formulation et le format de l'information doit être convenue avec le responsable de traitement avant la collecte de données.

8. Veiller à l'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).

Le sous-traitant s'engage à aider la CGLLS à répondre, au nom et pour le compte du 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.

Le sous-traitant informera le délégué à la protection des données (DPO) de toute demande de droit d'accès, à l'adresse mail suivante : dpo@cglls.fr

9. Notifier les 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 48 heures après en avoir pris connaissance, à l'adresse mail suivante : dpo@cglls.fr

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.

a) Notification 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 (catégories et nombre approximatif de personnes concernées par la violation et d'enregistrements de données),
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact,
- 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.

S’il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

b) Notification aux personnes concernées

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 les mêmes éléments que la notification ci-dessus.

10. Aider la CGLLS à respecter ses obligations relatives à la protection des données

Le sous-traitant aide le responsable de traitement pour la réalisation d’analyses d’impact relatives à la protection des données ainsi que pour la réalisation de la consultation préalable de l’autorité de contrôle.

11. Mettre en œuvre des mesures de sécurité

Le sous-traitant s’engage à mettre en œuvre les mesures de sécurité visant à apporter une protection suffisante des données à caractère personnel.

Les mesures mises en œuvre par le sous-traitant doivent être adaptées à la sécurité des données confiées. Le sous-traitant détaillera les mesures de protection des données à caractère personnel mises en œuvre au sein de son organisation, le cas échéant parmi les mesures suivantes :

- l’anonymisation des données : description des mécanismes d’anonymisation, des garanties qu'ils apportent contre une ré-identification éventuelle et à quelle fin ils sont mis en œuvre,
- le cloisonnement de données : description des méthodes utilisées pour cloisonner le traitement chez le sous-traitant,
- le contrôle des accès logiques : description de la manière dont les profils utilisateurs sont définis et attribués. Il conviendra de détailler les moyens d’authentification mis en oeuvre en précisant, le cas échéant les règles applicables aux mots de passe (longueur minimale, structure obligatoire, durée de validité, nombre de tentatives infructueuses avant blocage du compte, etc.),
- la politique de journalisation : description de la politique de journalisation des événements et de conservation des traces qui en résultent,
- la politique d’archivage : description de la politique de conservation et gestion d’archives électroniques contenant des données à caractère personnel mise en oeuvre pour garantir leur intégrité, leur authenticité, leur accessibilité et leur lisibilité, pendant toute la durée nécessaire,
- la politique de sécurisation des documents papiers : description de la sécurisation de la gestion des documents papiers (de l’impression au stockage jusqu’à la destruction et aux échanges de documents),
- la politique de minimalisation des données collectées : la sensibilité des données peut être réduite à l'aide des méthodes suivantes : filtrage et retrait, réduction de la sensibilité par transformation, réduction du caractère identifiant des données, réduction de l'accumulation de données, restriction de l’accès aux données.

12. Veiller au sort des données

Au terme du traitement des données, le sous-traitant s’engage à détruire toutes les données à caractère personnel. Une fois ces données supprimées, il doit justifier par écrit de leur destruction.

13. Communiquer les coordonnées de son 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, ou, à défaut, l'identité et les coordonnées d'un point de contact dédié à ces questions.

14. **Tenir un registre d'activités de traitement de données**

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 toutes les informations détaillées à l'article 30 du règlement européen sur la protection des données.

Dans le cas où le responsable de traitement lui en fait la demande, le sous-traitant s'engage à mettre ce registre à sa disposition afin qu'il puisse s'assurer que les traitements de données mis en œuvre dans le cadre de l'exécution du présent accord-cadre sont conformes au RGPD.

15. **Mettre à disposition la documentation démontrant le respect des obligations**

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.

E. 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 C 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**