ANNEXE 3 OBLIGATIONS RELATIVES À LA PROTECTION DES DONNÉES

I. Objet

Le présent document décrit les dispositions que le délégataire doit mettre en œuvre pour répondre aux exigences de protection des données personnelles et de sécurité informatique de la Métropole Aix-Marseille-Provence.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement en matière de sécurité des systèmes d'information et de protection des données personnelles 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 »).

Ce document est complété par le document PAS – Plan d'assurance sécurité, qui précise les mesures techniques et organisationnelles mises en œuvre par le délégataire.

II. Obligations du délégataire

Le délégataire s'engage à :

1. **traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet du marché ;**

En outre, si le délégataire 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 la Métropole Aix-Marseille-Provence avant la mise en œuvre du traitement ;

2. **garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat ;**

3. **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 ; et reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;**

4. **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 ;**

5. **Sous-traitance :**

Le sous-traitant éventuel du délégataire est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au délégataire 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 délégataire demeure pleinement responsable devant le responsable de traitement de l'exécution par le sous-traitant de ses obligations.

6. Droit d'information des personnes concernées

Le délégataire 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 définie avant la collecte de données.

7. Exercice des droits des personnes

Le délégataire doit 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).

Il doit répondre aux demandes des personnes concernées dans les délais prévus par le règlement européen sur la protection des données, via une adresse mail dédiée.

8. Notification des violations de données à caractère personnel

Le délégataire doit notifier toute violation de sécurité et/ou de données à caractère personnel dans un délai maximum de 72 heures après en avoir pris connaissance aux adresses mails fournies par la Métropole Aix-Marseille-Provence, avec copie à l'adresse dpo@ampmetropole.fr et rssi@ampmetropole.fr.

Le délégataire enregistre la violation dans son registre des violations.

Le délégataire notifie à l'autorité de contrôle compétente (la CNIL), les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures calendaires 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 la Métropole Aix-Marseille-Provence 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.

Le délégataire communique 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 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. Réalisation d'une analyse d'impact relative à la protection des données

Le délégataire réalise les analyses d'impact relative à la protection des données.

Le délégataire réalise éventuellement la consultation préalable de l'autorité de contrôle.

10. Mesures de sécurité

Le délégataire s'engage à mettre en œuvre les mesures de sécurité techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, y compris, 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.

Le détail des mesures de sécurité est précisé dans les pièces du contrat et dans le PAS.

11. Sort des données

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

- transmettre à la Métropole Aix-Marseille-Provence une copie du fichier Abonnés comme stipulé à l'article R2224-18 II du Code Général des Collectivités Territoriales ;
- conserver les données personnelles uniquement dans un objectif de respect des obligations comptables ;
- détruire toutes les copies existantes dans le système d'information du délégataire des données personnelles au-delà du délai de conservation des obligations comptables.

12. Délégué à la protection des données

Le délégataire communique à la Métropole Aix-Marseille-Provence 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.

13. Registre des catégories d'activités de traitement

Le délégataire déclare tenir par écrit un registre des activités de traitement comprenant :

- Le cas échéant, le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants
- Le cas échéant, le nom et les coordonnées 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;
- une description générale des mesures de sécurité techniques et organisationnelles.

14. Documentation

Le délégataire met à la disposition de la Métropole Aix-Marseille-Provence la documentation nécessaire dans le cadre du contrat pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par la Métropole Aix-Marseille-Provence ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

IV. Description détaillée du traitement

[à compléter par le délégataire]

Définition du niveau de responsabilité des parties :

☐ Identification du responsable de traitement :
☐ Identification du sous-traitant au sens du RGPD :

Le délégataire traite les données à caractère personnel nécessaires pour fournir le service, objet du contrat :

La ou les finalité(s) du traitement sont : [décrire pour quels objectifs l'échange de données personnelles est mis en place]

La durée du traitement est :

La nature des opérations réalisées sur les données est : **[cases à cocher]**

☐ Consultation : le délégataire
☐ Collecte / Saisie : le délégataire
☐ Analyse : le délégataire
☐ Conservation / Stockage : le délégataire
☐ Communication / Partage : le délégataire
☐ Effacement / Suppression / Destruction : le délégataire
☐ Enregistrement : le délégataire
☐ Extraction : le délégataire
☐ Interconnexion : le délégataire
☐ Limitation : le délégataire
☐ Modification : le délégataire
☐ Suivi : le délégataire
☐ Envoi / Transfert / Transmission : la Métropole

Les données à caractère personnel traitées sont : **[cases à cocher]**

☐ Données d'état-civil (nom, sexe, date de naissance, âge,…)
☐ Coordonnées (adresse mail, adresse postale, numéro de téléphone, …)
☐ Données d'identification (identifiant, mot de passe, matricule, numéro client, …)
☐ Données liées à la vie personnelle (habitudes de vie, situation familiale,…)
☐ Données d'ordre économique et financier (revenus, situation fiscale, numéro de carte de crédit,…)
☐ Données de connexion (adresse IP, logs,…)
☐ Données de localisation (déplacement, point de géolocalisation,…)
☐ Données sensibles : origines raciales
☐ Données sensibles : origines ethniques
☐ Données sensibles : opinions politiques
☐ Données sensibles : convictions religieuses
☐ Données sensibles : convictions philosophiques
☐ Données sensibles : appartenance syndicale
☐ Données sensibles : données génétiques
☐ Données sensibles : données biométriques
☐ Données sensibles : données de santé
☐ Données sensibles : numéro de sécurité sociale
☐ Données sensibles : orientation sexuelle
☐ Données sensibles : condamnations pénales
☐ Données sensibles : infractions

Les catégories de personnes concernées sont : [cases à cocher]

☐ Employés / salariés/ agents
☐ Utilisateurs
☐ Adhérents
☐ Etudiants / élèves

☐ Personnel militaire
☐ Clients / usagers
☐ Patients
☐ Mineurs
☐ Personnes âgées
☐ Personnes en difficulté sociale

Fait à ……..

Le ……..

Nom et signature :