

Direction des Systèmes de Transport et Exploitation

Programme fonctionnel

2024DC001 - Mise en œuvre et maintien en condition opérationnelle d'une plateforme des données de supervision des systèmes du Grand Paris Express

ÉMETTEUR

Date	Indice	Suivi des modifications
04/11/2024	1	Création

RÉFÉRENCES

Code GED : DSTE_06_ACT_STE_002360_1

2024DC001 – PROGRAMME FONCTIONNEL
CODE GED : DSTE_06_ACT_STE_002360_1

Ce document est la propriété de la Société des grands projets. Toute diffusion ou reproduction intégrale ou partielle est autorisée pour et dans la limite des besoins découlant des prestations ou missions du marché conclu avec le titulaire destinataire.

Sommaire

1	PRESENTATION DE LA SOCIETE DES GRANDS PROJETS	6
1.1	Origine et mission	6
1.2	Organisation de la SGP	7
1.3	Organisation avec les partenaires du Grand Paris Express	8
1.3.1	Ile-de-France Mobilités	8
1.3.2	RATP Infrastructures	8
1.3.3	Opérateurs de transport	9
1.4	Les systèmes du Grand Paris Express	9
2	PRESENTATION DU MARCHÉ	12
2.1	Contexte	12
2.2	Objet et finalité du marché	12
2.3	Objectifs	12
2.4	Exemple de cas d'usage	13
2.5	Synoptique de la plateforme des données de supervision	13
2.6	Description des différentes « zones » de la plateforme des données	14
2.6.1	Zone A - Stockage	14
2.6.2	Zone B - Interfaces	15
2.6.3	Zone C - Zone de traitement	15
2.6.4	Zone D - Restitution des données à la SGP et aux autres acteurs	15
2.7	Périmètre du marché	15
2.8	Description des données	15
2.8.1	Données de supervision des systèmes	15
2.8.2	Données d'exploitation et de maintenance	16
2.8.3	Données d'entrée	17
2.9	Outils en interface avec le projet	18
2.9.1	Zone de stockage « Outscale »	18
2.9.2	Sharepoint	18
2.9.3	Active Directory SGP	18
2.9.4	Utilisation de la GED SGP	18
3	DESCRIPTION DES PRESTATIONS	18
3.1	Prescriptions applicables à l'ensemble des prestations	18
3.2	Infrastructure, logiciels et maintenance associée	21
3.2.1	UO_I1 - Fourniture de l'infrastructure logicielle	21
3.2.2	UO_I2 - Installation et configuration des logiciels	21
3.2.3	UO_I3 - Audit et conformité des logiciels	22
3.2.4	UO_I4 - Mise à jour et évolution des logiciels	23
3.2.5	UO_I5 - Sécurité et sauvegarde des données	23
3.2.6	UO_I6 - Gestion des utilisateurs et des accès	23

3.2.7	UO_I7 - Suivi financier de la consommation du cloud	23
3.3	Accompagnement métier et développements	23
3.3.1	UO_D1 - Définition de l'architecture de la plateforme de données	23
3.3.2	UO_D2 - Développement et intégration des modules de base	24
3.3.3	UO_D3 - Requêtes sur critères	25
3.3.4	UO_D4 - Mise en place d'un outil de gestion des données de référence	27
3.3.5	UO_D5 - Découpe de fichiers selon des critères géographiques et systèmes	28
3.3.6	UO_D6 - Spécification et déploiement d'une solution basée sur du machine learning et/ou deep learning	31
3.3.7	UO_D7 - Accompagnement à l'analyse des défaillances	32
3.3.8	UO_D8 - Mise à disposition des données pour d'autres acteurs via une interface web sécurisée	34
3.3.9	UO_D9 - Formation et conduite du changement	37
3.3.10	UO_D10 - POC - preuve de concept	38
3.3.11	UO_D11 - Réversibilité	39
3.3.11.1	Objectifs	39
3.3.11.2	Description des prestations attendues	39
3.3.11.3	Livrables	41
3.3.12	UO_D12 - Maintenance évolutive	42
3.3.13	UO_D13 - Support utilisateur et assistance technique	43
3.3.14	UO_D14 - Monitoring de la plateforme de données	43
3.4	Prestations complémentaires sur devis	43
4	INFRASTRUCTURE ET SUITE LOGICIELLE	44
4.1	Exigences générales	44
4.2	Exigences relatives à l'infrastructure de la plateforme	45
4.2.1	Exigences techniques	45
4.2.1.1	Architecture	45
4.2.1.2	Supervision	46
4.2.1.3	Environnements	47
4.2.1.4	Gestion et optimisation de la capacité, de la disponibilité et de la performance globale	49
4.2.1.5	Interfaces Homme-Machine (IHMs)	50
4.2.1.6	Gestion des sauvegardes	50
4.2.1.7	Scalabilité et gestion de la charge	52
4.2.2	Exigences de services	52
4.2.2.1	Gestion des Demandes et Incidents	52
4.2.2.2	Administration	54
4.2.2.3	Exploitation courante des infrastructures systèmes et services	55
4.2.2.4	Priorités et engagements	55
4.3	Sécurité de la plateforme	58
4.3.1	Sécurité des prestations	58
4.3.2	Hébergement des données et des services	60
4.3.3	Disponibilité de la Plateforme	61
4.3.4	Sauvegardes	62
4.3.5	Chiffrement des flux et gestion des certificats	63

4.3.6	Développement sécurisé	65
4.3.7	Emails	66
4.3.8	Nom de domaine et hébergement	67
4.3.9	Lutte contre les intrusions	67
4.3.10	Lutte contre les attaques	68
4.3.11	Administration et gestion des accès	69
4.3.12	Traçabilité des accès et supervision	71
4.3.13	Sécurité des interfaces de programmation d'applications (API)	71
4.4	Intégration et orchestration des données	72
4.5	Stockage des données traitées	73
4.6	Visualisation et reporting	73
4.7	Gouvernance des données	73
4.8	Documentation, formation et support	73
5	MAINTIEN EN CONDITION OPERATIONNELLE (MCO)	75
5.1	Maintenance corrective, mise à jour et évolution des logiciels	75
5.2	SLA	77
5.3	Sécurité et sauvegarde des données	78
5.4	Gestion des utilisateurs et des accès	79
5.5	Suivi financier de la consommation du cloud	80
5.6	Support utilisateur et assistance technique	82
5.7	Monitoring de la plateforme de données	83
6	EXIGENCES RELATIVES AU MANAGEMENT DE PROJET	85
6.1	Organisation projet	85
6.2	Participation aux ateliers collaboratifs à la demande de la SGP	85
6.3	Reporting et suivi des indicateurs	86
6.4	Proposition technique pour le développement, le maintien ou l'optimisation de la plateforme de données	86
6.5	Pipeline de livraison	86
6.6	Qualité des livrables	87
7	MODALITES D'EXECUTION DES PRESTATIONS	88
7.1	Organisation au sein de la Société des grands projets	88
7.2	Organisation attendue du Titulaire	88
7.3	Gouvernance et comitologie	89
7.3.1	Gouvernance	89
7.3.2	Comitologie	89
7.4	Outil mis à disposition de la SGP dans le cadre du suivi de projet	90
7.4.1	Journal des modifications	90
7.4.2	Suivi des expressions de besoin et recueil des anomalies	90
7.5	Exigences qualités au titre du marché	91
7.5.1	Plan d'assurance sécurité (PAS)	91

7.5.2	Plan d'assurance qualité (PAQ)	91
7.6	Niveaux de séniorité des profils	92
8	LISTE DES SIGLES ET ABREVIATIONS	93
9	LISTE DES DOCUMENTS ANNEXES	95

LISTE DES FIGURES

Figure 1	: Carte du réseau de transport public du Grand Paris Express à horizon 2031.	7
Figure 2	: Organigramme de la Société des grands projets	8
Figure 3	: Les systèmes du GPE : les différents groupes d'ouvrage (GO) et leurs interfaces	10
Figure 4	: Les systèmes du GPE en gares et ouvrages de service	10
Figure 5	: Les systèmes du GPE en tunnel	11
Figure 6	: Synoptique de la plateforme des données	14

1 PRESENTATION DE LA SOCIETE DES GRANDS PROJETS

1.1 Origine et mission

Établissement public d'État, la Société des grands projets (SGP) est chargée de la conception et de la réalisation du Grand Paris Express (GPE), le nouveau métro en Île-de-France.

En tant que maître d'ouvrage, la SGP a pour missions d'assurer :

- La construction des quatre nouvelles lignes de métro (15, 16, 17 et 18) ainsi que le prolongement de la ligne 14 entre Mairie de Saint-Ouen et Saint-Denis - Pleyel ;
- La construction et l'aménagement des gares et ouvrages nécessaires au bon fonctionnement du réseau ;
- L'aménagement des futurs quartiers de gare du Grand Paris Express, en concertation étroite avec les élus locaux et les établissements publics concernés.

La SGP a temporairement délégué la maîtrise d'ouvrage opérationnelle du prolongement sud de la ligne 14 (entre Paris et l'aéroport d'Orly) à la RATP. Elle conserve néanmoins la responsabilité des relations territoriales, des acquisitions foncières et des projets de valorisation de ce prolongement.

▪ Le Grand Paris

La loi du 3 juin 2010 définit le Grand Paris comme « un projet urbain, social et économique d'intérêt national » qui vise à renforcer l'attractivité de la région capitale et soutenir la concurrence des autres métropoles mondiales.

Afin d'unir les grands territoires stratégiques de la Région Île-de-France et de réduire les déséquilibres sociaux et territoriaux, la loi du 3 décembre 2010 prévoit que le projet du Grand Paris s'appuie sur la création d'un réseau de transport public de voyageurs (Grand Paris Express) dont la réalisation est confiée à la Société du Grand Paris renommée Société des grands projets depuis la loi n°2023 1269 du 27 décembre 2023 et le financement des infrastructures est assuré par l'État.

▪ Le Grand Paris Express

Avec 200 km de métro, 4 nouvelles lignes, 1 ligne prolongée et 68 gares, le Grand Paris Express est le projet de transport et d'aménagement qui permettra chaque jour à près de 3 millions de voyageurs de se déplacer plus facilement et plus rapidement de banlieue à banlieue sans passer par Paris.

