

ANNEXE 1

Engagements relatifs à la gestion des données à caractère personnel par le prestataire dans le cadre de l'appel à candidatures

« **Accompagnement Social Lié au Logement Allocation Logement Temporaire (ASLL-ALT)** »

Note Explicative

Le RGPD est applicable depuis le 25 mai 2018. L'article 28 du RGPD relatif à la sous-traitance de traitement de données à caractère personnel s'applique pleinement aux marchés publics. Cette annexe décrit toutes les obligations et apporte les garanties des cocontractants (Responsable de Traitement et Sous-traitant) afin de protéger les personnes concernées.

Procédure à suivre par le Sous-Traitant

Veillez renseigner les parties en bleu.
Et nous retourner l'Annexe complétée par vos soins.

Le Département des Hautes-Pyrénées, situé à rue Gaston Manent – CS71324 - 65013 TARBES cedex 9 et représenté par M. Le Président du Conseil Départemental (Ci-après, « **le responsable de traitement** »)

D'une part,

ET

Le candidat retenu (ci-après, « **le sous-traitant** »)

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.

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** »).

Ces engagements sont valables pour la durée globale de la convention.

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)

La mise en œuvre d'un Accompagnement Social Lié au Logement auprès des personnes accueillies et logées dans des structures au titre de l'Allocation Logement Temporaire (ALT), sur l'ensemble du département des Hautes-Pyrénées.

La nature des opérations réalisées sur les données comprend toute saisie, stockage, transmission et mise à jour de données, qu'elle soit sur papier ou sous format électronique, en utilisant les outils bureautiques, le système d'information du sous-traitant et/ou sous IODAS.

L'objectif est de protéger les données pendant tout leur cycle de vie, de la saisie jusqu'à la destruction.

La ou les finalité(s) du traitement sont l'accompagnement de ce public dans l'élaboration et réalisation d'un projet logement réaliste et adapté à leurs besoins (cf chapitre 1 de l'appel à candidatures).

Les données à caractère personnel traitées sont uniquement celles strictement nécessaires au traitement du dossier (au sens de l'article Art L121-6-2 al 5 du CASF) et en particulier :

- l'Identité des personnes concernées (les membres du foyer)
- date et lieu de naissance de chacun,
- le lieu de résidence habituel,
- la situation familiale (personne seule, couple, couple avec enfants, parent seul avec enfant(s))
- les ressources du foyer, les charges (le budget du ménage), y compris l'existence de dettes ou de dossier de surendettement lorsque cela est nécessaire au traitement du dossier
- les éléments consignés dans le rapport d'évaluation sociale sous IODAS, en cas de demande d'aide financière
- les éléments consignés dans le document sous IODAS, établissant les objectifs de la personne vis-à-vis du logement, ainsi que le bilan des actions mises en place
- identification des structures assurant un suivi social de la situation, de façon concomitante avec l'ASLL-ALT
- les éléments à transmettre dans le cadre d'une demande de logement social, tels listés dans le cerfa 14096*05 et selon l'arrêté du 20 avril 2023 modifiant l'arrêté du 22 décembre 2020, relatif au nouveau formulaire de demande de logement locatif social et aux pièces justificatives fournies pour l'instruction de la demande de logement locatif social

Les catégories de personnes concernées sont des personnes accueillies et logées dans des structures agréées, au titre de l'Allocation Logement Temporaire (ALT), sur l'ensemble du département des Hautes-Pyrénées.

Pour l'exécution du service objet de l'appel à candidature, le responsable de traitement met à la disposition du sous-traitant un accès à son système d'information de l'action sociale. Cet accès sera réalisé via l'extranet du Département. Le règlement des usages du SI s'applique pour toute personne accédant à notre SI et le sous-traitant s'engage à le respecter et à le faire signer à ses agents (cf annexe 2). Le sous-traitant n'aura accès qu'aux dossiers des seules personnes accompagnées. Des comptes nominatifs (respect du principe RGPD) des agents du sous-traitant seront créés par le CD65.

Pour information

Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement organisation, conservation, adaptation, modification, extraction consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement).

Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

*Un traitement de données doit avoir un **objectif**, une finalité déterminée préalablement au recueil des données et à leur exploitation.*

Exemples de traitements : tenue du registre des sous-traitants, gestion des paies, gestion des ressources humaines, etc.

