Mairie de Carqueiranne
COMMUNE
Service des Marchés Publics
Place de la République
83320 CARQUEIRANNE
Tél : 04 94 01 40 40

ANNEXE RELATIVE AU RGPD DANS LES MARCHES PUBLICS

Déléguée à la protection des données du prestataire :

SICTIAM

Business Pôle 2 – 1047 route des Dolines

CS70257

06905 SOPHIA ANTIPOLIS CEDEX

Délégué à la protection des données "COLLECTIVITE"

VALENTIN Audrey

audrey.valentin@carqueiranne.fr

04 94 01 40 60

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** » ou « **le RGPD** »).

La présente annexe a 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 au sens du RGPD ci-après.

- Les obligations du responsable de traitement vis-à-vis du sous-traitant.

Les dispositions ci-après définies s'appliqueront à chaque fois que les prestations de services du sous-traitant peuvent le conduire à accéder à des données à caractère personnel provenant du responsable de traitement dans le cadre des traitements visés dans la présente.

I. OBLIGATIONS DU SOUS-TRAITANT VIS-A-VIS DU RESPONSABLE DE TRAITEMENT

1.1 Qualification des parties

La Commune de Carqueiranne reconnait revêtir la qualité de « responsable de traitement » c'est à dire être la seule personne habilitée à déterminer la finalité du traitement des données personnelles recueillies.

Le prestataire reconnait revêtir la qualité de « sous-traitant » c'est-à-dire traiter les données personnelles recueillies pour le compte, sur instruction ou sous l'autorité de la Commune de Carqueiranne, sans pouvoir déterminer la finalité du traitement des dites données.

1.2 Obligations du sous-traitant et description du traitement faisant l'objet de la sous-traitance

Le sous-traitant s'engage à :

1.2.1 Traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l'objet de la sous-traitance ;

1.2.2 Traiter les données **conformément aux instructions documentées** du responsable de traitement tel que prévu dans le 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 États 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'État 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 ;

Dans ce cadre, 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 services décrits au "III. DESCRIPTION DU TRAITEMENT FAISANT L'OBJET DE LA SOUS-TRAITANCE".

1.2.3 Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat, notamment :

- Ne prendre aucune copie des documents et supports d'informations comportant des données à caractère personnel ou des données à caractère personnel elles-mêmes, à l'exception de celles nécessaires pour les besoins de l'exécution de sa prestation, objet du Contrat ;
- Ne pas utiliser les documents et données à caractère personnel à des fins autres que celles spécifiées au Contrat ;
- Ne pas divulguer ces documents ou données à caractère personnel à des tiers non autorisés.

- Veiller à ce que **les personnes autorisées à traiter les données à caractère personnel** en vertu du présent avenant :

  - 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

- 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**.

1.3 Sous-traitance ultérieure

Le sous-traitant peut également 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 de quinze (15) jours à compter de la date de réception de cette information pour présenter par écrit 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 est autorisé à faire appel à d'autres sous-traitants dans le cadre des services de maintenance et d'hébergement fournis à la personne publique responsable de traitement.

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 son sous-traitant ultérieur de ses obligations.

Si le cas se présente :

Liste des sous-traitants intervenant au titre du présent marché

Noms et coordonnées

1.4 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.

1.5 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 à caractère personnel, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées exercent directement auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique au Délégué à la Protection des Données.

1.6 Violation de données

En cas de violation des données avérée ou suspectée susceptible de compromettre la sécurité des données à caractère personnel auxquelles le sous-traitant a accès (destruction, perte, altération, divulgation, accès non autorisé à des données à caractère personnel, de manière accidentelle ou illicite), le sous-traitant devra immédiatement :

- Prendre toutes mesures nécessaires pour en atténuer les conséquences et pour empêcher qu'une telle violation puisse perdurer et/ou se reproduire.

- Notifier au responsable de traitement dans les 60 (soixante) heures à compter de la découverte de la violation des données et par tous moyens écrits y compris les correspondances électroniques la cause, la nature et ainsi que l'étendue des données à caractère personnel affectées et le tenir informé de l'ensemble des mesures correctives prises. 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.

