# ANNEXE SÉCURITÉ ET PROTECTION DES DONNÉES

**Objet de la convention : ……**

**Adresse(s) mail de contact pour les notifications relatives à la protection des données (articles 5.3 à 5.5) :**

- **……..@ampmetropole.fr**
- **……..@ampmetropole.fr**

RSSI / DPO

**Contenu**

## 1. Objet

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement en matière de sécurité des systèmes d'information et de protection des 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 »).

Le présent document décrit les dispositions que le sous-traitant doit mettre en œuvre pour répondre aux exigences de sécurité de la Métropole Aix-Marseille-Provence.

Il est complété par le document PAS – Plan d'assurance sécurité, que le sous-traitant a remis à l'appui de son offre, et qui précise l'organisation qui sera mise en place, la méthodologie à suivre pour gérer la sécurité du projet et les mesures techniques et organisationnelles qui seront mises en œuvre par le sous-traitant.

## 2. Organisation de la sécurité

La Métropole désigne un interlocuteur responsable de la sécurité du projet. Cet interlocuteur unique sera rattaché directement au directeur de projet. Cet interlocuteur sera responsable de l'ensemble de la sécurité du projet pour la Métropole, tant sur les aspects sécurité du système d'information cible que sur les aspects sécurité des interfaces avec le sous-traitant.

Le responsable de la sécurité désigné par la Métropole a pour mission de faciliter les relations entre les différents intervenants, et de mettre à disposition de la maîtrise d'œuvre l'ensemble des documents nécessaires au bon déroulement du projet sécurité lié à l'opération d'externalisation : politique de sécurité interne de la Métropole, documentation technique du système (documents d'architecture, documents d'exploitation, etc.), spécifications, etc.

Il a également pour mission de s'assurer de la prise en compte globale de la sécurité, par la maîtrise d'ouvrage et la maîtrise d'œuvre.

Il décide de la conduite à tenir selon le résultat des audits, des incidents ou des conseils remontés par le sous-traitant d'externalisation.

Il valide l'ensemble des actions réalisées au titre de la gestion de la sécurité du projet.

En tant que maître d'œuvre, le sous-traitant désigne un interlocuteur responsable de la sécurité, pilotant l'ensemble de la sécurité du projet : sécurité des développements, sécurité du système d'information cible et intégration des composants sécurité.

Il conseille le client dans son approche de la sécurité du projet, selon les audits, les incidents perçus sur le système ou les évolutions du contexte opérationnel.

## 3. Cycle de vie des mesures de sécurité

Le sous-traitant est responsable de la rédaction du PAS, de son mémoire technique, ainsi que de l'organisation de sa sécurité pour répondre aux exigences de la Métropole pendant toute la durée du contrat.

Voici une liste (non exhaustive) des situations susceptibles d'entraîner une modification de l'organisation de la sécurité du sous-traitant :

- évolution du système d'information (configuration logicielle ou matérielle) ;
- évolution de l'environnement du système d'information (locaux, personnels, procédures, etc.) ;
- évolution législative ou réglementaire ;
- évolution du périmètre de l'opération.

En cas d'évolution, le sous-traitant vérifie si l'organisation de sa sécurité doit être modifiée. Si tel est le cas, il propose une modification à la Métropole. Le cas échéant, cette modification est approuvée par avenant.

Il s'agit d'une clause de réexamen, conformément aux dispositions de l'article R. 2194-1 du code de la commande publique.

## 4. Auditabilité

Le sous-traitant met à la disposition de la Métropole la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par la Métropole ou un autre auditeur qu'elle a mandaté, et contribuer à ces audits.

Cet audit est réalisé sur l'ensemble du périmètre du contrat et sur les services du sous-traitant en lien avec ce contrat. Il peut prendre la forme d'audits documentaires, d'interviews et/ou de tests d'intrusion.

Le sous-traitant doit se rendre disponible lors de ces audits et donner aux auditeurs l'accès à l'ensemble des éléments nécessaires.

Le rapport d'audit sera transmis au sous-traitant par la Métropole.

Le sous-traitant devra fournir dans le mois suivant la transmission du rapport d'audit un plan d'actions détaillé pour couvrir les non-conformités identifiées dans cet audit ou justifier de leur acceptation.

## 5. Obligations du sous-traitant

### 5.1. Obligations générales

Le sous-traitant est tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. En particulier il s'engage à informer le client des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention.

