*Ce document est l’un des modèles de la Bibliothèque de Protection des Données référencés dans la Boite à Outils pour la Protection des Données****. Il ne doit JAMAIS être modifié directement dans son emplacement Teams/SharePoint initial - la Bibliothèque****. Avant toute utilisation de ce modèle, veillez à le télécharger puis l’enregistrer sur votre espace de travail.*

*Le modèle et en particulier les termes entre <…> doivent être adaptés aux spécificités de votre service et des traitements qu’il réalise.*

1. **ARTICLE A INSERER DANS LE MARCHE / LA CONVENTION**

### ARTICLE XX- PROTECTION DES DONNEES A CARACTERE PERSONNEL

Dans le cadre <du marché/ de la convention>, le titulaire traite, au nom et pour le compte de l’acheteur public, les données à caractère personnel nécessaires à l’exécution de ses prestations.

L’acheteur public est le responsable de traitement, le titulaire est un sous-traitant de données à caractère personnel au sens du règlement UE n° 2016-679 du 27 avril 2016 dit Règlement général sur la protection des données RGPD.

Le titulaire déclare être parfaitement informé des obligations légales et réglementaires relatives à la protection des données à caractère personnel qui s’imposent tant au responsable de traitement qu’au sous-traitant, en vertu du RGPD, de la loi n°78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés et du décret n°2019-536 du 29 mai 2019. Il s’engage au respect de ces obligations.

Les modalités du traitement des données dans le cadre <du marché/ de la convention> sont fixées dans l’annexe 1.

1. **ANNEXE A JOINDRE AU MARCHE/ A LA CONVENTION**

**ANNEXE 1** <les références du marché/ de la convention>

**PROTECTION DES DONNEES A CARACTERE PERSONNEL**

**PREAMBULE :**

Dans le cadre de <les références du marché/de la convention>, <le nom de votre service> a recours à <le nom de la société> afin de réaliser <l’objet de la prestation>

Dans ce cadre, des données à caractère personnel seront traitées.

La présente annexe a pour objet de décrire les obligations respectives des parties en matière de protection des données à caractère personnel.

Dans le cadre de leurs relations contractuelles, les parties s’engagent à respecter la réglementation applicable au traitement de données à caractère personnel et, en particulier, la Loi informatique et libertés n°78-17 du 6 janvier 1978 modifiée ainsi que le Règlement UE 2016/679 du 27 avril 2016 dit Règlement européen sur la protection des données ou RGPD.

L’ensemble des notions utilisées dans la présente annexe (traitement, responsable de traitement, sous-traitant, personne concernée, donnée à caractère personnel, violation de données…), répondent aux définitions posées par la législation informatique et libertés (le règlement UE n° 2016-679 du 27 avril 2016 dit Règlement général sur la protection des données personnelles RGPD, la Loi n° 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés et le Décret n°2019-536 du 29 mai 2019 pris pour l’application de la loi n° 78-17 du 6 janvier 1978).

1. **RESPONSABLE DE TRAITEMENT – SOUS-TRAITANT**

Le responsable de traitement est le gouvernement de la Polynésie française. Le traitement est réalisé pour le compte de <le nom de votre service>,

Ci-après le « responsable de traitement » ou **«**<le nom de votre service> **»**

<le nom de la société> est le prestataire de services qui s’est vu confier les prestations de <l’objet de la prestation>

Dans le cadre de ces prestations, il est un sous-traitant de données à caractère personnel au sens du RGPD.

