SERVICES GENERAUX

GRAND PORT MARITIME DE LA GUYANE

ZI de DEGRAD-DES-CANNES

97354 REMIRE-MONTJOLY

|  |
| --- |
| Cahier des Cahier des Clauses Techniques Particulières  (C.C.T.P) |

|  |
| --- |
| DPO RGPD du Grand Port Maritime de Guyane |

CCTP GPM-G\_RX 25 13 RGPD VFC

Table des matières

[Article II. LE CONTEXTE 3](#_Toc200015137)

[Section 2.01 Le Grand Port Maritime de la Guyane 3](#_Toc200015138)

[Section 2.02 Eléments liés au dossier 3](#_Toc200015139)

[(a) Contexte du marché 3](#_Toc200015140)

[(b) Tâches réalisées par le précédent prestataire : 4](#_Toc200015141)

[(c) Tâches en cours qui seront à terminer : 4](#_Toc200015142)

[(d) Tâches qui n’ont pas été réalisées : 4](#_Toc200015143)

[(e) Allotissement 4](#_Toc200015144)

[(f) Objet du marché 4](#_Toc200015145)

[Article III. LES EXIGENCES 5](#_Toc200015146)

[Section 3.01 Généralités 5](#_Toc200015147)

[Section 3.02 Prestations attendues : 5](#_Toc200015148)

[(a) UO 1 : Mise en conformité au RGPD de l’ensemble des procédures, des documents et des outils. 5](#_Toc200015149)

[(b) UO 2 : Réaliser des audits réguliers pour vérifier la conformité au RGPD. 7](#_Toc200015150)

[(c) UO 3 : assistance totale en cas de fuite ou de violation de données. 8](#_Toc200015151)

[(d) UO 4 : Donner un conseil simple en réponse à une question simple (exemple : « Comment faire si un salarié demande à rectifier des données le concernant ? »). 9](#_Toc200015152)

[(e) UO 5 : Assurer la réversibilité. 10](#_Toc200015153)

[Article IV. LES CONTRAINTES 12](#_Toc200015154)

[Section 4.01 Documents 12](#_Toc200015155)

[Section 4.02 Encadrement de l’accompagnement du projet 12](#_Toc200015156)

[Section 4.03 Engagement de stabilité de l’équipe 12](#_Toc200015157)

# LE CONTEXTE

## Le Grand Port Maritime de la Guyane

Le Grand Port Maritime de la Guyane (GPM-Guyane) est un établissement public à caractère industriel et commercial (EPIC), créé par le décret n° 2012-1105 du 1ᵉʳ octobre 2012.

Il a pour mission principale la gestion, l’aménagement et le développement des ports de la Guyane, en particulier le port de Dégrad des Cannes, situé à Remire-Montjoly, à proximité de Cayenne.

Le GPM-Guyane est responsable de l’ensemble des activités portuaires de la région, couvrant le transport maritime, la logistique, les trafics pétroliers, rouliers, minéraliers ainsi que le cabotage. Il joue également un rôle d’acteur de l’aménagement territorial et du développement économique, en partenariat avec les acteurs locaux et nationaux.

Au 1ᵉʳ octobre 2023, le GPM-Guyane compte 46 salariés. Il collabore avec plusieurs fournisseurs et clients, et gère un volume important de factures émises et reçues. Il accueille sur sa plateforme environ une centaine de personnes autorisées et à qui il fournit un badge d’accès.

En 2024, le port a franchi un seuil historique en dépassant pour la première fois le million de tonnes de marchandises traitées, atteignant 1,015 million de tonnes contre 932 000 tonnes en 2023.

Le GPM-Guyane occupe une position stratégique dans l’économie locale, assurant près de 99 % du fret régional. En 2021, le complexe industrialo-portuaire de la Guyane, incluant le GPM et 67 autres entreprises, représentait 1 180 emplois, soit environ 2 % de l’emploi salarié du territoire.

D’autres initiatives traduisent la volonté du GPM-Guyane de moderniser ses infrastructures tout en intégrant des objectifs environnementaux, consolidant ainsi son rôle d’acteur clé du développement durable et économique de la région.

En tant qu’EPIC, l’établissement est soumis au Code de la commande publique, qui encadre les procédures de passation des marchés en garantissant les principes de transparence, de mise en concurrence et d’égalité de traitement des candidats.

