

## Annexe 1 : Protection des données personnelles

### 1. Description des traitements et engagements du sous-traitant

Le Titulaire est autorisé à traiter des Données Personnelles pour le compte du Maître d'ouvrage dans le cadre des traitements décrits en annexe 2.

#### Rôle du titulaire et de ses éventuels sous-traitants

Le Titulaire et ses sous-traitants agissent en qualité de sous-traitant du Maître d'ouvrage, responsable de traitement.

**Politique de protection des données.** Le Titulaire s'engage à communiquer au Maître d'ouvrage au plus tard au jour de la signature du Marché la politique de protection des données appliquée au sein de sa société.

Cette politique décrira notamment les mesures techniques et organisationnelles mise en œuvre par le Titulaire pour assurer la sécurité et la confidentialité des données dans le cadre de l'exécution du Marché.

Parallèlement, le Titulaire s'engage à mettre en œuvre des programmes de formation et de sensibilisation relatifs à la protection de la vie privée et des Données Personnelles à destination de ses salariés et sous-traitants ayant accès en permanence ou régulièrement aux Données Personnelles.

Le Titulaire s'engage à communiquer sans délai au Maître d'ouvrage toute modification et/ou évolution de sa politique de protection des données.

**Traitement des Données Personnelles selon les instructions du Maître d'ouvrage.** Le Titulaire s'engage à procéder au traitement des Données Personnelles conformément aux Instructions qu'il reçoit du Maître d'ouvrage.

En particulier, le Titulaire s'engage à :

- ne pas traiter et consulter les Données Personnelles collectées ou transmises à d'autres fins que l'exécution des prestations et pour les seuls besoins liés à l'exécution du Marché ;
- ne pas prendre de copie ou de stocker, quelles qu'en soit la forme et la finalité, tout ou partie des Données Personnelles qui lui ont été transmises ou qu'il a collectées au cours de l'exécution du marché en dehors de l'exécution du présent marché.
- prendre toutes les mesures utiles appropriées pour démontrer le respect des dispositions légales et réglementaires en matière de protection des Données Personnelles ;
- prendre toutes mesures permettant d'empêcher toute utilisation détournée, malveillante ou frauduleuse des Données Personnelles ;
- s'engager à prendre en compte, s'agissant des outils, produits, applications ou services, les principes de protection des données dès la conception et de protection par défaut ;
- ne pas insérer de données étrangères à l'exécution du Marché dans les Données Personnelles ;
- ne pas effectuer d'études statistiques sur les Données Personnelles ou de traitement autre que celui demandé par le Maître d'ouvrage ;

## Annexe 1 : Protection des données personnelles

- ne pas utiliser tout ou partie des Données Personnelles, dites de production, pour réaliser les phases de développements, de tests, de simulations ou de recette ;
- notifier immédiatement toute modification ou changement pouvant impacter le traitement des Données Personnelles ;
- à respecter les droits d'accès, de rectification, d'opposition et de suppression, le droit à la limitation du traitement et le droit à la portabilité dont bénéficient les personnes concernées. Ainsi, si les personnes concernées devaient contacter directement le Titulaire pour exercer leurs droits, ce dernier communiquera leurs demandes au Maître d'ouvrage dans un délai maximum de trois jours ouvrés et il coopèrera avec le Maître d'ouvrage. Le Titulaire ne fera droit à ces demandes que sur instruction écrite et préalable du Maître d'ouvrage à cette fin.

### 2. Sécurité

Le Titulaire s'engage à assurer la sécurité et la confidentialité des Données Personnelles qui lui sont communiquées.

Le Titulaire s'engage à ce que les mesures de sécurité organisationnelles mises en place répondent notamment aux exigences suivantes :

- la mise en place d'un engagement de confidentialité visant à ce que les personnes autorisées à traiter les Données Personnelles soient soumises à une obligation de confidentialité renforcée;
- l'élaboration de mesures restrictives d'accès aux Données Personnelles permettant de s'assurer que les personnes habilitées à utiliser le système de traitement de Données Personnelles ne puissent accéder qu'aux Données Personnelles auxquelles elles sont habilitées à accéder pour l'exécution de leur mission conformément à leurs droits d'accès et que, dans le cadre du traitement et de l'utilisation après stockage, les Données Personnelles ne puissent être lues, copiées, modifiées ou supprimées sans autorisation ;
- la mise en place de mesures pour empêcher le transfert des Données Personnelles à toute personne/entité non autorisée ;
- la mise en place d'une journalisation des connexions permettant de tracer les accès aux Données Personnelles.

