Annexe 4 – Clause RGPD de sous-traitance

Dans cette annexe :

- **le responsable de traitement est la Commune de xxxxxxxxxxxxxx**
- **le sous-traitant est Clermont Auvergne Métropole**

I. Règlement européen sur la protection des données personnelles .

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 définie dans la Convention d'adhésion de la commune au service commun d'instruction des Autorisations du Droit des Sols. 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 l'exécution des prestations objet de la Convention d'adhésion de la commune au service commun d'instruction des Autorisations du Droit des Sols.

La nature des opérations réalisées sur les données peut-être :

- traitements de reprise, de récupération ou de nettoyage de données
- traitements de transfert , d'import/export, de copies temporaires de données
- traitements de sauvegarde/restauration, réplication
- traitements de consultation et de modification
- traitements de sécurisation : chiffrement/déchiffrement, pseudonymisation …
- divers autres usages liées aux obligations des prestations prévues.

Les finalités des traitements sont décrites dans la convention et couvrent l'ensemble de la procédure d'instruction des autorisations et actes relatifs à l'occupation des sols, à compter du dépôt de la demande auprès de la commune jusqu'à la notification par le Maire de sa décision.

Les données à caractère personnel traitées sont celles qui sont requises par le code de l'urbanisme notamment pour instruire les demandes des usagers. Les catégories de personnes concernées sont principalement les pétitionnaires, les personnes contacts internes ou externes intervenant dans l'instruction des demandes.

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

- la liste, les qualifications et les informations de contact des personnels de la Collectivité intervenant dans le processus de prestations de services
- le cas échéant la liste, les qualifications et les informations de contact des personnels des autres sous-traitants de la Collectivité intervenant dans le processus de prestations de services
- toutes les procédures, codes d'accès, moyens techniques ou physiques et tout autre document utile pour permettre l'exécution des services objet du contrat dans les meilleures conditions (télémaintenance, pris de main à distance, documentations techniques …).
- l'accès aux règlements de la Collectivité

III. 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 du responsable de traitement. 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.

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 ainsi que les obligations de procéder à une analyse d'impact sur le protection des données.

6. **Sous-traitance**

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 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 minium de 10 jours 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.

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 oeuvre 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 coordonnées DPO ou autre Commune

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 4 heures après en avoir pris connaissance et par courrier électronique à coordonnées DPO ou autre Commune. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement d'évaluer si il y a nécessité 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.

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'une analyse d'impact relative à la protection des données lorsqu'elle est requise. 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 oeuvre les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, y compris, entre autres :

- 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.
- le cas échéant la pseudonymisation et le chiffrement des données à caractère personnel

Le sous-traitant s'engage à mettre en oeuvre toutes les mesures de sécurité prévues par les textes et recommandations en vigueur dans notre contexte public : notamment le RGS Référentiel Général de Sécurité et les recommandations de l'ANSSI.

Ces mesures s'appliquent dès lors que le sous-traitant agit avec des moyens humains et techniques placés sous sa responsabilité qui ne dépendent pas directement de la Collectivité (infrastructures, INTERNET, personnels …).

12. **Sort des données**

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage 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 sous-traitant et de tous les acteurs éventuels de la chaîne de sous-traitance sous sa responsabilité . Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

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

Nom et coordonnées du Délégué à la Protection des Données du responsable de traitement :
xxxxxxxxxxxxx
xxxxxxxxxxxx

Nom et coordonnées du Délégué à la Protection des Données du sous traitant :
Philippe BOST
E-mail : cnil@clermontmetropole.eu

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.

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. documenter par écrit toute instruction concernant le traitement des données par le sous-traitant

2. 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

3. superviser le traitement, y compris réaliser le cas échéant les audits et les inspections auprès du sous-traitant , de notifier cette violation à l'autorité de contrôle compétente.