Le projet est découpé en sept lots de travaux allant de :

- Olympiades à Aéroport d'Orly (Ligne 14 Sud) - Maîtrise d'ouvrage partagée avec la RATP ;
- Pont de Sèvres à Noisy - Champs (Ligne 15 Sud) ;
- Saint-Denis - Pleyel à Pont de Sèvres (Ligne 15 Ouest) ;
- Saint-Denis - Pleyel à Champigny Centre (Ligne 15 Est) ;

- Mairie de Saint-Ouen à Saint-Denis - Pleyel, Noisy - Champs au Bourget, du Bourget à Saint-Denis - Pleyel (Lignes 14 Nord, 16 et 17) ;
- Le Bourget au Mesnil-Amelot (Ligne 17 Nord) ;
- Aéroport d'Orly à Versailles Chantiers (Ligne 18).

Le nouveau métro couvrira donc les départements de l'Essonne, des Hauts-de-Seine, de la Seine-et-Marne, de la Seine-Saint-Denis, du Val-de-Marne, du Val d'Oise, des Yvelines et de Paris.

Il est progressivement mis en service à partir de 2024. Son achèvement aura lieu à l'horizon 2031.

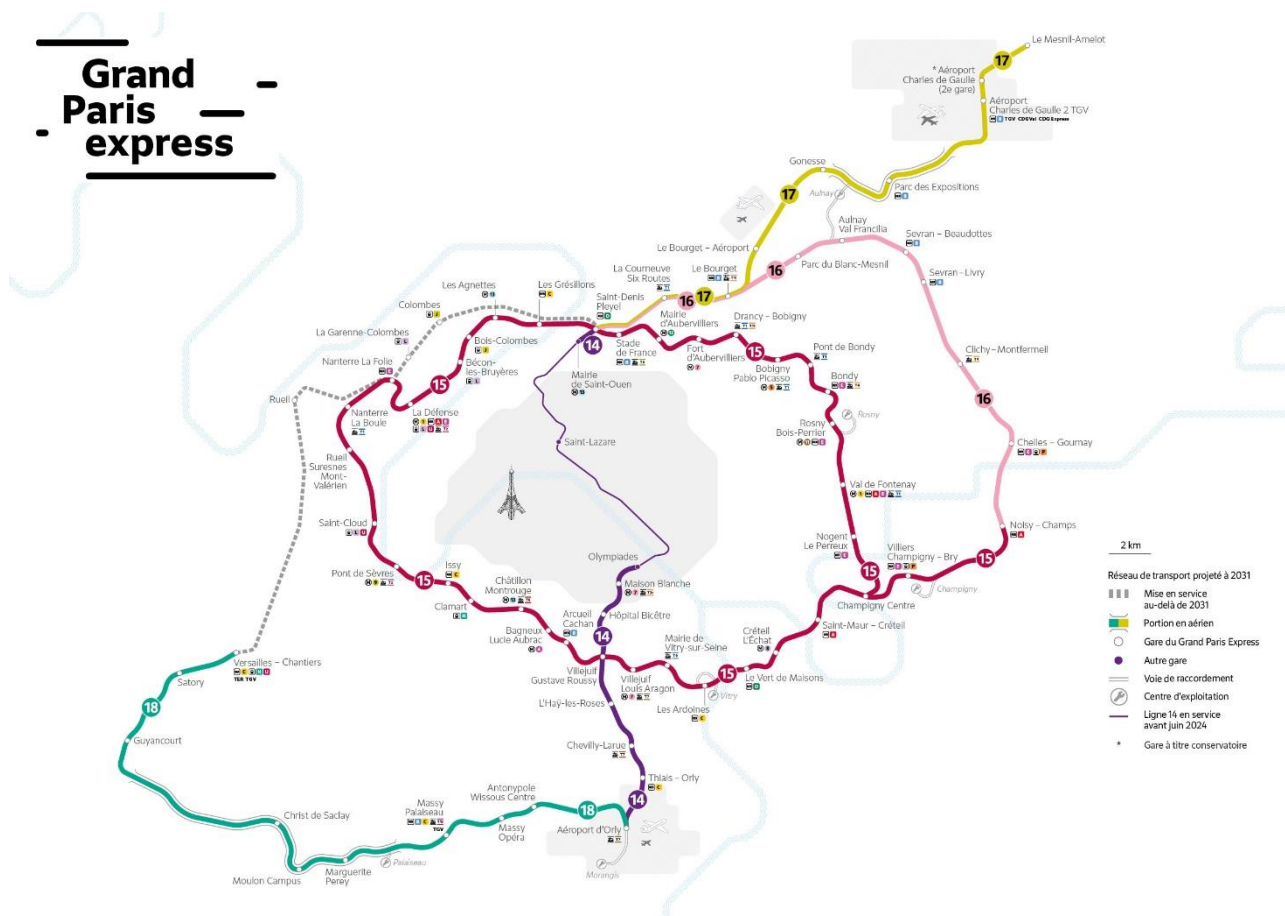


Figure 1 : Carte du réseau de transport public du Grand Paris Express à horizon 2031.

1.2 Organisation de la SGP

La SGP est organisée en « mode projet » à la fois pour privilégier l'opérationnel et être en prise avec les enjeux sectoriels du futur métro. La gouvernance de la SGP s'appuie principalement sur un directoire et un conseil de surveillance.

Le schéma ci-après détaille l'organisation de la SGP.

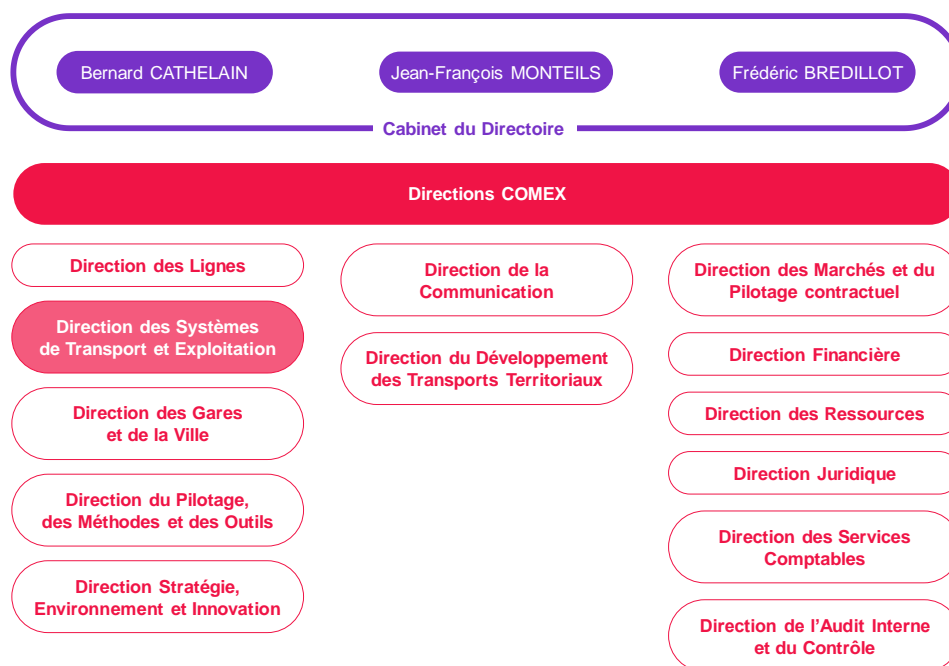


Figure 2 : Organigramme de la Société des grands projets

Les prestations de ce marché sont sous la responsabilité de la Direction des Systèmes de Transport et Exploitation (DSTE).

1.3 Organisation avec les partenaires du Grand Paris Express

1.3.1 Ile-de-France Mobilités

Île-de-France Mobilités (IdFM) est l'autorité organisatrice des services de transports publics réguliers de personnes dans la région Île-de-France et, à ce titre notamment, désigne les futurs exploitants (opérateurs de transport) des lignes du GPE, également mainteneurs du matériel roulant voyageurs.

De par son rôle, IdFM définit les niveaux de service, transmet la demande d'autorisation de mise en service du projet au préfet de la région Ile-de-France et organise les adaptations d'offre de transport en Ile-de-France en relation avec les impacts du projet (réseau de bus, gares existantes, etc.).

1.3.2 RATP Infrastructures

La RATP prise en sa qualité de Gestionnaire d'Infrastructure (RATP Infrastructures) est le gestionnaire technique des infrastructures des lignes 15, 16, 17 et 18 mises en service et est à ce titre garant du maintien de leur sécurité et de leur disponibilité opérationnelle.

Le périmètre du gestionnaire d'infrastructure couvre l'ensemble des infrastructures du GPE, les systèmes du transport (voie, énergie, ventilation/désenfumage en tunnel, automatismes de conduite, épuisement en voie, RMS, Radio exploitant, etc.), les ouvrages annexes ainsi que le gros œuvre des gares (bâtiment nu).

Ne rentrent pas dans le périmètre du mainteneur des infrastructures la maintenance du Matériel Roulant Voyageur ainsi que de l'ensemble des systèmes électromécaniques et relatifs à la communication en gare (billettique, vidéosurveillance, contrôle d'accès, information voyageurs, sonorisation et façades de quai par exemple). Cette responsabilité incombe aux opérateurs de transport.

La collaboration entre la SGP et RATP Infrastructures a pour objet la préparation de la gestion technique des lignes, des ouvrages et des installations du réseau de transport public du Grand Paris qui seront remises à RATP Infrastructures après leur réception.

1.3.3 Opérateurs de transport

Les Opérateurs de Transport (OT) sont désignés par l'autorité organisatrice Île-de-France Mobilités et ont notamment en charge l'exploitation et la maintenance des trains voyageurs, ainsi que de l'ensemble des systèmes électromécaniques et relatifs à la communication en gare (billettique, vidéosurveillance, contrôle d'accès, information voyageurs, sonorisation et façades de quai par exemple).

1.4 Les systèmes du Grand Paris Express

Les « systèmes » dans ce marché désignent l'ensemble des équipements techniques composant le système de transport du Grand Paris Express, à savoir (liste non exhaustive) :

- L'énergie électrique (haute tension, basse tension, énergie de traction),
- Le profil aérien de contact / caténaire ou 3ème rail d'alimentation,
- Les courants faibles,
- Les automatismes de conduite et commandes centralisées,
- Les matériels roulant et véhicules de maintenance,
- Les façades de quais
- Les équipements électromécaniques en gare, en ouvrage ou en ligne,
- La voie ferrée.

Ce périmètre correspond aux éléments figurant dans les schémas ci-dessous.