Ci-après le « sous-traitant » ou « <le nom de la société> »

1. **TRAITEMENTS CONCERNES**

Les traitements objet de la présente convention sont listés dans le tableau suivant :

|  |  |  |  |
| --- | --- | --- | --- |
| Désignation et finalités du traitement | Opérations pouvant être confiées au prestataire sur les données | Personnes concernées | Données traitées |
| Préciser clairement les finalités pour lesquelles le sous-traitant intervient  *Par exemple, maintenance d’une application, fiabilisation d’une base de données, extractions de données, numérisation de documents, hébergement de données…..* | Préciser quel type d’opérations le prestataire réalise sur les données.  *NB : Différentes formes de traitement existent : collecte, enregistrement organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement* | Préciser les catégories de personnes dont les données sont traitées à l’occasion de la prestation  *Préciser par exemple la catégorie d’usagers concernée (patients, élèves, agents publics, …)* | Lister les données ou types de données qui seront traités  *(identité, numéro CPS, coordonnées, données de santé…..)* |

1. **OBLIGATIONS GENERALES DU SOUS-TRAITANT**

Le sous-traitant s’engage à traiter les données uniquement pour les finalités objet de la prestation passée avec le responsable de traitement, telles que précisées à l’article 2 ci-dessus et pour le compte exclusif du responsable de traitement.

Il les traite conformément aux présentes clauses et aux instructions documentées reçues du responsable de traitement.

Il veille à ce que ses personnels autorisés à traiter les données à caractère personnel pour l’exécution de la prestation s’engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité et aient reçu la formation nécessaire en matière de protection des données à caractère personnel.

Dans l’exécution de la convention, le sous-traitant prend en compte les principes de protection des données dès la conception et de protection des données par défaut.

1. **OBLIGATIONS DU RESPONSABLE DE TRAITEMENT**

Conformément aux dispositions de l’article 5.2 RGPD, <le nom de votre service> en sa qualité de responsable du traitement est tenu au respect des principes énoncés à l’article 5.1 du RGPD et est en mesure de démontrer que celui-ci est respecté (responsabilité).

A ce titre, le responsable de traitement s’engage à :

* fournir au sous-traitant toutes les données dont ce dernier a besoin pour assurer les prestations prévues au contrat ;
* documenter par écrit toute instruction concernant le traitement des données par le sous-traitant ;
* garantir la licéité des données transmises au sous-traitant et informer immédiatement le sous-traitant de toute erreur ou irrégularité concernant les données, dont il aurait connaissance ;
* veiller au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le RGPD de la part du sous-traitant.

1. **CONFIDENTIALITE DES DONNEES**

Les données à caractère personnel objet du traitement sont strictement confidentielles.

<*Si la prestation implique un traitement de données de santé* : Le sous-traitant reconnait être parfaitement informé de la nature sensible des données de santé traitées dans le cadre de ses prestations, susceptible d’engendrer un risque élevé pour les droits et libertés des personnes. >

Le sous-traitant s’engage donc à respecter, de façon absolue, les obligations suivantes et à les faire respecter par son personnel :

* considérer comme confidentielles les données à caractère personnel, qu’il est amené à connaître durant l’exécution de ses prestations. Cette obligation de confidentialité se poursuit après l’expiration de la présente convention ;
* ne prendre aucune copie des données, à l’exception de celles nécessaires à l’exécution de ses prestations ;
* ne pas utiliser les données traités à des fins autres que celles spécifiées par la présente convention ;
* ne pas divulguer ces données à des tiers, quels qu’ils soient ;
* prendre toutes les mesures permettant d’éviter toute utilisation détournée ou frauduleuse des données ;
* prendre toutes les mesures, notamment de sécurité matérielle, pour assurer la conservation et la transmission sécurisées des données ;
* et plus généralement, mettre en œuvre tous les moyens nécessaires, eu égard aux risques liés au traitement et à la nature des données, permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement.

1. **DISPONIBILITE ET INTEGRITE DES DONNEES**

Le sous-traitant s’engage à assurer la parfaite disponibilité et l’intégrité des données qui lui sont confiées. Il met en œuvre toutes les mesures techniques et organisationnelles appropriées pour protéger les données contre toute destruction, perte, altération.

1. **REGISTRE DES TRAITEMENTS – DOCUMENTATION - AUDITS**

Le sous-traitant déclare tenir par écrit un registre de tous les traitements effectués pour le compte du responsable de traitement, comprenant une description de ces traitements ainsi qu’une description des mesures techniques et organisationnelles de sécurité appliquées à ces traitements. Il le tient à la disposition du responsable de traitement et s’engage à répondre, sans délai, à toute demande de communication de ce registre.