## Eléments liés au dossier

### Contexte du marché

Le Grand Port Maritime de Guyane (GPMG) souhaite procéder à une mise en conformité au RGPD, de l’ensemble de ses procédures, documents et outils.

A ce jour les données personnelles identifiées concernent :

* les salariés,
* les clients particuliers,
* les intervenants extérieurs (présents sur le port et qui font l’objet d’une enquête administrative pour des raisons de sureté),
* les candidats au recrutement (candidature spontanée ou réponse à une annonce) qui sont traités via un processus non informatisé dans un système RH.

Un précédent prestataire ayant déjà effectué pour cela plusieurs missions, il conviendra de partir du contexte existant.

Les données personnelles liées aux enquêtes administratives conduites pour des raisons de sureté sont particulièrement sensibles en raison de la grande exposition du GPMG aux risques liés aux différents trafics potentiels.

### Tâches réalisées par le précédent prestataire :

* La direction et les équipes ont été sensibilisées aux enjeux du RGPD et formées aux bonnes pratiques de protection des données.
* Les mentions légales et politiques de confidentialité ont été mises à jour selon le RGPD pour les actions en cours.
* Les formulaires de collecte de données intègrent des cases de consentement claires.

### Tâches en cours qui seront à terminer :

* La mise en conformité de l’ensemble des procédures, documents et outils a débuté.
* Les données personnelles traitées dans l’entreprise ont été identifiées en partie.
* Un registre de traitement de données existe mais devra être complété.
* Un contrôle des actions mises en place par le pôle SI concernant des mesures de protection (ex : chiffrement, accès restreints, mots de passe sécurisés) a débuté.
* L’implication des sous-traitants dans le respect du RGPD a été faite pour les sous-traitants actuels, mais pas pour les sous-traitants plus anciens.

### Tâches qui n’ont pas été réalisées :

* L’évaluation des risques liés aux traitement de données (ex : fuites, cyberattaques) n’a pas encore été faite, à date
* La mise en place d’un plan d’action en cas de fuite ou de violation de données n’existe pas.
* La procédure afin de savoir comment s’organiser pour notifier la CNIL sous 72h en cas de violation de données n’est pas écrite.
* Il n’y a pas d’audits réguliers pour vérifier la conformité au RGPD.

### Allotissement

Le présent marché n’est pas alloti, conformément à l’article R.2113-2 du Code de la commande publique.

### Objet du marché

Le présent marché a pour objet la mise en conformité au RGPD, de l’ensemble des procédures, documents et outils, pour le Grand Port Maritime de Guyane.  
Il s’agit de la protection des données personnelles des salariés, des clients particuliers, des intervenants extérieurs (présents sur le port et qui font l’objet d’une enquête de sureté), ainsi que des candidats au recrutement (en cas de processus non informatisé dans un système RH).  
Un précédent prestataire ayant déjà effectué pour cela plusieurs missions, il conviendra de partir du contexte existant.

# LES EXIGENCES

## Généralités

Le titulaire respecte l’ensemble des exigences précisées ci-dessous.

Il s’assure de mettre les moyens en œuvre pour, pour chaque exigence, être en mesure d’atteindre le niveau demandé pour chaque critère détaillant l’exigence.

Certaines exigences peuvent faire l’objet d’une réponse différente lors de l’offre initiale. Elles sont marquées « oui » dans la colonne « flexible au moment de l’offre ».

D’autres exigences peuvent faire l’objet de négociation pour les candidats qui seraient admis à déposer une offre. Elles sont marquées « oui » dans la colonne « Flexibilité au moment de la négociation ».

Enfin, certaines exigences peuvent être améliorées et amener une valeur interne meilleure lors de l’analyse des offres pour le critère d’attribution correspondant. Elles sont marquées « oui » dans la colonne « améliorable ? » ; Si elles sont marquées « non », le fait de faire mieux ne sera pas valorisé.

Le fournisseur s’assure qu’il est en mesure de respecter les exigences et décrit les moyens qu’il met en place dans son mémoire technique.

Tous les délais sont exprimés en jours ouvrés.