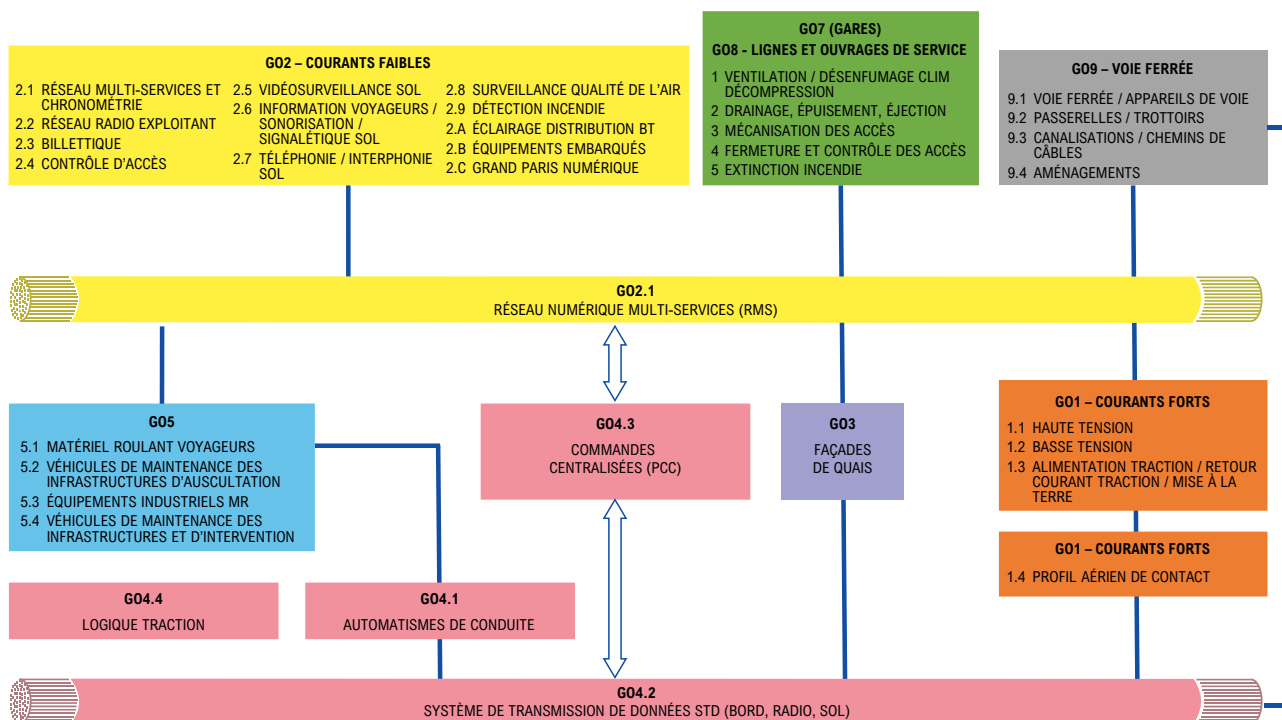


Figure 3 : Les systèmes du GPE : les différents groupes d'ouvrage (GO) et leurs interfaces

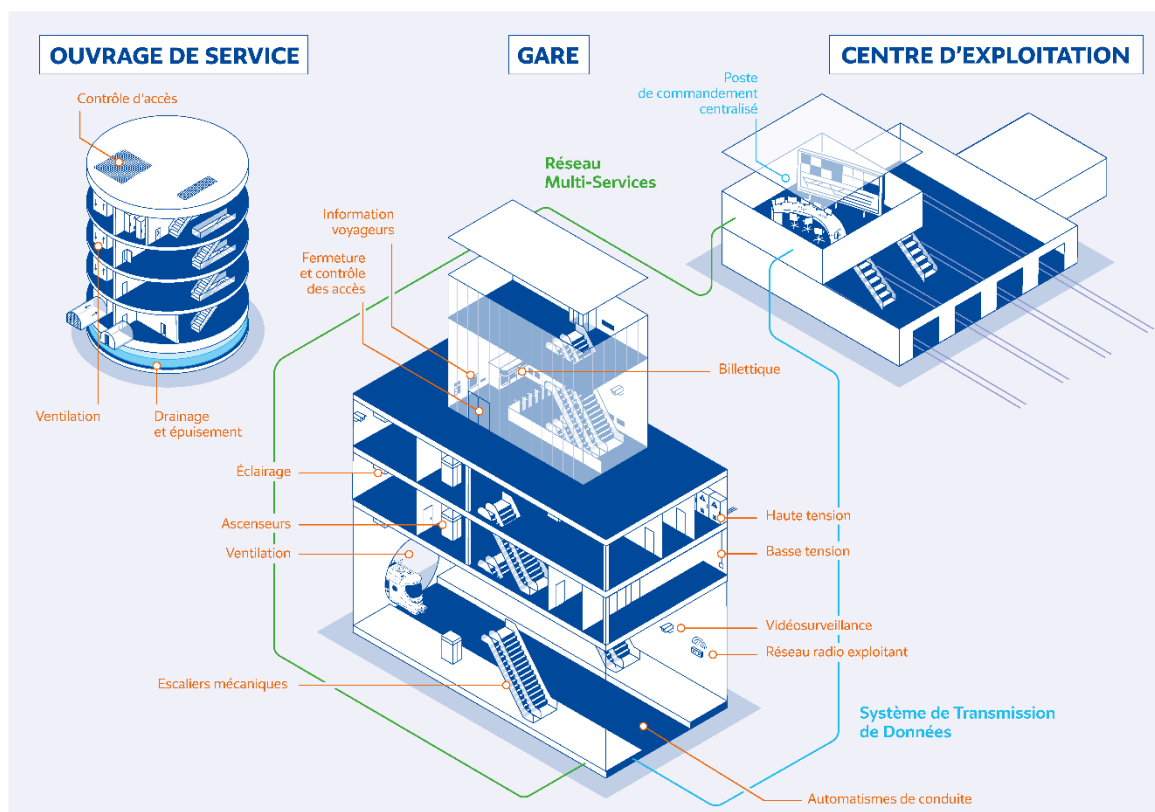


Figure 4 : Les systèmes du GPE en gares et ouvrages de service

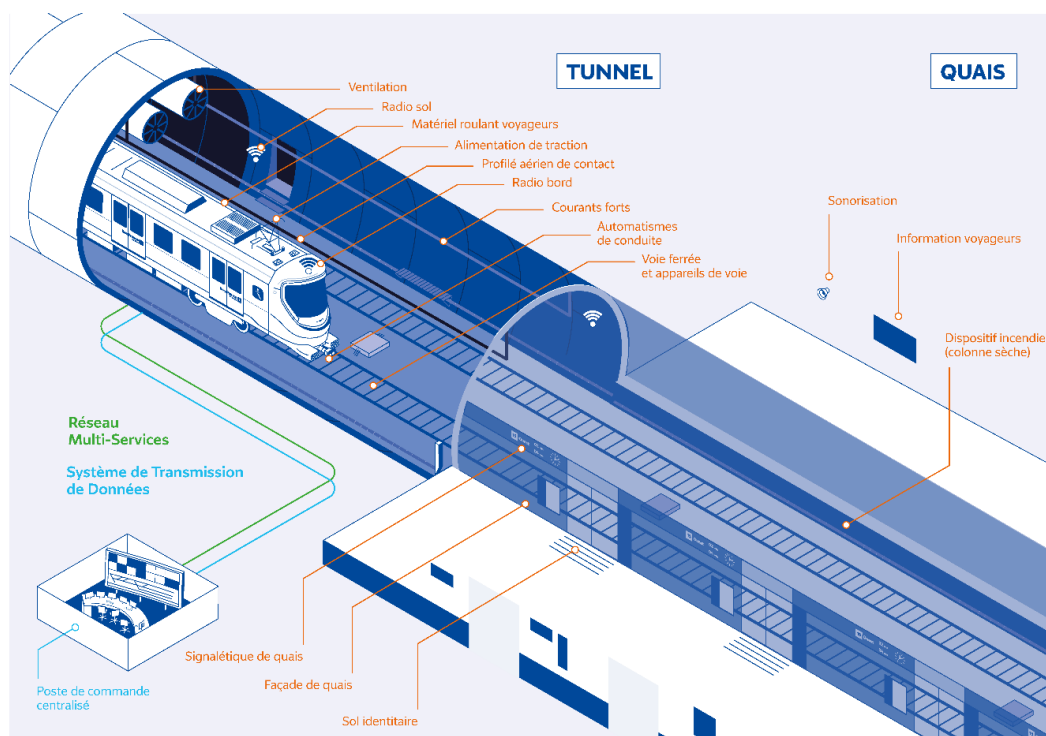


Figure 5 : Les systèmes du GPE en tunnel

Les Commandes Centralisées (CC) regroupent les équipements du système de transport qui permettent à un ensemble d'opérateurs ou à un automate de superviser et commander depuis un ou plusieurs sites des équipements distants.

Ainsi, les commandes centralisées sont en interface avec la quasi-totalité des équipements et permettent d'en faire la supervision et de collecter des informations et états associés. Les commandes centralisées ont ainsi la capacité de générer un ou plusieurs fichiers de synthèse agrégeant les données de supervision du GPE.

Le GPE est composé de trois Postes de Commandes Centralisées (PCC) - un par unité d'exploitation - qui fourniront chacun un fichier de données :

- Ligne 15 - éditeur Hitachi GTS ;
- Lignes 16/17 - éditeur Hitachi GTS ;
- Ligne 18 - éditeur Alstom.

2 PRESENTATION DU MARCHE

2.1 Contexte

La Société des grands projets (SGP) assure notamment la mise en œuvre des systèmes de transport du Grand Paris Express (GPE) et leur cohérence (matériel roulant et véhicules de maintenance, automatismes de conduite et commandes centralisées, courants faibles, voie ferrée et caténaire, énergie (haute tension / basse tension / traction), ventilation/désenfumage tunnel, etc.).

Les spécificités de l'exploitation du GPE (exploitation des lignes 16 et 17 incluant un tronçon commun, mutualisation de plusieurs fonctionnalités systèmes entre les lignes 15 et 16/17, etc.) et de la maintenance (un gestionnaire d'infrastructure unique pour toutes les lignes) nécessitent, au-delà de l'intégration traditionnelle entre infrastructures et systèmes, une cohérence de tous les systèmes du GPE quelle que soit la ligne.

Le présent marché s'inscrit dans le cadre du projet du Grand Paris Express.

2.2 Objet et finalité du marché

L'objet du marché est la réalisation d'une plateforme des données de supervision des systèmes du GPE. Les « systèmes » désignent l'ensemble des équipements techniques composant le Grand Paris Express, y compris les équipements en gare.

La finalité du marché est de pouvoir objectiver les défaillances remontées par différents acteurs et de mettre en place des retours d'expérience pour améliorer les systèmes du Grand Paris Express entre les différentes lignes et en prévision de leurs prolongements.

2.3 Objectifs

La SGP souhaite se doter d'une « plateforme des données de supervision des systèmes du GPE » (ou plus simplement dans le présent document « la plateforme de données ») permettant de répondre aux objectifs présentés ci-dessous.