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/font l'objet de la sous-traitance
2. traiter les données **conformément aux instructions documentées** du responsable de traitement figurant en annexe du 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. Sous-traitance – autorisation spécifique

NB : La sous-traitance de l'accompagnement social n'est pas autorisé. Ce paragraphe concerne uniquement la sous-traitance dans le traitement des données (maintenance informatique...)

Le sous-traitant est autorisé à faire appel à l'entité [... *Le sous-traitant précise ici l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance*] (ci-après, le « **sous-traitant ultérieur** ») pour mener les activités de traitement suivantes : [...*Le sous-traitant détaille ici clairement les activités de traitement de données sous-traitées*]

[Le paragraphe précédent est à renseigner autant de fois qu'il y a de sous-traitants ultérieurs]

En cas de recrutement d'autres sous-traitants ultérieurs en cours d'exécution du marché, le sous-traitant doit recueillir l'autorisation écrite, préalable et spécifique du responsable de traitement en précisant l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance, et en détaillant clairement les activités de traitement de données sous-traitées.

Respect des obligations par les sous-traitants ultérieurs

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

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 qu'il réalise. La formulation et le format de l'information (conformément aux articles 12,13 et 14 du RGPD doit être convenue avec le responsable de traitement avant la collecte de données.

En application de l'article 13 du Règlement Général sur la Protection des Données Personnelles (RGPD), le sous-traitant s'engage, dès la proposition de l'accompagnement ASLL-ALT, à présenter l'ensemble des règles de protection des données à la personne concernée et s'en assurer de sa compréhension. Un modèle d'information à la personne est proposé (cf annexe 1_bis). Le sous-traitant peut en fournir un autre, à condition d'être en conformité avec les mentions de la CNIL (<https://www.cnil.fr/fr/exemples-de-formulaire-de-collecte-de-donnees-caractere-personnel>).

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 au référent de l'appel à candidature [service.logement@ha-py.fr].

9. Notification des violations de données à caractère personnel

9.1. Information du sous-traitant au responsable de traitement

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 et par le moyen suivant [par courriel : delegue.donnees@ha-py.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.

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.

9.2 Information à la CNIL

Le responsable de traitement notifie à l'autorité de contrôle compétente (la **CNIL**), les violations de données à caractère personnel.

9.3. Information à la personne concernée

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 relative 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 mettre en œuvre les mesures de sécurité suivantes :

[Le sous-traitant doit ici décrire de manière précise les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté aux risques en fonction de l'objet de l'appel à candidatures]
[Le sous-traitant décrira, entre autres :

- *la pseudonymisation et le chiffrement des données à caractère personnel*
- *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]*
- *Moyens d'échanges sécurisés de données à caractère personnel entre le sous-traitant et le responsable de traitement*

[Le sous-traitant peut également annexer un document (par exemple un mémoire technique) décrivant l'ensemble des mesures de sécurité mises en œuvre].

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité prévues par :

-[code de conduite, certification : le sous-traitant précise ici s'il respecte un code de conduite ou de certification].

Pour vous aider, vous pouvez vous appuyer sur le kit de sécurité proposé par le site de l'ANSSI sur ce [sujet](#).

Le Département impose les mesures de sécurité suivantes :

- Transmission du bilan d'activité, version anonymisée via la plateforme sécurisée de transfert de fichiers du Département (Nextcloud)

[Commentaire - Dans la mesure où l'article 32 du règlement européen sur la protection des données prévoit que la mise en œuvre des mesures de sécurité incombe au responsable du traitement et au sous-traitant, il est recommandé de déterminer précisément les responsabilités de chacune des parties au regard des mesures à mettre en œuvre].

12. Sort des données

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

Ne conserver que les informations strictement nécessaires pour le traitement du dossier, conformément à ses obligations légales et en respectant le Code de l'Action Sociale et des Familles. Le Département est responsable des données saisies dans l'appliquatif métier IODAS.

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.

Nom, Prénom du DPO : [...]

Courriel : [...]

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 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;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
 - la pseudonymisation et le chiffrement des données à caractère personnel;
 - 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.

IV. 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 du présent document
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.