## Prestations attendues :

### UO 1 : Mise en conformité au RGPD de l’ensemble des procédures, des documents et des outils.

#### Attendu global

Dans le cadre de la présente mission, le titulaire assure la couverture de l’ensemble des besoins suivants :

* Mise en conformité des procédures et des outils documentaires concernant les salariés
* Mise en conformité des procédures et des outils documentaires concernant les clients particuliers
* Mise en conformité des procédures et des outils documentaires concernant les intervenants extérieurs faisant l’objet d’enquête de sureté
* Mise en conformité des procédures et des outils documentaires concernant les candidats au recrutement.

Il fournit les procédures et les documents

Il forme les interlocuteurs à ces procédures et outils documentaires

Il audite les outils informatiques y compris le site web et établira un plan d’action de mise en conformité si nécessaire.

Il indique à la CNIL le nom du DPO

#### Production de livrables :

Il sera au moins exigé la livraison des documents suivants :

* Registre des traitements (conforme à l’article 30 RGPD).
* Politique de confidentialité (site web, RH, partenaires…).
* Modèles de clauses contractuelles et avenants (sous-traitance, partenaires…).
* Procédures internes (gestion des droits des personnes, violation de données, conservation…).
* Plan de formation et de sensibilisation: pour l’ensemble du personnel.
* Rapport d’audit initial et rapport de fin de mission.
* Tout autre document précisé dans l’annexe 2 à l’acte d’engagement.

Pour cela, le titulaire prend en compte les contraintes et grands principes du RGPD :

* minimisation des données, limitation des finalités, exactitude, sécurité, etc.
* Mise en œuvre de mesures de sécurité appropriées (techniques et organisationnelles).
* Garantie de l’effectivité des droits des personnes concernées (accès, rectification, effacement, etc.).

#### Résumé des exigences (CRINIFLEX)

**Dans le cadre du contexte décrit** ci-dessus, et dans le respect des contraintes du paragraphe « contraintes », le titulaire respecte l’ensemble des exigences et atteint les niveaux décrits ci-dessous :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | CRI | NI | FLEX |
|  | Exigences | Critère d'exigence | Niveau | Variante | Négociable ou pas | Améliorable ou pas |
| **UO1** | **Mettre en conformité l’ensemble des procédures, des documents et des outils** | Conformité au niveau juridique | 100% | NON | NON | OUI |
| **UO1** | **Mettre en conformité l’ensemble des procédures, des documents et des outils** | Conformité au niveau technique | 100% | NON | NON | OUI |
| **UO1** | **Mettre en conformité l’ensemble des procédures, des documents et des outils** | Respect du délai mentionné en annexe 2 à l'Acte d'engagement | 100% | NON | OUI | OUI |

### 

### UO 2 : Réaliser des audits réguliers pour vérifier la conformité au RGPD.

Une fois l’UO1 terminée, il procède régulièrement (a priori 2 fois par an) à des audits, sur demande du GPM-Guyane.

L’audit porte *a minima* sur :

#### Vérification du maintien de la conformité

* Revue du registre des traitements : actualisation, complétude, cohérence avec les activités réelles.
* Contrôle de la mise à jour des politiques internes : confidentialité, gestion des incidents, conservation des données.
* Vérification de la documentation : PIA à jour, consentements, contrats avec les sous-traitants.
* Contrôle de la traçabilité des demandes liées aux droits des personnes (accès, effacement, etc.).

#### Évaluation des nouveaux risques

* Analyse des nouveaux traitements mis en place depuis le dernier audit.
* Identification de tout changement technique ou organisationnel ayant un impact sur la protection des données.
* Recommandations éventuelles de nouvelles analyses d’impact (PIA).

#### Tests de conformité opérationnelle

* Vérification terrain (entretiens, sondages, tests) pour s'assurer de l’effectivité des procédures (ex : procédure de notification des violations de données, gestion des droits).
* Évaluation du niveau de sensibilisation du personnel (par exemple par des questionnaires ou mises en situation).

#### Contrôle des relations avec les sous-traitants

* Vérification des clauses contractuelles RGPD (article 28).
* Contrôle de la traçabilité et du suivi des sous-traitants.
* Revue de la politique de transferts de données hors UE (si applicable).

#### Suivi des actions correctives précédentes

* Bilan des recommandations issues de l’audit précédent : lesquelles ont été mises en œuvre ? Lesquelles sont en retard ou inapplicables ?

