**ANNEXE 2 au Cahier des Clauses Particulières : Clauses RGPD**

# PROTECTION DE LA VIE PRIVEE ET DES DONNEES A CARACTERE PERSONNEL

Le Prestataire s'engage à respecter les dispositions du Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel (RGPD) ainsi que la législation nationale en matière de protection des données personnelles.

Le Prestataire, en tant que sous-traitant, s’engage à ne traiter les données personnelles que pour l'exécution des prestations définies dans le présent marché public et conformément aux instructions écrites et explicites du Responsable du Traitement, qui est l'acheteur public ou son représentant. Le Prestataire ne traitera pas les données à d'autres fins que celles spécifiées dans ce marché.

Il fournit un projet de contrat de sous-traitance qui détaille, à minima, les informations suivantes :

### Nature et finalité du traitement

Les données personnelles traitées dans le cadre du présent contrat sont de nature suivante :

|  |
| --- |
| [Décrire les types de données personnelles traitées : par exemple, nom, prénom, adresse, numéro de téléphone, etc.] |

### Les finalités du traitement sont les suivantes :

|  |
| --- |
| [Décrire la finalité du traitement, par exemple, gestion de la prestation, gestion des factures, suivi administratif, etc.] |

### Les conditions de mise à disposition des données :

|  |
| --- |
| [décrire] |

### Obligations du Prestataire

Le Prestataire s'engage à :

* Traiter les données personnelles uniquement sur instruction écrite et préalable du Responsable du Traitement, sauf si la loi impose un traitement différent ;
* Mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque, en conformité avec l’article 32 du RGPD ;
* Veiller à ce que les personnes autorisées à traiter des données personnelles aient pris connaissance de leurs obligations de confidentialité et aient reçu la formation nécessaire à cet effet ;
* Assister le Responsable du Traitement dans le respect de ses obligations, y compris en matière de sécurité des données, notification des violations de données, demandes d'exercice des droits des personnes concernées, et réalisation des analyses d'impact sur la protection des données (DPIA) ;
* Aider le Responsable du Traitement à garantir la confidentialité, l'intégrité et la disponibilité des données personnelles.

### Sous-traitance

Le Prestataire ne pourra pas faire appel à un autre sous-traitant sans l'accord préalable et écrit du Responsable du Traitement. En cas d'accord pour la sous-traitance, le Prestataire s’engage à imposer à tout sous-traitant les mêmes obligations en matière de protection des données personnelles que celles qui lui incombent en vertu du présent contrat.

#### Autorisation préalable du Responsable du Traitement

Le Prestataire ne pourra recourir à un sous-traitant ultérieur pour l'exécution de tout ou partie du présent contrat sans avoir obtenu l’autorisation préalable et écrite du Responsable du Traitement, conformément à l’article 28, paragraphe 2 du RGPD. Toute demande d'autorisation devra être accompagnée de la documentation nécessaire permettant au Responsable du Traitement d'évaluer la conformité du sous-traitant ultérieur au RGPD.

#### Évaluation de la conformité au RGPD

Le Prestataire s’engage à s’assurer que tout sous-traitant ultérieur sélectionné respecte les obligations du RGPD, notamment en matière de sécurité, de confidentialité et de traitement des données personnelles. À cette fin, le Prestataire devra procéder à une évaluation préalable de la conformité au RGPD de chaque sous-traitant ultérieur, en vérifiant que ce dernier :

* A mis en place des mesures techniques et organisationnelles appropriées pour garantir la sécurité des données personnelles ;
* Assure la confidentialité des données personnelles traitées ;
* Respecte les droits des personnes concernées, notamment les droits d'accès, de rectification, d'effacement, de limitation et de portabilité ;
* Fournit des garanties suffisantes en matière de protection des données personnelles.