Par ailleurs, le Titulaire s'engage à ce que les mesures de sécurité techniques mises en place répondent à minima aux exigences suivantes :

- une méthode de gestion des risques et une politique associée de management des risques de la confidentialité et de la sécurité (incluant notamment des analyses d'impact et des risques) ;
- la mise en place d'outils permettant de s'assurer que les Données Personnelles ne peuvent être lues, copiées, modifiées ou supprimées sans autorisation au cours de leur transfert électronique, de leur transport ou de leur stockage, et que les entités destinataires de tout transfert de Données Personnelles via les installations servant au transfert de données peuvent être identifiées et vérifiées ;
- l'établissement d'une piste d'audit afin de renseigner si quelqu'un, le cas échéant, a accédé, modifié ou supprimé des Données Personnelles du traitement. Les journaux de sécurité essentiels seront conservés pendant une durée de 12 mois ;

## Annexe 1 : Protection des données personnelles

- la mise en place de contrôles permettant de s'assurer que les Données Personnelles sont protégées contre les destructions ou les pertes accidentelles ;
- la mise en place de mesures permettant de veiller à ce que les Données Personnelles fournies par le maître d'ouvrage puissent être traitées distinctement des données personnelles des autres clients en utilisant des séparations logiques ;
- des mesures sécurisées d'authentification pour l'accès aux outils notamment au moyen de mots de passe respectant les recommandations de la Cnil ;
- des mesures de sécurisation physique des locaux, du réseau interne, des matériels, des serveurs et des applications (alarmes, badges, vidéosurveillance, etc).

En tout état de cause, le Titulaire s'engage, en cas de changement des moyens visant à assurer la sécurité, l'intégrité et la confidentialité des Données Personnelles, à les remplacer par des moyens d'une performance supérieure.

### 3. Notification d'une violation de Données Personnelles

Une violation de données s'entend comme une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée à des tiers de Données Personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Le Titulaire s'engage à notifier sans délai au Maître d'ouvrage, et en particulier à la personne désignée comme point de contact, par téléphone et par email (06.78.09.51.24) et par email (DPO@foyer-remois.fr), puis confirmer par lettre recommandée avec accusé de réception, toute violation de données.

Cette notification doit préciser :

- la nature et les conséquences de la violation de données,
- les catégories et le nombre approximatif de données
- les mesures déjà prises ou celles qui sont proposées pour y remédier ;
- les personnes auprès desquelles des informations supplémentaires peuvent être obtenues ; une estimation du nombre de personnes susceptibles d'être impactées par l'Incident.

Dès qu'il est informé d'une violation de données, le Titulaire procède à toutes les investigations utiles sur les manquements aux règles de protection afin d'y remédier promptement, au mieux de ses possibilités et de faire en sorte d'en diminuer l'impact pour les personnes concernées.

Le Titulaire s'engage à informer le Maître d'ouvrage de ses investigations, à les lui communiquer et à répondre favorablement à toute demande de collaboration émanant de ce dernier.

### 4. Sous-traitance

Le Titulaire ne peut sous-traiter, au sens de la Règlementation Informatique et libertés, tout ou partie des prestations, qu'après avoir obtenu l'accord préalable, écrit et exprès du Maître d'ouvrage.

Dans le cas où le Maître d'ouvrage aurait autorisé par écrit, expressément et préalablement, le Titulaire à sous-traiter les prestations confiées, le Titulaire s'oblige à conclure un contrat qui se réfère à la totalité des obligations et des garanties stipulées aux présentes, et à tenir à la disposition du Maître d'ouvrage une liste qu'il tient à jour du ou des sous-traitants impliqués dans le traitement de Données Personnelles et la communique à première demande de ce dernier.

## **Annexe 1 : Protection des données personnelles**

Il est rappelé au Titulaire que celui-ci est et demeure pleinement responsable devant le Maître d'ouvrage de l'exécution par les sous-traitants de leurs obligations en matière de protection des Données Personnelles.

### **5. Flux transfrontières de Données Personnelles**

Le Titulaire privilégie l'hébergement et le traitement des Données Personnelles au sein des datacenters situés sur le territoire de l'Union Européenne pendant toute la durée du Marché.