#### Livrables obligatoires de l’audit annuel

Le fournisseur remet un rapport d’audit détaillé, avec :

* Constatations,
* Écarts éventuels,
* Recommandations.
* Un plan d’action actualisé avec priorités, échéances et personnes responsables.
* Une synthèse destinée à la direction, claire et exploitable pour le pilotage RGPD.

#### Résumé des exigences (CRINIFLEX)

**Dans le cadre du contexte décrit** ci-dessus, et dans le respect des contraintes du paragraphe « contraintes », le titulaire respecte l’ensemble des exigences et atteint les niveaux décrits ci-dessous :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | CRI | NI | FLEX |
|  | Exigences | Critère d'exigence | Niveau | Variante | Négociable ou pas | Améliorable ou pas |
| **UO2** | **Réaliser des audits réguliers pour vérifier la conformité au RGPD** | Audit à une fréquence annuelle pour la partie juridique | OUI | OUI | OUI | OUI |
| **UO2** | **Réaliser des audits réguliers pour vérifier la conformité au RGPD** | Audit à une fréquence annuelle pour la partie technique | OUI | OUI | OUI | OUI |
| **UO2** | **Réaliser des audits réguliers pour vérifier la conformité au RGPD** | Livraison d’un rapport d’audit | OUI | NON | NON | OUI |
| **UO2** | **Réaliser des audits réguliers pour vérifier la conformité au RGPD** | Respect du délai mentionné dans l'annexe "Valeur Technique" à l'Acte d'engagement | 100% | NON | OUI | OUI |

### UO 3 : assistance totale en cas de fuite ou de violation de données.

En cas de déclenchement, le titulaire assure sur demande les taches suivantes :

* + Une aide à l’analyse de la violation :
* Aide à détermination si c’est une violation au sens du RGPD.
* Identifier les données concernées, les personnes affectées, les causes probables.
* Une qualification de la gravité de la violation (risque élevé ou non pour les droits et libertés).
* Mise à jour du registre des violations.
* Documentation de la gestion de l’incident pour preuve de conformité (traçabilité, preuves de réaction rapide, etc.).
* Mise à jour du registre des traitements si nécessaire (ex : si un traitement a été modifié ou arrêté suite à l’incident).
* Analyse du risque juridique et réputationnel.
  + Une aide pour décider s’il faut notifier la CNIL et/ou informer les personnes concernées (conformément aux articles 33 et 34 RGPD).

Puis sur demande, en cas de nécessité :

* Assistance à la notification CNIL et à la rédaction des communications
* Aide à la rédaction de la notification CNIL, avec les éléments exigés : nature de la violation, mesures correctives, contacts, etc.
* Aide à la rédaction de la communication aux personnes concernées, si nécessaire, avec un langage clair.
* Conseil sur le timing et les obligations formelles (ex. : délai de 72 h pour notifier la CNIL).

Et au temps passé, si nécessaire :

* Revue des procédures de sécurité
* Réalisation d’un audit réactif des mesures de sécurité existantes.
* Révision ou formalisation des nouvelles procédures internes (ex : gestion des accès, conservation, sauvegarde)
* Appui en cas de contrôle de la CNIL.
* Coordination éventuelle avec les équipes SSI, juridiques et DSI.

#### Résumé des exigences (CRINIFLEX)

**Dans le cadre du contexte décrit** ci-dessus, et dans le respect des contraintes du paragraphe « contraintes », le titulaire respecte l’ensemble des exigences et atteint les niveaux décrits ci-dessous :

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Exigences | Critère d'exigence | Niveau | Variante | Négociable ou pas | Améliorable ou pas |
| **UO3** | **Faire appliquer le plan d'action en cas de fuite ou de violation de données**. | Documenter l’incident en interne | Délai max 48h | NON | NON | OUI |
| **UO3** | **Faire appliquer le plan d'action en cas de fuite ou de violation de données**. | Prévenir la CNIL | Délai max 72h | OUI | OUI | OUI |
| **UO4** | **Donner un conseil simple en réponse à une question simple** | Respect du délai mentionné dans l'annexe "Valeur Technique" à l'Acte d'engagement | Délai max 72h | OUI | OUI | OUI |

### UO 4 : Donner un conseil simple en réponse à une question simple (exemple : « Comment faire si un salarié demande à rectifier des données le concernant ? »).