- Procéder aux investigations permettant de fournir par écrit, au fur et à mesure de leur réalisation, au responsable de traitement toute information utile sur la nature et l'étendue des données à caractère personnel éventuellement déjà affectées et les mesures correctrices prises ou envisagées.

1.7 Documentation - Audits

Le sous-traitant met à la disposition du responsable de traitement les informations nécessaires pour démontrer le respect de ses obligations prévues à l'article 28 du RGPD et pour lui permettre de réaliser des audits, y compris des inspections, aux frais du responsable de traitement. Ils doivent permettre notamment de s'assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées sans que cela ne soit détecté et notifié.

L'audit sera mené par le responsable du traitement ou un auditeur qu'il aura mandaté, non-concurrent du sous-traitant, et soumis à une obligation de confidentialité.

Le responsable de traitement s'engage à notifier avec un préavis minimum de quinze (15) jours au sous-traitant tout audit, en lui communiquant notamment l'objet de la mission, la date de l'audit, la durée envisagée, et le nom du ou des auditeur(s).

Le sous-traitant ne pourra pas refuser, sans motif légitime, l'auditeur choisi par le responsable de traitement pour réaliser cet audit.

Le sous-traitant mettra en place les moyens raisonnables pour permettre à l'auditeur de mener à bien son audit. Les opérations d'audit et les demandes d'information devront être effectuées pendant les heures normales d'ouverture du sous-traitant et ne devront pas perturber le bon fonctionnement des activités de ce dernier.

Au titre de cette assistance fournie au responsable de traitement par le sous-traitant, ce dernier interviendra sans frais supplémentaire pour le responsable de traitement dans la limite de deux (2)

jours/homme par an. Toute mobilisation complémentaire de ressource du sous-traitant pour cette assistance sera facturée au responsable de traitement.

Un exemplaire du rapport d'audit sera remis gracieusement au sous-traitant. Les parties examineront de bonne foi ce rapport dans le cadre d'un comité de pilotage, et identifieront, le cas échéant, les actions qui devront être engagées par l'une ou l'autre des parties pour mettre en œuvre les décisions prises lors de ce comité. Ce rapport est confidentiel et strictement réservé aux parties. Si le rapport fait apparaitre un manquement aux obligations du sous-traitant, ce dernier s'engage à mettre en œuvre, à ses frais, toute mesure corrective appropriée dans un délai de 3 mois. En cas de contestation du rapport d'audit par le sous-traitant, ce dernier proposera à ses frais un nouvel audit par un autre cabinet de son choix.

Le responsable de traitement ne pourra pas réaliser plus d'un audit du sous-traitant sur une période glissante de 12 mois, sauf accord de ce dernier.

1.8 Aide du Sous-traitant

Sur demande du responsable de traitement, et après accord sur la proposition technique et financière du sous-traitant, ce dernier peut apporter son aide au responsable de traitement pour l'assister dans la réalisation d'analyses d'impact relatives à la protection des données à caractère personnel, ainsi que pour la préparation de la consultation préalable de l'autorité de contrôle.

La personne publique responsable du traitement demeure seule maître de la finalité du traitement et de la décision de soumettre ou non le traitement, après conseil du sous-traitant, à une analyse d'impact ou une consultation préalable de l'autorité de contrôle nationale.

1.9 Sécurité

Le sous-traitant s'engage conformément à la règlementation applicable à la protection des données à caractère personnel, à mettre en œuvre les mesures techniques et organisationnelles appropriées au regard de la nature des données et des risques présentés par le traitement, afin de préserver la confidentialité, la sécurité et l'intégrité des données à caractère personnel auxquelles il pourra avoir accès à l'occasion de la réalisation des prestations, et notamment empêcher toute déformation, altération, endommagement, destruction de manière fortuite ou illicite, perte, divulgation et/ou tout accès par des tiers non autorisés préalablement.

Afin de garantir un niveau de sécurité adapté, le sous-traitant mettra notamment en œuvre, en tenant compte des risques pour la sécurité des données à caractère personnel et pour la vie privée des personnes, selon les besoins et les caractéristiques du marché, les mesures de sécurité appropriées telles que

- 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.
- Sécurité des traitements de support.
- Sécurité des traitements de reprise de données et répartition des responsabilités.