- Objectiver la qualité de service :
 - Pouvoir fournir des arguments objectifs pour assurer des imputations justes des défaillances et retards ;
 - Challenger les indicateurs fournis par les différents acteurs du GPE (y compris les équipementiers).
- Construire des retours d'expérience de la performance des équipements :
 - Appliquer des actions correctives, à la suite d'un incident, à l'ensemble des lignes impactées par ce type d'incident ;

- Bénéficier des retours d'expérience dans le cadre des prolongements et interlignes.

Les informations consolidées et traitées sont ensuite mises à disposition d'utilisateurs de la SGP et de ses partenaires, parmi lesquels :

- Ile-de-France Mobilités ;
- Les opérateurs de transports (1 entité par unité d'exploitation) ;
- RATP Infrastructures ;
- Les Titulaires des marchés systèmes de la SGP pendant les phases de garantie de leurs équipements.

2.4 Exemple de cas d'usage

Parmi les cas d'usage envisagés pour la plateforme des données, la SGP souhaite récupérer l'ensemble des informations utiles à la compréhension d'un incident ou de la défaillance d'un composant du système de transport pendant les essais ou l'exploitation de celui-ci.

Exemple de cas d'usage : un freinage d'urgence non identifié conduisant à une interruption de trafic a lieu sur la ligne 18 entre les stations Massy Opéra et Massy Palaiseau. Les mainteneurs de l'opérateur de transport et du gestionnaire d'infrastructure sont intervenus afin de permettre la reprise du trafic. Toutefois, il n'est pas possible a priori d'identifier précisément l'origine de cette interruption et d'imputer éventuellement une responsabilité vers un des acteurs impliqués. En recroisant un certain nombre de données issues de plusieurs sous-systèmes, la plateforme doit ainsi permettre d'identifier plus facilement l'origine de la panne et la(les) responsabilité(s) associée(s).

2.5 Synoptique de la plateforme des données de supervision

La plateforme de données de supervision des systèmes est composée de différentes « zones ». Ces zones portent des fonctions différentes et sont représentées ci-dessous dans un synoptique simplifié. Le présent marché porte sur la solution de traitement des données et ses interfaces (zones désignées B, C et D du schéma ci-après).

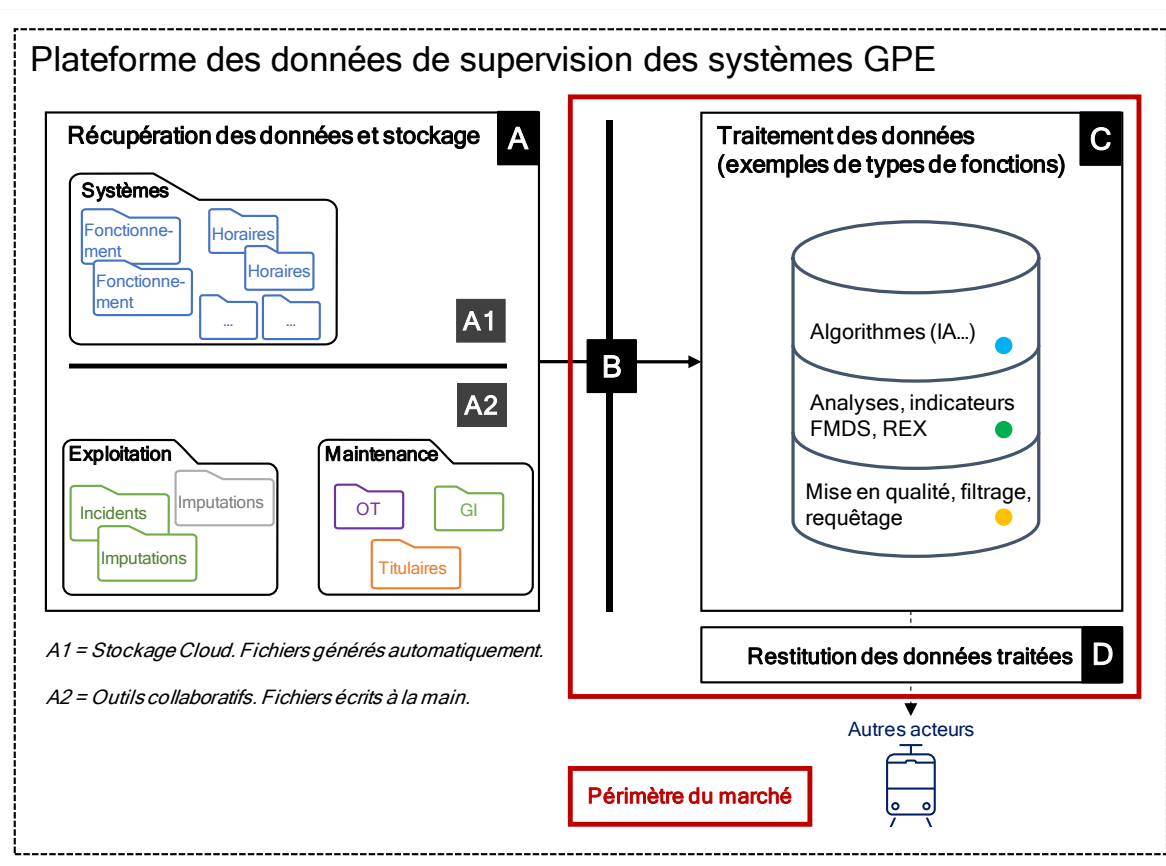


Figure 6 : Synoptique de la plateforme des données

2.6 Description des différentes « zones » de la plateforme des données

La plateforme de données de supervision des systèmes est composée de 4 zones distinctes désignées A, B, C et D. Cette décomposition représentée dans le synoptique ci-dessus permet de modulariser les fonctions que la plateforme de données de supervision des systèmes devra remplir. Chaque zone assurant un rôle fonctionnel précis détaillé ci-dessous.

2.6.1 Zone A – Stockage

Un espace sécurisé composé de deux sous-zones distinctes : A1 et A2

- A1 - Stockage des données de supervision issues des systèmes du Grand Paris Express

A1 est une zone de stockage cloud de type 3DS Outscale, Infrastructure as a Service (IaaS). Elle porte les données de supervision des systèmes. Ces données seront considérées comme fiables.

Cette zone est compartimentée par unité d'exploitation (L15, L16/17 et L18).

Ces données sont issues des commandes centralisées.

- A2 - Stockage des données d'exploitation et de maintenance

A2 est une zone basée sur une solution SharePoint et collectant les données d'exploitation et de maintenance.

A2 porte les informations issues des opérations de maintenance, des incidents d'exploitation et des imputations.

2.6.2 Zone B - Interfaces

La zone B doit permettre l'interface entre les différents espaces de stockage et l'espace de traitement. Cette zone est susceptible d'accueillir un ensemble de services qui permettront l'ingestion et la transformation des différentes données (intégration en lots, virtualisation des données, structuration des données etc.).

Cette fonction est incluse dans le présent marché.

2.6.3 Zone C - Zone de traitement

La zone C doit permettre de déployer les cas d'usage de la SGP afin d'atteindre les objectifs attendus par la solution.

2.6.4 Zone D - Restitution des données à la SGP et aux autres acteurs

La restitution doit permettre la mise à disposition à la SGP et à d'autres acteurs, des données selon différents critères (fichiers bruts, agrégés, après traitement...) en garantissant notamment la sécurité et la confidentialité entre les acteurs.

2.7 Périmètre du marché

Le présent marché porte les zones B, C et D à l'échelle du Grand Paris Express, pour l'ensemble des fichiers de données mis à disposition.

2.8 Description des données

2.8.1 Données de supervision des systèmes

Les données de supervision des systèmes se présentent sous format de fichiers plats type .csv, .json, .xml. Ces fichiers seront mis à disposition pour chaque unité d'exploitation (L15, L16-17, L18).

Deux typologies de fichiers seront mises à disposition : un même type pour les unités d'exploitation 15 et 16/17 et un autre type pour la ligne 18.

Chaque fichier est susceptible de représenter plusieurs dizaines voire centaines de giga-octets par jour. Toutefois, le volume initial sera faible (quelques dizaines de giga-octets) et évoluera en fonction des mises en service et des prolongements des lignes.

Les données étant fournies directement par les systèmes de commandes centralisées, elles seront définies par des exigences et leur format sera fixe. Les questions de qualité des données de supervision sont donc a priori à exclure.

La source de données pourra être indisponible au plus une journée.

Les données de supervision des systèmes regroupent les informations suivantes :

- États fonctionnels ou techniques ;
- Évènements systèmes ;
- Informations sur les différents modes des équipements ;
- Commandes réalisées par les opérateurs et/ou les systèmes ;
- Retours d'information de prise en compte des commandes ;
- Alarmes remontées par les systèmes et leur traitement (début, fin, acquittement) ;
- Mises à niveau des équipements supervisés (ex : changements de version).

Les données de supervision sont récupérées à intervalles réguliers : entre 15 minutes et toutes les 24 heures. Ce délai reste à préciser dans le cadre des études d'interfaces avec le système de commandes centralisées et peut varier entre les différentes unités d'exploitation. La récupération des données en temps réel n'est en aucun cas envisagée pour la réalisation de la plateforme.

2.8.2 Données d'exploitation et de maintenance

Les données d'exploitation sont des transmis par les différents partenaires de la SGP. Ces données se présentent sous forme de fichier .csv, .xls ou .json Ces fichiers sont déposés à des fréquences variables et non déterminées.

Certains champs sont déterminés par les outils des exploitants/mainteneurs mais d'autres sont des champs libres renseignés par les agents.

Les données d'exploitation et de maintenance regroupent les informations suivantes :

- Signalements¹ imputés aux systèmes pour lesquels la SGP porte une responsabilité (par exemple : garanties) ;
- Données de maintenance :
 - Description du constat par le mainteneur
 - Actions réalisées par le mainteneur
 - Durée d'intervention...
- Liste des incidents imputables aux industriels, titulaires des marchés systèmes de la SGP ;
- Données d'exploitations ;
- Informations de supervision y compris les informations pour la maintenance ;
- Informations sur les différents modes des équipements ;
- Commandes réalisées par les opérateurs de/ou les systèmes ;
- Retours d'information de prise en compte des commandes ;
- Alarmes remontées par les systèmes et leur traitement (début, fin, acquittement) ;
- Mises à niveau des équipements supervisés (ex : changements de version).

Les informations concernant la maintenance portent sur la maintenance corrective et, le cas échéant, sur la maintenance préventive.

