ANNEXE N° 2 A L'ACTE D'ENGAGEMENT

Numéro de la consultation : 2021-50502_0022

Obligations relatives à la protection des données personnelles et à la politique de sécurité de la Ville de Marseille

I. Objet

La présente annexe a pour objet de définir les conditions dans lesquelles le Titulaire s'engage à effectuer pour le compte de la Collectivité les opérations de traitement de données à caractère personnel conformément à l'article 5 du CCAG applicable au marché entré en vigueur le 1er avril 2021 ; le Titulaire s'engage également à respecter les consignes de sécurité édictées par la Collectivité.

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 Général sur la Protection des Données* »).

II. Description détaillée du traitement

Partie à compléter par le candidat / titulaire

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

Durée du service fourni par le Titulaire

.....

Nature des opérations réalisées par le Titulaire sur les données
[à compléter précisément pour décrire le traitement, par exemple : collecte de données personnelles, consultation, modification, analyse, sauvegarde, maintenance,…]

……..….…..……..........…......……..…...........….……............……..…...…….……….........……....….
……..…..………………………………………………..….…..….……………………….

Finalité(s) du traitement

……
………………………………………………………………………………………………...

Type de données à caractère personnel collectées et traitées *: [cocher les cases correspondant à votre traitement]*

❐ Données d'état-civil, données d'identification, images

❐ Données concernant la vie personnelle (habitudes de vie, situation familiale,etc)

❐ Informations d'ordre économique et financier (revenus, situation financière, situations fiscale, etc)

❐ Données de connexion (adresse IP, logs, etc)

❐ Données de localisation (déplacements, données GPS, adresse,etc)

❐ Données sensibles - origines raciales ou ethniques, opinions politiques, religieuses ou philosophiques, appartenance syndicale, orientation sexuelle

❐ Données sensibles – données génétiques, biométriques, données de santé

❐ Données sensibles – condamnations pénales, infractions

❐ Données sensibles – Numéro de Sécurité Sociale (NIR)

Catégories de personnes concernées :

❐ Agents de la Ville de Marseille

❐ Citoyens, administrés

❐ Personnel du titulaire

❐ Personnes vulnérables

❐ Autres (préciser) : ………………………

III. Obligations du Titulaire vis-à-vis de la Ville de Marseille, 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 de la Collectivité, responsable de traitement.**
   Si le Titulaire considère qu'une instruction constitue une violation du Règlement Général sur la Protection des Données ou de toute autre disposition du droit de l'Union ou du droit des États membres relative à la protection des données, il en informe immédiatement la Collectivité.
   En outre, conformément à l'article 5.2.1 du CCAG TIC, 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'État membre auquel il est soumis, il doit informer la Collectivité 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 marché**

4. **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 ; et 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 du Titulaire**

   Le sous-traitant du Titulaire est tenu de respecter les obligations du présent marché 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.

7. **Droit d'information des personnes concernées**

En amont de la collecte de toute donnée à caractère personnel, la formulation et le format de l'information à fournir aux personnes concernées doit être convenu entre la Collectivité et le Titulaire.
Au moment de la collecte des données, le Titulaire doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise.

8. **Exercice des droits des personnes**

Dans la mesure du possible, le Titulaire doit aider la Collectivité 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 informer la Collectivité, responsable de traitement, et répondre, au nom et pour le compte du responsable de traitement, 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.

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

Une violation de données à caractère personnel se définit par une perte de disponibilité, d'intégrité ou de confidentialité de données personnelles, de manière accidentelle ou illicite.

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 les mêmes éléments que ceux fournis à l'autorité de contrôle.

10. Devoir de conseil du Titulaire dans le cadre du respect par la Collectivité de ses obligations

Le titulaire est tenu à une obligation permanente de conseil et de mise en garde, relative aux matériels, logiciels et prestations fournies à la Collectivité.

Dans ce cadre, le titulaire communique notamment à la Collectivité toute information permettant d'améliorer le niveau de sécurité du système d'information et signale les difficultés et risques que certains choix peuvent entraîner dès lors que cette information relève des prestations objet du marché.

Lorsque cela est nécessaire, le Titulaire aide la Collectivité pour la réalisation d'analyses d'impact relative à la protection des données et pour la réalisation de la consultation préalable de l'autorité de contrôle.

Dans l'hypothèse où le titulaire ne respecte pas cette obligation, il ne peut se prévaloir d'une incohérence dans le marché pour s'exonérer de sa responsabilité.