1.10 Sort des données

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

- À renvoyer toutes les données à caractère personnel au responsable de traitement dans les conditions spécifiées par celui-ci,
- Détruire, et à en justifier par écrit la destruction, toutes les données à caractère personnel présentes dans ses systèmes d'information, sauf si leur conservation est exigée en vertu de l'article 28 du RGPD.

1.11 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.

Pour le présent marché :

1.12 Tenue du registre

Le sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, conformément aux dispositions du RGPD, 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 ;

- Une description générale des mesures de sécurité techniques et organisationnelles.

Le sous-traitant donnera accès au registre au responsable de traitement sur demande.

1.13 Localisation des données

Le sous-traitant s'engage à opérer le traitement et héberger ces données en France ou dans l'union Européenne et à effectuer toutes les démarches administratives et techniques visant à garantir la conformité des traitements avec la législation en vigueur.

Le sous-traitant pourra ajouter d'autres sites situés sur le territoire français ou européen, sans nécessité l'accord du responsable de traitement, à condition que ce changement n'affecte pas la prestation.
Les données restent localisées sur des serveurs basés dans l'union Européenne.
Les nouveaux sites seront exclusivement situés en France ou dans l'union Européenne

II. OBLIGATIONS DU RESPONSABLE DE TRAITEMENT VIS-A-VIS DU SOUS-TRAITANT

Le responsable de traitement s'engage à respecter le RGPD et toute norme législative ou réglementaire applicable aux données à caractère personnel traitées, et notamment à :

- Respecter le principe de limitation des données à caractère personnel nécessaires au regard des finalités de traitement. Par conséquent, le responsable de traitement s'engage à

anonymiser ou pseudonymiser autant que possible ses données à caractère personnel, et en tout état de cause à ne confier au sous-traitant que les données à caractère personnel strictement nécessaires à l'exécution des prestations,

- S'assurer que les traitements et leurs finalités sont conformes au RGPD,

- Fournir au sous-traitant la description du traitement et les instructions associées,

- Veiller, au préalable et pendant toute la durée du traitement, au respect par le sous-traitant des obligations prévues par le RGPD, dont notamment les dispositions de l'article 25 dudit règlement,

- Superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant, selon les conditions et modalités visées ci-dessus (article 1.7 « Documentation / audit »).

Fourniture de données au sous-traitant

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

III. 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 la ou les prestations suivante(s) objet de l'avenant.

Le responsable de traitement déclare que :

- La nature des opérations réalisées sur les données est

    - L'accès et/ou le transfert à la base de données du logiciel, dans le cadre :
        - D'une reprise de données
        - D'une migration de version de base
        - De la récupération d'une base corrompue afin de la remettre en état
    - Les activités de support dont la reproduction d'incidents et de bugs, via central téléphonique/site internet avec espace clients dédié et un outil interne de suivi clients
    - La maintenance de la solution
    - La télémaintenance de la solution et la prise de main à distance
    - La formation des utilisateurs, l'assistance technique et fonctionnelle
    - Si mode Saas :
        - Hébergement des données
        - Sauvegardes

- La ou les finalité(s) du traitement sont

  La ou les finalité(s) du traitement sont la réalisation d'une prestation de maintenance à l'initiative du responsable de traitement et une prestation d'hébergement de la solution MGDIS Essentiel Aides aux associations.

- Les données à caractère personnel traitées sont

- Le type de données à caractère personnel :

<u>Pour les agents de la Collectivité</u> :
Identité, données d'identification

Pour les représentants des Organismes :
Identité, données d'identification
Autres (à préciser)

Pour les Organismes :
Informations d'ordre économique et financier (revenus, situation fiscale)
Données bancaires (IBAN)
Autres (à préciser) :

- Les catégories de personnes concernées :

Organismes déposant une demande d'aide ou de subvention à la Collectivité
Agents de la Collectivité

Le Responsable de traitement s'engage à donner au Sous-traitant des instructions et finalités de traitement de ses données à caractère personnel conformes au RGPD.