Outre le respect de ses obligations au titre de la convention de service, le sous-traitant informera préalablement le client de toute opération susceptible de provoquer l'indisponibilité (ou une dégradation des performances) du système.

Le sous-traitant est responsable du maintien en condition de sécurité du système pendant toute la durée des prestations.

Les mécanismes de sécurité mis en œuvre doivent évoluer conformément à l'état de l'art : la découverte de failles dans un algorithme, un protocole, une implémentation logicielle ou matérielle, ou encore l'évolution des techniques de cryptanalyse et des capacités d'attaque par force brute doivent être pris en compte.

Le sous-traitant s'engage à :

- traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la convention ;

- traiter les données conformément aux instructions de la Métropole ;

  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 Etats membres relative à la protection des données, il en informe immédiatement la Métropole.

  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'Etat membre auquel il est soumis, il doit informer la Métropole de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;

- garantir la confidentialité des données à caractère personnel traitées dans le cadre de la présente convention ;

- veiller à ce que les personnes autorisées à traiter les données à caractère personnel le fasse conformément à la règlementation:

  - 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.

### 5.2. Sous-traitance

Le sous-traitant du sous-traitant est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions de la Métropole. Il appartient au sous-traitant 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 sous-traitant demeure pleinement responsable devant la Métropole de l'exécution par le sous-traitant de ses obligations.

Le sous-traitant veille à la bonne prise en compte des principes et exigences de sécurité de la Métropole pour ses sous-traitants et notamment :

- Du respect des réglementation nationales et internationales :
    - Le RGPD
    - Le RGS
- De la mise en œuvre chez le sous-traitant d'une démarche SSI cohérente avec les exigences de la PSSIE
- De la présence chez son sous-traitant d'un responsable de la sécurité
- De l'existence d'un processus de gestion des alertes et incidents de sécurité informatique
- De l'existence d'un processus de gestion de la continuité d'activité

Le sous-traitant a la charge de réaliser au moins un audit de ses sous-traitants pendant la durée de la convention et doit fournir à la Métropole, lorsqu'elle le demande, les résultats de ces audits ainsi que les plans d'actions de remédiation associés.

### 5.3. Droit d'information des personnes concernées

Dans le cas où le sous-traitant procède à la collecte des données pour le compte du responsable de traitement, le sous-traitant, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise. La formulation et le format de l'information doit être convenue avec le responsable de traitement avant la collecte de données.

Dans les autres cas, 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.

### 5.4. Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider la Métropole 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).

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à l'adresse mail (ou aux adresses mail) mentionnée(s) en page de garde du présent document, et copie à dpo@ampmetropole.fr.

### 5.5. Notification des violations de sécurité et/ou de données à caractère personnel

Le sous-traitant notifie à la Métropole toute violation de sécurité et/ou de données à caractère personnel dans un délai maximum de 48 heures calendaires après en avoir pris connaissance et par courrier électronique à l'adresse mail (ou aux adresses mail) mentionnée(s) en page de garde du présent document, avec copie à dpo@ampmetropole.fr et rssi@ampmetropole.fr. Cette notification est accompagnée de toute documentation utile afin de permettre à la Métropole, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Après accord de la Métropole, le sous-traitant notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte de la Métropole, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures calendaires 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 La Métropole 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 de la Métropole, le sous-traitant communique, au nom et pour le compte de la Métropole, 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 :

- 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 la Métropole 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.

### 5.6. Aide du sous-traitant dans le cadre du respect par la Métropole de ses obligations

Le sous-traitant aide la Métropole pour la réalisation éventuelle d'analyses d'impact relative à la protection des données.

Le sous-traitant aide la Métropole pour la réalisation de la consultation préalable de l'autorité de contrôle.

### 5.7. Mesures de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, y compris, entre autres :

- 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.

### 5.8. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à renvoyer toutes les données à caractère personnel à la Métropole ou à renvoyer les données à caractère personnel au sous-traitant désigné par la Métropole.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

Le sous-traitant apporte l'assistance nécessaire durant la période de migration pour faciliter le transfert des données, et la reprise de leur exploitation par la Métropole, ou par un autre prestataire de service.

### 5.9. Délégué à la protection des données

Le sous-traitant communique à la Métropole 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.

### 5.10. Registre des catégories d'activités de traitement

Le sous-traitant déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte de la Métropole comprenant :

- le nom et les coordonnées de la Métropole pour le compte de laquelle 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 Métropole ;
- 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 ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
    - la pseudonymisation et le chiffrement des données à caractère personnel ;
    - des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
    - des 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.