Ainsi, le Titulaire évitera tout flux transfrontalier de Données Personnelles, quel qu'il soit, en dehors du territoire de l'Union Européenne, sauf consentement préalable et écrit du Maître d'ouvrage.

Dans le cas où le Titulaire serait autorisé par écrit, expressément et préalablement au transfert, par le Maître d'ouvrage, à transférer ces Données Personnelles hors du territoire de l'Union Européenne, notamment dans le cadre de la sous-traitance des prestations qui lui sont confiées par le Titulaire, et que ce transfert a lieu vers un pays « n'offrant pas un niveau suffisant de protection des Données Personnelles » par la Commission Européenne, le Titulaire aura l'obligation – préalablement à tout transfert – de formaliser une convention de transfert de Données Personnelles hors de l'Union Européenne signée entre le Titulaire, agissant en qualité de mandataire du Maître d'ouvrage et d'« exportateur de Données Personnelles » et son sous-traitant qualifié d'« importateur de Données Personnelles » et de faire respecter scrupuleusement les termes et obligations de cette convention par son sous-traitant, sur la base des Clauses Contractuelles Types de la Commission européenne, ou le cas échéant, de celles adoptées par une autorité de contrôle conformément au mécanisme de contrôle de la cohérence, puis par la Commission.

### **6. Tenue du Registre**

Le Titulaire en tant que sous-traitant, donnera au Maître d'ouvrage accès au registre des traitement sur demande.

### **7. Conservation des données**

Au terme du Marché, le Titulaire s'engage à restituer les fichiers et données au Maître d'ouvrage dans les conditions spécifiées par celui-ci puis à détruire tous fichiers manuels ou informatisés stockant les informations collectées, sauf disposition impérative contraire résultant du droit communautaire ou du droit d'un Etat membre de l'Union européenne applicable aux traitements objets des présentes.

Le Titulaire s'engage à fournir à première demande et dans un délai raisonnable un certificat de suppression des Données Personnelles au Maître d'ouvrage.

### **8. Audit**

Le Titulaire s'engage à répondre aux demandes d'audit du Maître d'ouvrage ou d'un tiers de confiance sélectionné, reconnu en tant qu'auditeur indépendant, c'est-à-dire indépendant ayant une qualification adéquate, et libre de fournir les détails de ses remarques et conclusion d'audit au Maître d'ouvrage. Les audits doivent permettre une analyse du respect par le Titulaire de ses obligations au titre du Marché, ainsi qu'au titre de la Réglementation Informatique et libertés.

Les audits sont aux frais du Maître d'ouvrage, en revanche, les mesures de mise en conformité préconisées dans le cadre desdits audits sont placées intégralement à la charge du Titulaire défaillant, sans préjudice de l'application éventuelle des pénalités stipulées à la clause intitulée « Pénalités » des présentes, ainsi que des sanctions prévues.

## Annexe 1 : Protection des données personnelles

### 9. Coopération

Le Titulaire s'engage à coopérer avec le Maître d'ouvrage afin de permettre le respect des obligations pesant sur le Maître d'ouvrage au regard de la Réglementation Informatique et libertés, telles que notamment ses obligations de notification à l'autorité de contrôle et de communication d'une violation de données aux personnes concernées.

En cas de contrôle d'une autorité compétente, les Parties s'engagent à coopérer entre elles et avec l'autorité de contrôle.

Dans le cas où le contrôle mené ne concernerait que les traitements mis en œuvre par le Titulaire en tant que responsable du traitement, le Titulaire fera son affaire du contrôle et s'interdira de communiquer ou de faire état des Données Personnelles du Maître d'ouvrage.

Dans le cas où le contrôle mené chez le Titulaire concernerait les traitements mis en œuvre au nom et pour le compte du Maître d'ouvrage, le Titulaire s'engage à en informer immédiatement le Maître d'ouvrage et à ne prendre aucun engagement pour ce dernier.

En cas de contrôle d'une autorité compétente chez le Maître d'ouvrage portant notamment sur les prestations délivrées par le Titulaire, ce dernier s'engage à coopérer avec le Maître d'ouvrage et à lui fournir toute information dont ce dernier pourrait avoir besoin ou qui s'avèrerait nécessaire.