#### Documentation et transparence [à fournir]

Avant d'engager un sous-traitant ultérieur, le Prestataire devra fournir au Responsable du Traitement toutes les informations pertinentes concernant les mesures prises par le sous-traitant ultérieur pour assurer la conformité au RGPD. Cette documentation comprendra notamment :

* Les contrats ou accords conclus avec les sous-traitants ultérieurs, précisant leurs obligations en matière de protection des données personnelles ;
* Une description des mesures techniques et organisationnelles mises en place par le sous-traitant ultérieur pour assurer la sécurité et la confidentialité des données personnelles ;
* Toute certification ou autre preuve de conformité au RGPD obtenue par le sous-traitant ultérieur.

#### Responsabilité du Prestataire

Le Prestataire demeure pleinement responsable du respect des obligations prévues par le RGPD, même en cas de recours à un sous-traitant ultérieur. En cas de non-conformité d'un sous-traitant ultérieur, le Prestataire devra en informer immédiatement le Responsable du Traitement et prendre toutes les mesures nécessaires pour remédier à cette situation, y compris, le cas échéant, la résiliation des relations avec le sous-traitant concerné.

### Durée du traitement et des données

Le traitement des données personnelles par le Prestataire commence à la date de signature du présent contrat et prendra fin lors de l'exécution complète des prestations.

À la fin du contrat, ou sur demande du Responsable du Traitement, le Prestataire s'engage à restituer ou supprimer toutes les données personnelles traitées, sauf si une législation applicable impose leur conservation.

|  |
| --- |
| [décrire les conditions d’apurement ou de remise à disposition des données] |

### Droits des personnes concernées

Le Prestataire s’engage à informer immédiatement le Responsable du Traitement de toute demande émanant d’une personne concernée exerçant ses droits en vertu des articles 15 à 22 du RGPD (droit d'accès, de rectification, d’effacement, de limitation du traitement, de portabilité des données, et d'opposition).

Le Prestataire assiste le Responsable du Traitement dans la gestion des demandes des personnes concernées, conformément aux obligations prévues par le RGPD.

### Notification de violation de données

En cas de violation de données personnelles, le Prestataire s'engage à notifier cette violation au Responsable du Traitement sans délai et, dans la mesure du possible, dans les 72 heures suivant la prise de connaissance de la violation. Cette notification devra contenir toutes les informations nécessaires à la gestion de l’incident par le Responsable du Traitement.

### Audits et contrôles

Le Responsable du Traitement pourra, sur demande, effectuer un audit ou un contrôle de la conformité du Prestataire aux obligations prévues dans le cadre du présent marché, y compris en matière de sécurité des données et de protection de la vie privée. Le Prestataire s'engage à coopérer pleinement et à fournir toute l'assistance nécessaire dans le cadre de ces audits.

### Transfert de données hors de l’Union Européenne

Le Prestataire s'engage à ne pas transférer les données personnelles vers un pays tiers en dehors de l'Union Européenne sans l'accord préalable du Responsable du Traitement et, le cas échéant, sans garantir que ce transfert soit effectué dans le respect des exigences du RGPD.

### Responsabilités

Le Prestataire est responsable de toute non-conformité aux dispositions du RGPD résultant de son propre manquement ou de ses actions ou omissions. Le Prestataire déclare qu’il est informé de ses obligations au titre du RGPD et qu’il dispose de toutes les ressources nécessaires pour y satisfaire.

En cas de violation des dispositions de la présente clause, le Prestataire sera tenu de réparer tout préjudice ou dommage causé au Responsable du Traitement, y compris les amendes, pénalités et autres frais imposés par les autorités compétentes.

**Grille d'analyse pour un marché public selon l'article 28 du RGPD**

Cette grille d'analyse permet de vérifier la conformité des prestataires dans un cadre de marché public avec les obligations imposées par l'article 28 du RGPD. Elle couvre les aspects contractuels, la sécurité, la confidentialité, la gestion des sous-traitants, la durée et la gestion des données, ainsi que la collaboration avec les autorités compétentes.