2.8.3 Données d'entrée

Pour la réalisation de la plateforme des données de supervision, la SGP met à disposition les données d'entrée suivantes :

- Une description des fichiers de données correspondant aux unités d'exploitation ligne 15 et 16/17 ;
- Une description des fichiers de données correspondant à l'unité d'exploitation ligne 18 ;
- Le référentiel technique des données du GPE ;
- Une description des fichiers de données issus des systèmes de GMAO des Opérateurs de Transport et Gestionnaire d'Infrastructure ;
- Exemple d'un fichier de IoTList contenant les variables systèmes/Dictionnaire des données systèmes ;
- Une description des processus FMD, VSR, GPA, FRACAS et CTEVP : cf. Annexe 2 - PN2030-1_06_HPH_NOT_000027_3.

¹ Un signalement correspond à un dysfonctionnement nécessitant l'intervention d'un opérateur afin de corriger ce dysfonctionnement

2.9 Outils en interface avec le projet

2.9.1 Zone de stockage « Outscale »

Les données brutes de supervision des systèmes seront stockées sous format objet dans le cloud Outscale. Il y aura trois espaces : un par unité d'exploitation (ligne 15, lignes 16/17, ligne 18). Le lien entre cet espace Outscale et le GPE est hors du périmètre du présent marché.

Le lien entre cet espace Outscale et la plateforme des données de supervision fait partie du périmètre de responsabilité du présent marché.

2.9.2 Sharepoint

Les informations de maintenance et d'indicateur d'exploitation sont disponibles dans différents dossiers Sharepoint en respect des règles de secret industriel.

2.9.3 Active Directory SGP

Sur demande de la SGP, le Titulaire met en place un système de contrôle de gestion des identités et des accès (IAM), afin de donner aux utilisateurs en fonction des rôles, la possibilité d'accéder aux différents composants/ressources de la plateforme de données de supervision.

2.9.4 Utilisation de la GED SGP

La SGP dispose d'un outil de gestion documentaire (GED). Le Titulaire dispose d'accès à l'outil et doit y déposer les différentes documentations du projet, en particulier la documentation technique et fonctionnelle.

3 DESCRIPTION DES PRESTATIONS

3.1 Prescriptions applicables à l'ensemble des prestations

[EXI:PDS_GPE_3-001]

L'ensemble des livrables doivent être en langue française, y compris les commentaires du code source. Le code source est à documenter en français et pourra faire l'objet d'un audit externe pour vérifier la qualité de la documentation.

[FIN]

[EXI:PDS_GPE3-002]

Pour chacune des unités d'œuvre (UO) décrites ci-après, le Titulaire doit proposer une liste de livrables associés à la bonne réalisation de la prestation. La liste ci-dessous peut être prise en considération à titre d'information et en complément des livrables listés dans le descriptif de chacune des prestations au sein des paragraphes suivants.

L'ensemble des jalons et délais associés aux différentes prestations sont listés dans l'annexe 4 du programme fonctionnel.

Activités	Livrables
Cadrage	<ul style="list-style-type: none"> • Rapport d'Évaluation des Besoins • Spécifications fonctionnelles • Spécifications techniques • Diagrammes d'architecture • Description des composants • Diagrammes de flux de données • Spécifications de transformation des données • Plan de gestion des données • Document de plan de test
Développement	<ul style="list-style-type: none"> • Code source et documentation des modules de base • Rapport de conception des modules • Guide d'installation et de configuration • Manuels de développement • Journal des modifications • Maquettes et prototypes d'interfaces • Spécifications des processus ETL • Scripts ETL • Journal des processus ETL • Rapport de performance des ETL • Plan d'Archivage des Données • Politique d'Archivage • Rapports de Conformité • Documentation des Accès aux Archives <p>Modules fonctionnels :</p> <ul style="list-style-type: none"> • Code source documenté <p>Interfaces utilisateurs :</p> <ul style="list-style-type: none"> • Maquettes et prototypes d'interfaces

Activités	Livrables
	<ul style="list-style-type: none"> Code source et documentation des interfaces
Intégration	<ul style="list-style-type: none"> Spécifications techniques des connecteurs Code source des connecteurs Guide d'installation et de configuration Version finale de l'architecture validée
Tests et validation	<p>Tests unitaires :</p> <ul style="list-style-type: none"> Scripts de tests unitaires Rapports de tests unitaires <p>Tests d'intégration :</p> <ul style="list-style-type: none"> Scripts de tests d'intégration Rapports de tests d'intégration <p>Tests de performance :</p> <ul style="list-style-type: none"> Scripts de tests de performance Rapports de tests de performance Recommandations d'optimisation <p>Cloud :</p> <ul style="list-style-type: none"> Suivi de la consommation cloud
Documentation	<ul style="list-style-type: none"> - Manuel d'installation <ul style="list-style-type: none"> - Guide de configuration - Guide d'administration - Documentation de sauvegarde et de restauration - Checklist de vérification post-installation - Journal des modifications <ul style="list-style-type: none"> - Guide de maintenance logiciel - Base de données des anomalies - Documentation des actions correctives - Guide d'utilisateur - Dossier d'architecture technique - Dossier d'architecture fonctionnelle - Documentation technique ou fonctionnelle - Documentation relative aux nouveaux environnements

[FIN]

3.2 Infrastructure, logiciels et maintenance associée

3.2.1 UO I1 - Fourniture de l'infrastructure logicielle

[EXI:PDS_GPE_I1-001]

Objectif : Doter la plateforme de données des ressources matérielles/logicielles nécessaires pour son bon fonctionnement. Cela comprend l'acquisition de logiciels y compris le stockage, et de solutions de réseau, en veillant à ce qu'ils répondent aux critères de performance, de sécurité et de scalabilité définis par la SGP (voir également §4 - Infrastructure et suite logicielle).

[FIN]

[EXI:PDS_GPE_I1-002]

Cadrage : Définir les spécifications techniques et les besoins en infrastructure, incluant les exigences en termes de capacité, de performance, de sécurité et de compatibilité. Évaluer les contraintes budgétaires et élaborer des critères de sélection pour les fournisseurs.

[FIN]

[EXI:PDS_GPE_I1-003]

Achat : Procéder à la sélection et à l'acquisition des composants auprès de fournisseurs identifiés en ayant l'assurance de la conformité des produits livrés aux spécifications requises.

[FIN]

[EXI:PDS_GPE_I1-004]

Installation : Assurer la mise en place et la configuration de l'infrastructure achetée. Vérifier que l'infrastructure est opérationnelle et conforme aux exigences de la SGP, en procédant aux tests nécessaires pour garantir son bon fonctionnement.

[FIN]

3.2.2 UO I2 - Installation et configuration des logiciels

[EXI:PDS_GPE_I2-001]

Objectif : L'objectif est de garantir l'installation et la configuration optimales des logiciels et/ou composants sur l'infrastructure de la plateforme de données de la SGP. Le Titulaire doit s'assurer que les logiciels sont correctement déployés, configurés pour répondre aux exigences spécifiques de la SGP, et documentés pour faciliter leur gestion et maintenance futures.

[FIN]

[EXI:PDS_GPE_I2-002]

Installation : Installer les logiciels sur les serveurs et les postes de travail désignés, en suivant les procédures standardisées pour garantir une installation conforme aux exigences définies par la SGP. Cela inclut la vérification des prérequis matériels et logiciels, la gestion des dépendances, et la validation de l'installation initiale.

[FIN]

[EXI:PDS_GPE_I2-003]

Configuration : Configurer les logiciels installés selon les spécifications techniques et fonctionnelles de la SGP. Cette étape comprend le paramétrage des options de sécurité, l'intégration avec les systèmes existants, et l'ajustement des paramètres de performance pour optimiser l'utilisation des ressources.

[FIN]

[EXI:PDS_GPE_I2-004]

Documentation : Produire une documentation complète et détaillée des processus d'installation et de configuration. Cela inclut des guides d'installation, des manuels de configuration, des procédures de sauvegarde et de restauration, et des consignes de dépannage.

[FIN]

3.2.3 UO I3 - Audit et conformité des logiciels

[EXI:PDS_GPE_I3-001]

Objectif : Le Titulaire doit assurer que les logiciels utilisés par la SGP sont conformes aux normes, aux politiques internes, et aux réglementations en vigueur. Le Titulaire doit également assurer l'optimisation de l'utilisation des logiciels pour maximiser l'efficacité des ressources logicielles.

[FIN]

[EXI:PDS_GPE_I3-002]

Évaluation de la conformité : Vérifier que tous les logiciels déployés respectent les exigences légales, les normes de sécurité, et les politiques internes de la SGP. Cela inclut la vérification des licences, l'évaluation des risques de non-conformité, et la validation des configurations de sécurité pour s'assurer que les logiciels répondent aux exigences de la SGP.

[FIN]

[EXI:PDS_GPE_I3-003]

Optimisation des licences : Analyser l'utilisation des licences logicielles pour identifier les excédents, les insuffisances ou les abus potentiels. Optimiser l'allocation des licences en fonction des besoins réels, en réduisant les coûts.

[FIN]

[EXI:PDS_GPE_I3-004]

Audit et recommandations : Le Titulaire doit réaliser des rapports détaillant les résultats de l'audit de conformité, incluant les éventuelles non-conformités détectées, les risques associés et les recommandations pour corriger les anomalies. Le rapport doit également fournir des conseils pour l'amélioration continue de la gestion des logiciels, incluant des stratégies de mise à jour et de migration pour rester à jour avec les réglementations et les meilleures pratiques technologiques.

[FIN]

3.2.4 UO I4 - Mise à jour et évolution des logiciels

Voir paragraphes 5.1 - Maintenance corrective, mise à jour et évolution des logiciels et 5.2 - SLA

3.2.5 UO I5 - Sécurité et sauvegarde des données

Voir paragraphes 5.3 - Sécurité et sauvegarde des données, 4.3.1 - Sécurité des prestations et 4.3.4 - Sauvegardes

3.2.6 UO I6 - Gestion des utilisateurs et des accès

Voir paragraphe 5.4 - Gestion des utilisateurs et des accès

3.2.7 UO I7 - Suivi financier de la consommation du cloud

Voir paragraphe 5.5 - Suivi financier de la consommation du cloud

3.3 Accompagnement métier et développements

3.3.1 UO D1 - Définition de l'architecture de la plateforme de données

[EXI:PDS_GPE_D1-001]

Objectif : Il s'agit de concevoir et formaliser une architecture robuste et évolutive pour la mise en œuvre de la plateforme des données de la SGP. Cette architecture doit satisfaire les besoins métiers, garantir l'intégrité et la sécurité des données, et permettre une intégration fluide avec les systèmes existants et futurs.