Le sous-traitant tient également à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de la loi n°78-17 du 6 janvier 1978 et du RGPD, sans préjudice pour le responsable de traitement du droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées, notamment dans le cadre d’audits dont les modalités seront fixées d’accord parties, dans le respect de la confidentialité attachée aux activités du sous-traitant.

1. **DELEGUES A LA PROTECTION DES DONNEES**

La déléguée à la protection des données du responsable de traitement est Tania BERTHOU [dpo@administration.gov.pf](mailto:dpo@administration.gov.pf) - 689. 40. 544 397. Le référent informatique et libertés de <le nom de votre service> est <le nom et les coordonnées du RIL de votre service>

Le délégué à la protection des données du sous-traitant est <le nom et les coordonnées du DPO de la société >

Ou/ Le sous-traitant n’a pas nommé un délégué à la protection des données <le sous -traitant doit préciser les motifs pour lesquels il considère ne pas être soumis à cette exigence>.

1. **INFORMATION ET DROITS DES PERSONNES CONCERNEES**
2. Information à l’initiative du responsable de traitement

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. Exercice des droits

Si le sous-traitant est saisi d’une demande d’exercice de ses droits par une personne concernée (notamment relative au droit d’accès, de rectification, d’opposition, à la limitation, à l’effacement, à la portabilité), il doit l’adresser dès réception, par courrier électronique, <les coordonnées du RIL ou à défaut du secrétariat de votre service> et à la déléguée à la protection des données [dpo@administration.gov.pf](mailto:dpo@administration.gov.pf).

De manière générale, lorsqu’une personne exerce ses droits, le sous-traitant doit, dans toute la mesure du possible et avec diligence, aider le responsable de traitement à donner suite à cette demande notamment en procédant aux opérations qui lui seraient demandées par <le nom de votre service>(par exemple l’extraction, la suppression, la rectification de données…..).

1. **SORT DES DONNEES**

Au terme <du marché/de la convention>, le sous-traitant saisit le responsable de traitement pour connaître ses instructions sur le sort des données. Selon les instructions reçues, le sous-traitant procède :

* soit à la destruction de toutes les données à caractère personnel de ses systèmes d’information et dossiers ;
* soit au renvoi de toutes les données au responsable de traitement. Dans ce cas le sous-traitant procède, après renvoi, à la destruction de toutes les copies existantes dans ses systèmes d’information ou dossiers.

Dans les deux cas, le sous-traitant justifie par écrit de la destruction des données.

1. **HEBERGEMENT DES DONNEES**

<*Si la prestation comprend un hébergement de données de santé* : Le sous-traitant s’engage à procéder à l’hébergement des données de santé chez un hébergeur de données de santé dument certifié/agréé en application des dispositions de l’article L 1111-8 du Code de la santé publique et en justifie. >

1. **TRANSFERT HORS DE L’UNION EUROPEENNE**

Dans le cadre de la convention, il n’est pas prévu de transfert de données hors de l’Union européenne ou de l’Espace économique européen.

Le sous-traitant doit informer le responsable de traitement de tout transfert envisagé vers un pays tiers. Ce transfert est soumis à l’accord préalable, spécifique et écrit du responsable de traitement. Le sous-traitant doit justifier que ce transfert présente l’une des garanties appropriées exigées par le RGPD et fournir les documents attestant de l’existence de ces garanties. Il communique la documentation utile préalablement à tout transfert.

**OU**  <Dans le cadre de la convention, il est prévu un transfert de données hors de l’UE : Préciser quel type de transfert est prévu et quel pays tiers est concerné.

Le transfert présente les garanties suivantes : (Préciser les garanties sur lesquelles le transfert s’appuie et produire les justificatifs (cf. chapitre V du RGPD). >

1. **SOUS TRAITANCE ULTERIEURE**

Dans le cadre de la présente convention, il n’est pas autorisé de sous-traitance ultérieure.

En cas de recours à une sous-traitance ultérieure, le sous-traitant doit obtenir l’accord préalable, spécifique et écrit du responsable de traitement qui n’est pas tenu d’accepter cette sous-traitance ultérieure.