## 6. Management de la SSI du sous-traitant

Le sous-traitant dispose d'un corpus documentaire SSI composé de :

- une PSSI : celle est revue à minima tous les 3 ans. Elle respecte les principes de la PSSIE.
- une analyse de risque : elle s'appuie sur une méthode d'analyse de risques en cohérences avec les principes de l'ISO27005, est revue régulièrement et définit des actions de suppression ou limitation des risques.
- une démarche d'audit : elle définit les principes de contrôle internes permettant au sous-traitant de vérifier le maintien en condition de sécurité de son système.

### 6.1. Sécurité des ressources humaines

Lors du processus de recrutement des contrôles de vérification de fond sur tous les candidats sont effectués par le sous-traitant en conformité avec les lois, les règlements pertinents et l'éthique. Ces contrôles doivent être proportionnées aux exigences métier, à la classification des informations accessibles et aux risques identifiés.

L'ensemble du processus d'arrivée et départ d'un collaborateur est piloté par les Ressources Humaines du sous-traitant.

Des plans de formation et des plans de sensibilisation aux mesures de sécurité sont mis en place à l'attention du personnel du sous-traitant et, quand cela est pertinent, des sous-traitants. De plus, le personnel et les sous-traitants reçoivent régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leurs fonctions.

### *6.2.* Sécurité des infrastructures

#### 6.2.1. Cartographie du service

Le sous-traitant dispose d'une cartographie des principaux composants entrant dans le cadre des prestations de cette convention.

Cette cartographie est tenue à jour.

#### 6.2.2. Accès logiques

Les systèmes d'exploitation, applications et équipements réseaux utilisés doivent exiger que chaque utilisateur soit authentifié avec succès avant d'autoriser toute autre action pour le compte de cet utilisateur. Les droits sont configurés afin que :

- chaque profil d'utilisateurs n'ait accès qu'aux fonctions nécessaires pour remplir sa mission
- chaque utilisateur n'ait accès qu'au profil qui lui est attribué

Aucun authentifiant ne doit être stocké en clair (sans chiffrement ou condensat) quelle que soit la méthode de stockage (fichier, base de données, scripts …).

Des droits doivent être positionnés afin qu'aucun authentifiant ne soit accessible en lecture, même sous forme chiffrée, aux utilisateurs.

Les procédures de création, modification et suppression de compte doivent être décrites dans un document.

L'ajout d'utilisateur ou les modifications entrainant l'attribution de privilèges supplémentaires, doivent être officiellement validés et tracées dans l'outil.

Tous les comptes (système et applicatif) doivent être configurés de manière sécurisée (complexité de mots de passe, blocage au bout 5 tentatives, changement de mot de passe régulier, etc.)

Toute utilisation ou modification d'un compte doit être tracée.

<u>Règles spécifiques pour les administrateurs :</u>

Les comptes à privilèges (comptes administrateurs) doivent être nominatifs et distincts des comptes utilisateurs standards.

Les comptes à très hauts privilèges (administrateurs de domaines par exemple) doivent être sécurisés (mots de passes très complexes), nominatifs et distincts des comptes administrateurs standards.

#### 6.2.3. Cloisonnement

Les infrastructures en charge du projet sont positionnées dans des zones réseau en cohérence avec leur criticité et leurs fonctions, et dans le respect des principes de cloisonnement.

Le sous-traitant dispose d'une matrice des flux à jour pour l'ensemble des équipements du projet.

#### 6.2.4. Sécurité des serveurs

Tous les serveurs respectent les bonnes pratiques de sécurisation (recommandations constructeurs, guides de l'ANSSI, etc.). Ces pratiques sont listées et maintenues dans un document.

Une solution contre les codes malveillants est déployée sur tous les serveurs du périmètre projet du sous-traitant.

#### 6.2.5. Sécurité des postes

L'installation des postes utilisés dans le cadre du projet respecte les bonnes pratiques de sécurisation. Ces pratiques sont listées et maintenues dans un document.

Une solution contre les codes malveillants est déployée sur chaque poste du périmètre projet du sous-traitant.

#### 6.2.6. Supervision de la sécurité

Le sous-traitant doit disposer de solutions de supervision de la sécurité (EDR, SIEM, puits de logs, etc.).