[FIN]

[EXI:PDS_GPE_D1-002]

Cadrage : Le Titulaire doit élaborer une architecture qui soutienne efficacement les cas d'usage métier identifiés, tout en restant adaptable à l'évolution des exigences et des technologies. Cette architecture inclura des mesures de sécurité rigoureuses telles que le chiffrement, les contrôles d'accès et les audits pour protéger les données sensibles (respect du secret industriel). L'architecture doit également inclure des mécanismes de scalabilité pour gérer l'augmentation des volumes de données et des utilisateurs.

[FIN]

[EXI:PDS_GPE_D1-003]

Conception : Le Titulaire est responsable de la production de documents techniques détaillés, incluant des diagrammes d'architecture, des descriptions des flux de données, et des spécifications techniques pour chaque composant. Ces documents serviront de référence pour les équipes de développement et d'exploitation, assurant une compréhension commune et une mise en œuvre cohérente des solutions.

[FIN]

[EXI:PDS_GPE_D1-004]

Validation finale : Organisation de sessions de validation avec les parties prenantes pour obtenir leur approbation.

[FIN]

Nota : se référer également aux exigences techniques, en particulier au paragraphe 4.2.1.1 Architecture.

3.3.2 UO D2 - Développement et intégration des modules de base

[EXI:PDS_GPE_D2-001]

Objectif : Cette prestation confie au Titulaire la responsabilité de concevoir, développer, intégrer et valider les composants essentiels de la plateforme de données.

[FIN]

[EXI:PDS_GPE_D2-002]

Développement : La phase de développement concerne la création des différents modules fondamentaux de la plateforme de données. Ces modules doivent être conçus de manière à être réutilisables, évolutifs, et capables de supporter la création future de cas d'usage spécifiques. Le Titulaire doit développer les modules de base nécessaires, tels que les systèmes de gestion des données, les pipelines, et les interfaces, en respectant les spécifications techniques et

fonctionnelles. Il est également chargé de produire la documentation du code et des processus associés pour garantir une maintenance future efficace.

[FIN]

[EXI:PDS_GPE_D2-003]

Intégration : Le Titulaire intégrera ces modules développés en veillant à leur compatibilité avec les autres systèmes et services. Cette activité inclut la configuration des environnements, la mise en place des connecteurs nécessaires pour l'interopérabilité et la gestion des dépendances entre les composants.

[FIN]

[EXI:PDS_GPE_D2-004]

Tests/Validation : Le Titulaire est responsable de réaliser une série de tests, incluant des tests unitaires, d'intégration et de performance, pour s'assurer du bon fonctionnement et de l'optimisation des modules. Les résultats des tests devront être documentés, et les corrections nécessaires apportées pour résoudre les problèmes détectés. Cette unité d'œuvre assure ainsi que le Titulaire livre une infrastructure de données solide et fiable, apte à supporter les opérations et analyses de données de la SGP.

[FIN]

3.3.3 UO D3 - Requêtes sur critères

[EXI:PDS_GPE_D3-001]

Objectif : Permet l'exploration et l'analyse des données stockées en fonction de critères géographiques, d'équipements, temporels, et des variables présentes dans les données d'entrée.

Le Titulaire doit mettre en place un outil permettant à des acteurs de pouvoir réaliser des requêtes permettant d'obtenir des jeux de données selon des critères prédéfinis :

- Géographique (ligne, station, interstation...)
- Type d'équipement (porte palière, ventilateur, ascenseur)
- Numéro de l'équipement (ascenseur n°3, caméra vidéo 24...)
- Temporel (année, mois, jour, heure, minute, seconde)
- État fonctionnel (porte ouverte, fermé, alarme, sens de l'ascenseur, état de marche, commande passée par l'opérateur...)

Les critères se baseront sur une base de données maitre à réaliser en amont de cette prestation :
cf. 3.3.4 UO_D4 - Mise en place d'un outil de gestion des données .

[FIN]

[EXI:PDS_GPE_D3-002]

Cadrage : Le Titulaire doit d'abord définir les besoins en matière de requêtes, en collaboration avec les parties prenantes, et concevoir l'architecture des requêtes et les cas d'utilisation associés.
[FIN]

[EXI:PDS_GPE_D3-003]

Développement : Le Titulaire est responsable du développement des modules fonctionnels nécessaires pour effectuer ces requêtes, incluant la création d'algorithmes de filtrage et de tri.
[FIN]

[EXI:PDS_GPE_D3-004]

Intégration : Ensuite, il intègre ces modules dans l'infrastructure existante, en veillant à ce qu'ils soient compatibles avec les bases de données actuelles et les systèmes d'analyse de données.
[FIN]

[EXI:PDS_GPE_D3-005]

Tests/Validation : Enfin, le Titulaire effectue des tests pour valider le bon fonctionnement des requêtes selon les critères définis en documentant les résultats pour assurer une utilisation optimale par les utilisateurs finaux.
[FIN]

[EXI:PDS_GPE_D3-006]

Pour mettre en œuvre cette prestation, le Titulaire doit réaliser au minimum toutes les activités et livrables cités ci-dessous :

Activités	Livrables
Cadrage	<ul style="list-style-type: none"> • Dossier de cas d'usage • Définition de l'architecture du cas d'usage
Développement	<p>Modules fonctionnels :</p> <ul style="list-style-type: none"> • Code source • Documentation • Rapport de conception des modules • Guide d'installation et de configuration • Manuels de développement • Journal des modifications <p>Interfaces utilisateurs :</p> <ul style="list-style-type: none"> • Maquettes et prototypes d'interfaces • Code source et documentation des interfaces

	<ul style="list-style-type: none"> • Guide de style • Rapport d'ergonomie
Intégration	<p>Intégration générale :</p> <ul style="list-style-type: none"> • Rapport d'intégration <p>Transformation des données spécifiques :</p> <ul style="list-style-type: none"> • Spécifications des processus ETL • Scripts ETL • Journal des processus ETL • Rapport de performance des ETL
Tests et validation	<ul style="list-style-type: none"> • Document de plan de test <p>Tests unitaires :</p> <ul style="list-style-type: none"> • Scripts de tests unitaires • Rapports de tests unitaires <p>Tests d'intégration :</p> <ul style="list-style-type: none"> • Scripts de tests d'intégration • Rapports de tests d'intégration <p>Tests de performance :</p> <ul style="list-style-type: none"> • Scripts de tests de performance • Rapports de tests de performance • Recommandations d'optimisation <p>Cloud :</p> <ul style="list-style-type: none"> • Suivi de la consommation cloud <p>Documentation générale :</p> <ul style="list-style-type: none"> • Base de données des anomalies • Documentation des actions correctives

[FIN]

3.3.4 UO D4 - Mise en place d'un outil de gestion des données de référence

[EXI:PDS_GPE_D4-001]

Objectif : Créer une base de données centralisée et fiable, appelée base de données de référence, qui servira de source unique et cohérente pour l'ensemble des données de la plateforme. Cette base de données doit intégrer et harmoniser les données provenant de diverses sources internes et externes, tout en garantissant leur qualité, leur intégrité et leur sécurité. Elle est conçue pour être évolutive et flexible, permettant d'ajouter de nouvelles données et de répondre aux besoins changeants des utilisateurs.

[FIN]

[EXI:PDS_GPE_D4-002]

Le Titulaire doit ainsi construire un outil contenant l'ensemble des données maitres définissant l'infrastructure du GPE, ses différents systèmes et les codes et ID des statuts/commandes des systèmes à partir de la base documentaire de la SGP et en particulier de la liste des données référentielles du RTPGP (réf. : UMQO_02_HPH_DRF_000003).

[FIN]

[EXI:PDS_GPE_D4-003]

Dans ce cadre, le Titulaire s'appuie sur les livrables suivants, dont la liste peut être complétée par le Titulaire :

1. **Modèle de données de référence** : Schéma détaillé décrivant la structure des données, les relations entre les entités, et les attributs spécifiques inclus dans la base de données de référence.
2. **Guide de gouvernance des données** : Document détaillant les politiques de gestion des données, les processus de qualité des données, et les responsabilités pour maintenir l'intégrité des données.
3. **Manuel d'intégration des données** : Procédures et protocoles pour l'extraction, la transformation, et le chargement (ETL) des données dans la base de données de référence, incluant les règles de validation des données.
4. **Documentation de sécurité et conformité** : Ensemble de directives et de pratiques pour assurer la sécurité des données, y compris les contrôles d'accès, le chiffrement des données sensibles, et les mesures de conformité aux réglementations.
5. **Rapport de validation des données** : Résultats des tests de qualité des données, incluant les analyses de cohérence, de précision, et de complétude des données intégrées dans la base de données de référence.

[FIN]

3.3.5 UO D5 - Découpe de fichiers selon des critères géographiques et systèmes

[EXI:PDS_GPE_D5-001]

Objectif : Le but de cette prestation est de permettre la gestion et la transformation des fichiers d'entrée en fonction de critères spécifiques, tels que la géographie ou les systèmes. Le Titulaire

doit automatiser la création d'un fichier issu des données brutes selon des critères déterminés avec la SGP.

[FIN]

[EXI:PDS_GPE_D5-002]

Cadrage : Le Titulaire doit d'abord définir les critères de découpage en collaboration avec les parties prenantes, pour concevoir une règle de transformation des fichiers adaptée aux besoins.

[FIN]

[EXI:PDS_GPE_D5-003]

Développement : Ensuite, le Titulaire développera les scripts et les outils nécessaires pour automatiser le processus de découpage des fichiers, garantissant la transformation des données en fonction des critères définis.

[FIN]

[EXI:PDS_GPE_D5-004]

Intégration : Ces outils seront intégrés dans le système de gestion des fichiers existant afin d'assurer que les fichiers transformés soient accessibles facilement (interface adaptée).

[FIN]

[EXI:PDS_GPE_D5-005]

Tests/Validation : Le Titulaire doit tester les processus de découpage pour s'assurer de leur exactitude et de leur efficacité, en vérifiant que les fichiers transformés répondent aux spécifications et sont disponibles quotidiennement à 8h30 pour tous les acteurs concernés, tout en documentant les résultats pour une utilisation future.