Dans tous les cas où une sous-traitance ultérieure est acceptée, le sous-traitant doit avoir imposé à son sous-traitant les mêmes obligations en matière de protection de données que celles qui lui incombent en vertu du marché/de la convention. 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 l’autre sous-traitant de ses obligations.

**OU** Les parties conviennent que le(s) sous-traitant(s) ultérieur(s) autorisé(s), à la date de signature de la présente convention, est/sont listé(s) dans le tableau ci- dessous.

|  |  |
| --- | --- |
| Nom et coordonnées du sous-traitant ultérieur | Nature de la prestation confiée |
|  |  |
|  |  |

1. **VIOLATIONS DE DONNEES**

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 24 heures après en avoir pris connaissance, par courriel à <le nom de votre service>, <les coordonnées du RIL ou à défaut du secrétariat de votre service> et à la déléguée à la protection des données ([dpo@administration.gov.pf](mailto:dpo@administration.gov.pf)).

Cette notification est accompagnée de toute documentation utile afin de permettre au responsable du traitement de notifier, si nécessaire, cette violation à la commission nationale informatique et libertés (CNIL) et aux personnes concernées.

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 délégué́ 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 qu’il est proposé 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.

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 sous-traitant fera les meilleurs efforts pour identifier la cause de toute violation de données à caractère personnel et prendre toutes les mesures raisonnables et nécessaires afin d’y apporter les mesures de remédiation appropriées.

1. **ANALYSES D’IMPACT POUR LA PROTECTION DES DONNEES**

Compte tenu de la nature des traitements et données à caractère personnel objet des prestations, le sous-traitant peut être appelé par le responsable de traitement à apporter son concours dans la documentation d’une analyse d’impact sur la vie privée dont les traitements feraient l’objet. Il apportera les moyens, informations et documents utiles et nécessaires pour l’aider dans la réalisation de cette analyse.

1. **MESURES DE SECURITE** <le paragraphe sur les mesures de sécurité doit être complété et adapté selon la prestation>

Le sous-traitant met en œuvre les mesures techniques et organisationnelles appropriées afin d’assurer la sécurité des données, et notamment la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement.

Ces mesures doivent permettre de :

* prévenir tout accès et usage non autorisé aux systèmes d’information hébergeant les traitements de données à caractère personnel (contrôle d’accès) ;
* garantir que les personnes autorisées à opérer les systèmes d’information hébergeant les traitements de données à caractère personnel n’ont accès aux données personnelles qu’en respect du besoin d’en connaître et que les données à caractère personnel concernées ne peuvent être lues, copiées, altérées ou supprimées sans autorisation dans le cadre de leur traitement, usage ou après stockage (contrôle d’accès) ;
* garantir que les données à caractère personnel ne peuvent être lues, copiées, altérées ou supprimées sans autorisation pendant leur transport, numérique ou non, et qu’il est possible de vérifier et de tracer l’ensemble des intermédiaires concourant à la transmission des données à caractère personnel (contrôle de transmission) ;
* garantir qu’il est possible de vérifier et de tracer si et par qui des données à caractère personnel ont été intégrées, altérées ou supprimées des systèmes d’information hébergeant les traitements de données à caractère personnel (contrôle d’accès en entrée) ;
* garantir que le traitement des données à caractère personnel est strictement réalisé conformément aux instructions du donneur d’ordre (contrôle d’origine) ;
* garantir que les données à caractère personnel sont protégées contre toute destruction accidentelle ou malveillante des moyens (contrôle de disponibilité) ;
* garantir le rétablissement de la disponibilité des données et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique (contrôle de disponibilité).

Le sous-traitant met en œuvre toute procédure utile permettant de tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

1. **RESPONSABILITES**

La méconnaissance des présentes clauses est susceptible d’engager la responsabilité du sous-traitant. Le responsable de traitement pourra prononcer la résiliation immédiate de marché/ de la convention, sans indemnité en faveur du sous-traitant, en cas de non-respect des dispositions précitées.