11. Mesures de sécurité

La Collectivité indique ci-dessous au Titulaire les mesures générales organisationnelles et techniques qu'elle met en œuvre dans son Système d'Information pour répondre aux exigences réglementaires :

Accès sécurisé au SI

Afin d'assurer la sécurité de son Système d'Information, tout en permettant aux titulaires de télé-maintenir les serveurs et/ou les applicatifs dont ils ont la charge, la Ville de Marseille met à leur disposition une solution d'accès sécurisé via Internet.

La Ville de Marseille a validé la solution OPENVPN comme unique moyen d'accéder à son Système d'Information depuis Internet dans le cadre d'une télémaintenance sur des serveurs. Elle fournit, pour ce faire, un installeur ainsi qu'un certificat et un mot de passe associé à ce dernier.

Concernant l'envoi du certificat et de son mot de passe, afin de sécuriser leurs transmissions, il est impératif d'indiquer une adresse de courriel et un numéro de téléphone portable pour lesquels le demandeur est le seul utilisateur; il peut s'agir d'un numéro personnel, la Ville de Marseille n'utilisera en aucun cas celui-ci à d'autres fins que l'envoi du mot de passe VPN.

Cette solution implique également la création d'un compte d'accès externe individuel pour chaque personnel intervenant au nom du Titulaire.

La mise en œuvre de cette solution d'accès sécurisé engage le Titulaire à accepter les conditions d'utilisation suivantes :

- Les postes du Titulaire utilisés pour la télémaintenance devront avoir un antivirus à jour et actif ainsi qu'un système d'exploitation à jour et supporté par les labels propriétaires (Apple ; Linux ; Windows).

- Le Titulaire accepte que tout poste établissant une liaison VPN avec le réseau de la Ville de Marseille se retrouve isolé de son propre réseau durant la télémaintenance.

- Les personnels du Titulaire destinataires d'un mot de passe doivent le changer à la première utilisation. Il doit être conforme à la politique de mot de passe de la Ville de Marseille (12 caractères minimum ; contenir des caractères numériques, lettres minuscules et/ou majuscules, caractères spéciaux; ne pas être lié à l'identité de l'utilisateur) et ne doit jamais être enregistré dans l'application.

- Les intervenants du Titulaire accéderont aux seuls serveurs et/ou aux applicatifs dont le Titulaire assure la maintenance. Toute tentative d'accès à d'autres ressources sera considérée comme une atteinte à la Sécurité du Système d'Information de la Ville de Marseille, qui pourra prendre à l'encontre du Titulaire les mesures et sanctions adéquates (cf Art 323-1 du nouveau code pénal relatif à l'accès frauduleux et au maintien dans tout ou partie d'un système d'information).

- Le Titulaire prendra toutes les dispositions nécessaires lui permettant de maintenir un historique des interventions (date, heure, identité de l'intervenant, actions réalisées, ...).

La Ville de Marseille autorise cet accès sécurisé dans les plages horaires suivantes : 6h30 à 23h (heure française), 7 jours sur 7 ;

Les autorisations d'accès délivrées aux personnels du Titulaire ne sont valables que pendant la durée du marché en cours et doivent être systématiquement renouvelées tous les douze mois.

Le Titulaire indique ci-dessous les mesures organisationnelles et techniques qu'il s'engage à mettre en œuvre pour assurer la sécurité, la confidentialité, la traçabilité et l'intégrité des données à caractère personnel.

Partie à compléter par le candidat / titulaire

Les mesures organisationnelles mises en place sont les suivantes : ……..
……..
……..
……...

Les mesures techniques mises en place sont les suivantes : ……..
……..
……..
……...

12. **Sort des données**

Au terme de la prestation de services relatifs au traitement de ces données, quelle qu'en soit la cause, le Titulaire s'engage à détruire toutes les données à caractère personnelle.

13. **Délégué à la Protection des Données**

Le Titulaire communique à la Collectivité 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 Général sur la Protection des Données

Partie à compléter par le candidat / titulaire

Nom et prénom du DPO :……..……

Adresse mail du DPO :……

Téléphone du DPO : ……

14. **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 de la Collectivité, responsable de traitement comprenant :
- le nom et les coordonnées des représentants de la Collectivité 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 de la Collectivité;
- 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 Général 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 :
    - 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.

15. **Documentation**

Le Titulaire met à la disposition de la Collectivité, 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 la Collectivité ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

IV. Obligations de la Collectivité responsable de traitement vis-à-vis du Titulaire

La Ville de Marseille s'engage à :

- 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 Général sur la Protection des Données de la part du Titulaire
- superviser le traitement, y compris réaliser les audits et les inspections auprès du Titulaire