Annexe au CCAE : obligations relatives à protection des données

# I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le titulaire s’engage à effectuer pour le compte du pouvoir adjudicateur (ci-après « 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 »).

# II. Description du traitement faisant l’objet du marché

Le titulaire est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) objet du présent marché.

La nature des opérations réalisées sur les données est l’accompagnement des propriétaires dans la réalisation d’un projet de réhabilitation de leur logement, qu’ils soient occupants, bailleurs ou en copropriété. En copropriété, les missions peuvent, en amont des travaux, viser le rétablissement de l’organisation tant juridique administrative que financière. Pour accomplir les missions, la tenue de bases de données à caractère personnel est nécessaire.

La ou les finalité(s) du traitement sont le recensement des situations, le suivi des dossiers aux différentes étapes, jusqu’au paiement des subventions par l’Anah et les collectivités locales. D’autres organismes sociaux (Carsat, CAF, ..) ou bancaires (SACICAP) peuvent être associés à l’accompagnement des propriétaires.

Les données à caractère personnel traitées sont l’identité des personnes accompagnées ainsi que leur patrimoine, la situation géographique et administrative des (co)propriétés, les processus d’organisation et de réalisation des projets de réhabilitation ou d’organisation, intégrant les budgets et plans de financements des opérations réalisées.

Les catégories de personnes concernées sont les propriétaires, les syndics et les occupants des logements traités.

Pour l’exécution du service objet du présent contrat, le responsable de traitement met à la disposition du titulaire, à sa demande, les informations nécessaires suivantes : historique des études et des aides apportées sur le bien, informations du Registre National des copropriétés et tout information relative à la bonne exécution de la mission (rapports de visite, arrêtés d’insalubrité, de péril, etc..).

# III. Obligations du titulaire vis-à-vis du responsable de traitement

Le titulaire s'engage à :

1. **traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l’objet du marché ;**
2. **traiter les données conformément aux instructions du responsable de traitement.**

Si le titulaire 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 titulaire 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 ;

1. **garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent marché ;**
2. **veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent marché :**
* **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**
1. **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**
2. **Sous-traitance :**

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

1. **Droit d’information des personnes concernées**

Le titulaire, 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 doit être convenue avec le responsable de traitement avant la collecte de données.

1. **Exercice des droits des personnes**

Dans la mesure du possible, le titulaire 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 titulaire doit 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 du présent marché.

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

Après accord du responsable de traitement, le titulaire 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 titulaire 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.
1. **Aide du titulaire dans le cadre du respect par le responsable de traitement de ses obligations**

Le titulaire aide le responsable de traitement pour la réalisation d’analyses d’impact relative à la protection des données.

Le titulaire aide le responsable de traitement pour la réalisation de la consultation préalable de l’autorité de contrôle.

1. **Mesures de sécurité**

Le titulaire s’engage à mettre en œuvre les mesures de sécurité suivantes :

* 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
1. **Sort des données**

Au terme de la prestation de services relatifs au traitement de ces données, le titulaire s’engage à :

* à renvoyer toutes les données à caractère personnel au responsable de traitement
* Le renvoi doit s’accompagner de la destruction de toutes les copies existantes dans les systèmes d’information du titulaire.
* Une fois détruites, le titulaire doit justifier par écrit de la destruction.
1. **Délégué à la protection des données**

Le titulaire 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.

1. **Registre des catégories d’activités de traitement**

Le titulaire 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.
1. **Documentation**

Le titulaire 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 titulaire

Le responsable de traitement s’engage à :

* fournir au titulaire les données visées au II des présentes clauses
* documenter par écrit toute instruction concernant le traitement des données par le titulaire
* 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 titulaire
* superviser le traitement, y compris réaliser les audits et les inspections auprès du titulaire