[FIN]

[EXI:PDS_GPE_D5-006]

Pour mettre en œuvre cette prestation le Titulaire doit réaliser au minimum toutes les activités et livrables cités ci-dessous :

Activités	Livrables
Cadrage	<ul style="list-style-type: none"> Dossier de cas d'usage Définition de l'architecture du cas d'usage
Développement	Modules fonctionnels : <ul style="list-style-type: none"> Code source

Activités	Livrables
	<ul style="list-style-type: none"> • Documentation • Rapport de conception des modules • Guide d'installation et de configuration • Manuels de développement • Journal des modifications <p>Interfaces utilisateurs :</p> <ul style="list-style-type: none"> • Maquettes et prototypes d'interfaces • Code source et documentation des interfaces • Guide de style • Rapport d'ergonomie
Intégration	<p>Intégration générale :</p> <ul style="list-style-type: none"> • Rapport d'intégration <p>Transformation des données spécifiques :</p> <ul style="list-style-type: none"> • Spécifications des processus ETL • Scripts ETL • Journal des processus ETL • Rapport de performance des ETL
Tests et validation	<ul style="list-style-type: none"> • Document de plan de test <p>Tests unitaires :</p> <ul style="list-style-type: none"> • Scripts de tests unitaires • Rapports de tests unitaires <p>Tests d'intégration :</p> <ul style="list-style-type: none"> • Scripts de tests d'intégration • Rapports de tests d'intégration <p>Tests de performance :</p> <ul style="list-style-type: none"> • Scripts de tests de performance • Rapports de tests de performance • Recommandations d'optimisation <p>Cloud :</p> <ul style="list-style-type: none"> • Suivi de la consommation cloud • Documentation générale : • Base de données des anomalies • Documentation des actions correctives

Le Titulaire pourra être amené à réaliser cette UO plusieurs fois au cours du projet afin de répondre aux sollicitations des différents métiers de la SGP et responsabilité des acteurs.

[FIN]

3.3.6 UO D6 - Spécification et déploiement d'une solution basée sur du machine learning et/ou deep learning

[EXI:PDS_GPE_D6-001]

Objectif : L'objectif de cette prestation est d'utiliser des modèles d'intelligence artificielle pour analyser les données et déterminer des patterns à partir de signaux faibles non issus de la conception des systèmes.

[FIN]

[EXI:PDS_GPE_D6-002]

Cadrage : Le Titulaire commencera par identifier les objectifs d'analyse et les types de signaux faibles pertinents à détecter, en définissant les données d'entrée et les attentes des utilisateurs finaux.

[FIN]

[EXI:PDS_GPE_D6-003]

Développement : Le Titulaire développera et entraînera des modèles d'IA, tels que des algorithmes de machine learning ou de deep learning, pour analyser les grandes quantités de données et identifier les anomalies ou les tendances associées.

[FIN]

[EXI:PDS_GPE_D6-004]

Intégration : Les modèles d'IA seront intégrés dans l'infrastructure existante, avec des pipelines de données automatisés pour assurer une capacité d'analyse continue et en temps réel.

[FIN]

[EXI:PDS_GPE_D6-005]

Tests/Validation : Le Titulaire est chargé de tester les modèles pour évaluer leur précision et leur capacité à détecter efficacement les signaux faibles, en ajustant les paramètres des modèles si nécessaire. Les résultats des tests seront documentés et les modèles validés seront déployés.

[FIN]

[EXI:PDS_GPE_D6-006]

Pour mettre en œuvre cette prestation, le Titulaire doit réaliser les activités et livrables cités ci-dessous, dont la liste pourra être complétée par le Titulaire :

Activités	Livrables
Cadrage	<ul style="list-style-type: none"> • Dossier de cas d'usage / recueil de besoin • Choix du modèle d'IA / stratégie Make or Buy • Définition de l'architecture • Définition des flux de données
Développements	<p>Modules fonctionnels :</p> <ul style="list-style-type: none"> • Code source • Documentation • Rapport de conception des modules • Guide d'installation et de configuration • Manuels de développement • Journal des modifications <p>Interfaces utilisateurs :</p> <ul style="list-style-type: none"> • Maquettes et prototypes d'interfaces • Code source et documentation des interfaces • Guide de style • Rapport d'ergonomie

[FIN]

3.3.7 UO D7 - Accompagnement à l'analyse des défaillances

[EXI:PDS_GPE_D7-001]

Objectif : Mettre en place des outils visuels pour analyser et suivre les défaillances à travers des indicateurs clés de performance (KPI) pertinents, mais également de fournir une assistance experte pour analyser, interpréter et évaluer les données relatives aux défaillances remontées par le système, en s'appuyant sur les compétences métiers spécifiques.

[FIN]

[EXI:PDS_GPE_D7-002]

Le Titulaire est chargé de mobiliser ses ressources pour examiner les données de défaillance, et identifier les causes. L'objectif est de renforcer la capacité de la SGP à anticiper, comprendre et gérer les défaillances de manière proactive, en intégrant une perspective métier pour permettre une objectivité justifiée des défaillances.

[FIN]

2024DC001 – PROGRAMME FONCTIONNEL
CODE GED : DSTE_06_ACT_STE_002360_1

Ce document est la propriété de la Société des grands projets. Toute diffusion ou reproduction intégrale ou partielle est autorisée pour et dans la limite des besoins découlant des prestations ou missions du marché conclu avec le titulaire destinataire.

[EXI:PDS_GPE_D7-003]

Cadrage : Le Titulaire doit d'abord définir les besoins en matière de suivi des défaillances en collaboration avec la SGP, en identifiant les KPI à construire.

[FIN]

[EXI:PDS_GPE_D7-004]

Développement : Le Titulaire produira ensuite les tableaux de bord, intégrant des visualisations dynamiques et des filtres permettant une analyse détaillée des défaillances. Ces tableaux de bord s'appuieront sur les modules d'intelligence de la plateforme de données et devront être connectés aux sources de données intégrées dans la plateforme de données GPE.

[FIN]

[EXI:PDS_GPE_D7-005]

L'analyse de défaillances et la mise en place des KPIs associés sont différenciées en trois niveaux de complexité :

Type	Définition	Exemple
Simple	BDD disponible Information facilement trouvable Calcul basique	Dépassement de seuils Alerte intempestive
Intermédiaire	BDD disponible Nécessité de réflexion pour retrouver l'information voulue Calcul avec un peu de complexité	Corrélations entre données Détermination de pattern issu du fonctionnement de la conception système Recherche dans l'historique
Complexe	BDD à construire Expertise métier sollicité Recherche dans la documentation technique Calcul complexe à mettre en place	Analyse de signaux faibles Analyse proactive des défaillances

[FIN]

[EXI:PDS_GPE_D7-006]

En complément de la liste citée en amont, pour cette prestation, le Titulaire devra apporter les éléments suivants. Cette liste pourra être complétée par le Titulaire :

Activités	Livrables
Cadrage	<ul style="list-style-type: none">Définition de KPI pertinents
Analyse	<ul style="list-style-type: none">Rapport de Justification des DéfaillancesAnalyse des Causes Racines (RCA)

[FIN]

3.3.8 UO D8 - Mise à disposition des données pour d'autres acteurs via une interface web sécurisée

[EXI:PDS_GPE_D8-001]

Objectif : Cette prestation vise à permettre à la SGP de fournir des données et restituer les différents traitements et analyses issues de celles-ci de manière sécurisée et structurée à ses partenaires ou autres acteurs externes.

[FIN]

[EXI:PDS_GPE_D8-002]

Cadrage : Le Titulaire définit les types de données à partager, les critères de sélection, et les exigences légales et contractuelles, en collaboration avec les parties prenantes.

Les jeux de données doivent être mis à disposition automatiquement via une interface web sécurisée. Le choix de la méthode d'accès est fait en respect des règles de sécurité.

À ce stade, la SGP souhaite réaliser trois espaces imperméables entre eux. Chaque espace étant dédié à une unité d'exploitation :

- Ligne 15 ;
- Lignes 16/17 ;
- Ligne 18.

Ces jeux de données pourront être issus de la prestation « 3.3.5 UO_D5 - Découpe de fichiers selon des critères géographiques et systèmes ». Il sera ensuite possible de créer des accès dérivés avec des droits spécifiques pour garantir le secret industriel entre les acteurs.

Le Titulaire assure la mise en place de l'espace, la gestion des droits d'accès et la mise à disposition automatique de jeux données. Le Titulaire a uniquement la responsabilité de mettre à disposition les données et de maintenir les interfaces.

Actuellement, les acteurs identifiés devant obtenir un accès aux données via cet espace sont :

- Ile-de-France Mobilités ;
- Les opérateurs de transports (1 entité par unité d'exploitation) ;
- RATP Infrastructures ;
- Les Titulaires des marchés systèmes de la SGP en phase de garantie.

[FIN]

[EXI:PDS_GPE_D8-003]

Développement : le Titulaire développe les interfaces nécessaires pour l'accès aux données, en garantissant la structuration appropriée des données et l'application des politiques de gouvernance des données, incluant les règles de qualité et le respect du secret industriel.

[FIN]

[EXI:PDS_GPE_D8-004]

Tests/Validation : le Titulaire procède à des tests de sécurité et de fonctionnalité pour s'assurer que les données sont transmises de manière sécurisée et que les partenaires peuvent accéder aux données. Les résultats seront documentés, et les ajustements nécessaires seront effectués.

[FIN]

[EXI:PDS_GPE_D8-005]

Pour mettre en œuvre cette prestation, le Titulaire s'appuie sur les activités et livrables ci-dessous, dont la liste peut être complétée par le Titulaire :

Activités	Livrables
Cadrage	<ul style="list-style-type: none"> • Catalogue de données à jour • Plan de Mise à Disposition des Données • Plan de Continuité de Service • Plan de Scalabilité • Étude de Capacité • Procédures de Mise à Échelle
Développement	Modules fonctionnels : <ul style="list-style-type: none"> • Code source

	<ul style="list-style-type: none"> • Documentation • Rapport de conception des modules • Guide d'installation et de configuration • Manuels de développement • Journal des modifications <p>Interfaces utilisateurs :</p> <ul style="list-style-type: none"> • Maquettes et prototypes d'interfaces • Code source et documentation des interfaces • Guide de style • Rapport d'ergonomie
Intégration	<p>Connecteurs :</p> <ul style="list-style-type: none"> • Spécifications techniques des connecteurs • Code source des connecteurs • Guide d'installation et de configuration
Tests et validation	<ul style="list-style-type: none"> • Document de plan de test <p>Tests unitaires :</p> <ul style="list-style-type: none"> • Scripts de tests unitaires • Rapports de tests unitaires <p>Tests d'intégration :</p> <ul style="list-style-type: none"> • Scripts de tests d'intégration • Rapports de tests d'intégration <p>Tests de performance :</p> <ul style="list-style-type: none"> • Scripts de tests de performance • Rapports de tests de performance • Recommandations d'optimisation <p>Cloud :</p> <ul style="list-style-type: none"> • Suivi de la consommation cloud • Documentation générale : • Base de données des anomalies • Documentation des actions correctives

[FIN]

3.3.9 UO D9 - Formation et conduite du changement

[EXI:PDS_GPE_D9-001]

Objectif : Élaborer et mettre en œuvre la stratégie d'accompagnement pour aider les utilisateurs à prendre en main efficacement la plateforme de données et les fonctionnalités associées.