Le titulaire répond aux questions simples du correspondant RGPD du port, ou de toute personne mandatée en cas d’absence, au cas par cas.

#### Résumé des exigences (CRINIFLEX)

**Dans le cadre du contexte décrit** ci-dessus, et dans le respect des contraintes du paragraphe « contraintes », le titulaire respecte l’ensemble des exigences et atteint les niveaux décrits ci-dessous :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | CRI | NI | FLEX |
|  | Exigences | Critère d'exigence | Niveau | Variante | Négociable ou pas | Améliorable ou pas |
| **UO4** | **Donner un conseil simple en réponse à une question simple** | Respect du délai mentionné dans l'annexe "Valeur Technique" à l'Acte d'engagement | Délai max 72h | OUI | OUI | OUI |

### UO 5 : Assurer la réversibilité.

#### X.1. Objet de la réversibilité

La réversibilité vise à assurer une transition efficace des connaissances techniques, fonctionnelles et juridiques RGPD du titulaire vers le(s) futur(s) DPO, garantissant la continuité de la conformité et des actions menées.

##### X.2. Obligations du Titulaire en matière de réversibilité (spécifiques DPO RGPD)

Le titulaire s'engage à :

* Fournir une documentation exhaustive spécifique RGPD, incluant notamment : registre des activités de traitement, AIPD, politiques et procédures, conseils RGPD, relations CNIL, supports de sensibilisation, état des mises en conformité.
* Transmettre cette documentation au plus tard deux mois avant la fin du marché, avec un inventaire.
* Organiser des sessions de transfert de connaissances spécifiques RGPD sur l'état de la conformité, les procédures, la méthodologie (registre, AIPD), les bonnes pratiques, la gestion des violations, l'exercice des droits et les relations CNIL.
* Fournir une assistance technique post-transfert spécifique RGPD ponctuelle.

#### X.3. Modalités de mise en œuvre

Les modalités (calendrier, contenu des sessions, assistance) seront définies en concertation avec le GPM-Guyane. Un plan de réversibilité RGPD pourra être élaboré.

#### X.4. Documents et informations à fournir (liste non exhaustive)

* Registre des activités de traitement (à jour)
* AIPD (réalisées et méthodologie)
* Politiques et procédures RGPD internes
* Guides exercice des droits
* Procédures gestion des violations
* Modèles clauses protection des données
* Informations outils RGPD
* Préconisations et plans d'actions conformité
* Rapports d'activité DPO
* Contacts pertinents

#### X.5. Conditions de collaboration

Le titulaire désignera des interlocuteurs experts RGPD. Le GPM-Guyane désignera les personnes chargées de la réception et de la participation. Une communication régulière sera essentielle.

#### Résumé des exigences (CRINIFLEX)

**Dans le cadre du contexte décrit** ci-dessus, et dans le respect des contraintes du paragraphe « contraintes », le titulaire respecte l’ensemble des exigences et atteint les niveaux décrits ci-dessous :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | CRI | NI | FLEX |
|  | Exigences | Critère d'exigence | Niveau | Variante | Négociable ou pas | Améliorable ou pas |
| **UO5** | **Assurer la réversibilité à l'issue du marché** | Fournir l'ensemble des documents concernés dans le délai de deux mois avant la fin du marché | 100% | NON | NON | OUI |

# LES CONTRAINTES

## Documents

Les documents fournis sont fournis en mode « documents de la suite office ». Les PDF sont proscrits.

## Encadrement de l’accompagnement du projet

Afin de garantir une mise en œuvre efficace et adaptée à la taille de l’établissement, le titulaire est tenu de respecter les principes suivants pendant toute la durée du projet :

Le titulaire désigne un interlocuteur unique (chef de projet) dédié, qui assurera le suivi régulier du projet, en lien avec le référent du pouvoir adjudicateur.

## Engagement de stabilité de l’équipe

Dans le cadre de cette mission, le candidat s’engage sur la stabilité de l’équipe projet. Tout changement devra être expressément validé par la maîtrise d’ouvrage. En cas de remplacement, le candidat devra assurer une période de transition avec passation effective, sans surcoût pour l’acheteur.