## 1. Conformité de l'offre du prestataire

- Le prestataire est-il un sous-traitant au sens du RGPD ? (Le sous-traitant est une entité qui traite des données personnelles pour le compte d'un responsable du traitement.)

- Le contrat spécifie-t-il que le prestataire agira uniquement sur instruction du responsable du traitement ? (Article 28, paragraphe 3 a)

## 2. Garanties fournies par le sous-traitant

- Le prestataire fournit-il des garanties suffisantes pour mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir la sécurité des données ? (Article 28, paragraphe 3 c)

- Le prestataire a-t-il mis en place des mesures pour assurer la confidentialité des données traitées ? (Article 28, paragraphe 3 b)

- Les personnes autorisées à traiter des données personnelles sont-elles tenues à des obligations de confidentialité (Article 28, paragraphe 3 b)

## 3. Sous-traitance ultérieure

- Le contrat prévoit-il la possibilité pour le sous-traitant de faire appel à d’autres sous-traitants ? (Article 28, paragraphe 2)

- Si le sous-traitant fait appel à un autre sous-traitant, est-ce qu’il obtient l’autorisation préalable et écrite du responsable du traitement ? (Article 28, paragraphe 2)

-Le prestataire indique-t-il les conditions dans lesquelles il peut recourir à un sous-traitant ultérieur ? (Article 28, paragraphe 2)

## 4. Droit de vérification et audit

- Le contrat prévoit-il la possibilité d'audits pour vérifier la conformité du prestataire avec le RGPD ? (Article 28, paragraphe 3 h)

- Le sous-traitant s'engage-t-il à fournir toute l’assistance nécessaire pour permettre au responsable du traitement de mener des audits ou des inspections ? (Article 28, paragraphe 3 h)

## 5. Assistance en matière de sécurité, de confidentialité et de notification

- Le prestataire s'engage-t-il à aider le responsable du traitement à garantir la sécurité des données personnelles, notamment en cas de violation de données ? (Article 28, paragraphe 3 f)

- Le prestataire assiste-t-il le responsable du traitement pour répondre aux demandes des personnes concernées (par exemple, demandes d'accès, de rectification, etc.) ? (Article 28, paragraphe 3 e)

- Le prestataire a-t-il prévu un mécanisme pour notifier une violation de données personnelles au responsable du traitement dans les plus brefs délais ? (Article 28, paragraphe 3 d)

- Les mesures de sécurité sont-elles détaillées ? (article 28, paragraphe 5 f)

- Les mesures de sécurité sont-elles adaptées au regard du traitement de données confié au sous-traitant ?

## 6. Durée du traitement et suppression des données

- Le contrat spécifie-t-il la durée du traitement des données ? (Article 28, paragraphe 3 e)

- Le prestataire s'engage-t-il à retourner ou à supprimer toutes les données personnelles à la fin du contrat, conformément aux instructions du responsable du traitement ? (Article 28, paragraphe 3 g)

## 7. Transfert de données en dehors de l'UE

- Le prestataire a-t-il informé le responsable du traitement de tout transfert de données en dehors de l'Union européenne, le cas échéant ? (Article 28, paragraphe 3 d)

- Le prestataire s'assure-t-il que les données transférées en dehors de l'UE sont protégées conformément aux exigences du RGPD ? (Article 44 et suivants du RGPD)

## 8. Collaboration avec les autorités de protection des données

- Le contrat prévoit-il que le prestataire coopère avec les autorités de protection des données en cas de demande ou d'audit ? (Article 28, paragraphe 3 h)

## 9. Responsabilités et assurances

- Le contrat mentionne-t-il les responsabilités du prestataire en cas de non-conformité ou de violation des obligations prévues par l'article 28 du RGPD ? (Article 28, paragraphe 3)

- Des assurances sont-elles fournies pour couvrir les risques associés au traitement des données personnelles ? (Article 28, paragraphe 3)

## 