[FIN]

[EXI:PDS_GPE_D9-002]

Cadrage de la conduite du changement : Le Titulaire débute par l'analyse des impacts du changement, en identifiant les utilisateurs concernés et les compétences nécessaires. Il élabore une stratégie globale incluant les objectifs, les messages clés, les canaux de communication et le calendrier des formations.

[FIN]

[EXI:PDS_GPE_D9-003]

Animation de formations : Le Titulaire est chargé de concevoir et d'animer des sessions de formation adaptées aux différents profils d'utilisateurs. Cela comprend des sessions en présentiel, des webinaires interactifs et des ateliers pratiques, visant à familiariser les utilisateurs avec les nouvelles fonctionnalités.

[FIN]

[EXI:PDS_GPE_D9-004]

Production de documents de formation : Le Titulaire produit une variété de supports pédagogiques, incluant des manuels d'utilisateur, des tutoriels... Ces documents sont conçus pour être clairs et accessibles, couvrant l'ensemble des fonctionnalités de la plateforme de données. Ils sont mis à disposition sur une plateforme en ligne, permettant un accès facile et continu pour tous les utilisateurs.

Activités	Livrables
Cadrage	<ul style="list-style-type: none"> Plan d'accompagnement au changement Programme de formation
Animation de formation	<ul style="list-style-type: none"> Sessions de formation Webinaires et sessions de Q&A Ateliers pratiques
Production de documents de formation	<ul style="list-style-type: none"> Matériels de sensibilisation

	<ul style="list-style-type: none"> • Manuels de formation • Guides de démarrage rapides • Tutoriels en ligne • FAQ et feuilles de référence • Guides et manuels
--	--

[FIN]

3.3.10 UO D10 - POC - preuve de concept

[EXI:PDS_GPE_D10-001]

Le Titulaire est en mesure d'étudier la faisabilité et d'organiser la mise en œuvre d'une Proof Of Concept (POC) sur une thématique ou technologie donnée. Une POC a pour vocation d'évaluer la faisabilité d'un procédé, d'une innovation ou d'un modèle économique. Le Titulaire est force de proposition ; il étudie la faisabilité de la POC et rédige ses spécifications en vue d'une éventuelle mise en œuvre.

[FIN]

[EXI:PDS_GPE_D10-002]

Si la SGP estime l'opportunité intéressante, elle peut éventuellement demander au Titulaire de procéder au suivi de la mise en œuvre de la POC. La prestation inclut le contrôle et le reporting relatif aux phases de suivi.

[FIN]

[EXI:PDS_GPE_D10-003]

Livrables envisagés :

- Étude de faisabilité de la POC ;
- Spécifications de la POC ;
- Rapport d'avancement du suivi de la réalisation et de la mise en œuvre de la POC.

[FIN]

[EXI:PDS_GPE_D10-004]

En complément de cette liste prévue pour la prestation, le Titulaire doit apporter les éléments suivants. Cette liste pourra être complétée par le Titulaire

Activités	Livrables
Cadrage	<ul style="list-style-type: none"> • Spécifications fonctionnelles et techniques • Proposition d'architecture

	<ul style="list-style-type: none"> • Estimation de la solution à déployer • Synthèse des risques • Planning provisoire
--	---

[FIN]

3.3.11 UO D11 - Réversibilité

3.3.11.1 Objectifs

[EXI:PDS_GPE_D11-001]

La réversibilité consiste à prendre des précautions particulières de sauvegarde et de transfert de connaissances pour assurer, à la demande de la SGP, la reprise des prestations par la SGP ou par un tiers, et ce dans les meilleures conditions et sans discontinuité du service.

[FIN]

[EXI:PDS_GPE_D11-002]

La prestation de réversibilité est réalisée en fin de marché ou à tout moment souhaité par la SGP. Cette prestation est le pendant de la prise de connaissance.

Cette phase est menée en accompagnement d'une phase prise de connaissance par la SGP ou par le titulaire garant de la reprise du périmètre sur lequel porte la réversibilité. Il s'agira de restituer, par un processus de réversibilité, la connaissance acquise par l'équipe du Titulaire vers la SGP ou un tiers habilité par la SGP, à la fin d'un bon de commande ou du marché subséquent.

[FIN]

3.3.11.2 Description des prestations attendues

[EXI:PDS_GPE_D11-003]

Il s'agit d'une prestation à bon de commande effectuée parallèlement aux autres prestations du présent marché. La prestation de réversibilité débute par la réception du bon de commande émis par la SGP. Elle s'exécute conformément au Plan de Réversibilité.

La prestation de réversibilité inclut :

- Le transfert de connaissances de l'équipe de maintenance du Titulaire vers l'équipe du nouveau Titulaire ou vers la SGP sur l'ensemble des fonctionnalités mises en œuvre à la SGP à la date de la réversibilité ;
- La fourniture de l'ensemble de la documentation mise à jour ;

- La réalisation en « tandem » (nouveau et ancien Titulaire) de la maintenance corrective et du support ;
- La réversibilité des normes, procédures et règles en vigueur à la SGP ;
- La préparation de la réversibilité de l'ensemble des activités, la gestion en doublon et le transfert de responsabilité vers la SGP ou un tiers désigné par celle-ci.

[FIN]

[EXI:PDS_GPE_D11-004]

Le processus de réversibilité intègre la formation technique et fonctionnelle de la nouvelle équipe désignée par la SGP durant toute la période nécessaire pour parvenir au bon accomplissement de cette prestation.

[FIN]

[EXI:PDS_GPE_D11-005]

Durant cette période, et quelle que soit la dégressivité de la prestation, les responsabilités du Titulaire restent engagées. Il est attendu dans l'offre technique un plan de réversibilité présentant, a minima :

- La formation de la nouvelle équipe désignée par la SGP ;
- Les modalités de recouvrement des équipes du Titulaire du présent marché avec la nouvelle équipe désignée par la SGP (activités dégressives des équipes du Titulaire et assistance à la nouvelle équipe dans ses nouvelles tâches) ;
- Les moyens humains mis en œuvre ;
- Les livrables (tout au long du marché et lors de l'engagement de la phase de réversibilité).

[FIN]

[EXI:PDS_GPE_D11-006]

La qualité de la prestation de réversibilité est largement conditionnée par la qualité de la formation et du soutien apporté par le Titulaire durant cette période à l'équipe désignée par la DSI. Elle dépendra également de la lisibilité et du caractère opérationnel de la réversibilité.

[FIN]

[EXI:PDS_GPE_D11-007]

Tant que les critères d'acceptation ne seront pas satisfaits, la phase de réversibilité se prolongera aux frais du Titulaire. Au constat qu'ils sont satisfaits, la phase de réversibilité est qualifiée comme concluante.

[FIN]

[EXI:PDS_GPE_D11-008]

Il est attendu un plan de réversibilité dès le lancement du marché. Il devra être actualisé une fois par an dès le premier anniversaire d'exécution du présent marché.

La documentation du plan de réversibilité et ses mises à jour annuelles sont à la charge du Titulaire.

[FIN]

[EXI:PDS_GPE_D11-009]

En amont de la phase de réversibilité, le Titulaire procédera à une phase de préparation portant sur l'organisation de la réversibilité, incluant *a minima* les activités suivantes :

- La définition des procédures de restitution et du contenu des livrables ;
- La préparation et la construction du planning en concertation avec la DSI et/ou le fournisseur reprenneur du service ;
- La définition des compétences minimales pour assurer la continuité de service ;
- Le pilotage du déroulement de la phase.

[FIN]

3.3.11.3 Livrables

Livrables attendus	Délai maximal de remise
Plan de réversibilité initial	1 mois après la réception du bon de commande
Document de transfert de connaissances	2 semaines avant le début de la phase de réversibilité
Documentation complète des systèmes et processus	1 mois après la réception du bon de commande
Rapport de doublon de maintenance	Hebdomadaire pendant toute la phase de réversibilité
Guide des normes, procédures et règles en vigueur	1 mois après la réception du bon de commande
Rapport de formation de la nouvelle équipe	1 semaine après chaque session de formation
Planning détaillé de la réversibilité	2 semaines avant le début de la phase de réversibilité
Rapport de gestion en tandem	Mensuel pendant toute la phase de réversibilité

Liste des compétences minimales requises	3 semaines après la réception du bon de commande
Rapport final de réversibilité	2 semaines après la fin de la phase de réversibilité

3.3.12 UO D12 - Maintenance évolutive

[EXI:PDS_GPE_D12-001]

Objectif : La maintenance évolutive a pour but d'adapter et d'améliorer continuellement les systèmes informatiques pour répondre aux besoins d'évolutions émis par les utilisateurs et aux évolutions technologiques. Elle vise à introduire de nouvelles fonctionnalités, à optimiser les performances, à améliorer la sécurité, et à prolonger la durée de vie des systèmes et donc plus largement de la plateforme de données. L'objectif est de maintenir l'infrastructure à jour, compétitive, et alignée avec les exigences métier, techniques et organisationnelles de la SGP.

[FIN]

[EXI:PDS_GPE_D12-002]

Les activités à réaliser dans le cadre de la maintenance évolutive sont listées ci-dessous et sont découpées selon trois niveaux de complexité décrits ci-dessous. Le Titulaire doit déployer des évolutions spécifiées par la SGP en cours de projet.

[FIN]

[EXI:PDS_GPE_D12-003]

Les livrables attendus en fonction de niveaux d'évolutions à effectuer sont les suivants :

Type d'évolution	Définition	Exemple	Livrables
Simple	<ul style="list-style-type: none"> - Expression de besoin ne nécessitant pas d'expertise métier - Peu de risque de régression - Peu de tests nécessaires 	Modification de texte dans un formulaire Ajout de graphique simple ou modification d'un format de tableau	Code source Rapport de tests
Moyenne	<ul style="list-style-type: none"> -Expertises métier sollicitées sur l'expression de besoin initial (1h à 4h) - Test d'intégration - Plusieurs composants 	Mise en place d'une IHM Mise en place d'une API prédéfini	Spécifications fonctionnelles et techniques Code source Documentation Rapport de tests

	impactés - Risque modéré à définir en amont		
Complexe	-Besoin d'atelier(s) avec experts métier (>4h) -Nombreux composants du système impacté - Suivi post implémentation de la performance pour garantir la stabilité du système - Planification détaillée avec gestion de risque dédiée	Modification de la structure de la base de données Introduction de nouvelles infrastructure	Spécifications fonctionnelles et techniques Plan de tests Rapports de tests Code source Plan de déploiement Rapport de déploiement Si nécessaire, support de formation Matrice de risque Planning

[FIN]

[EXI:PDS_GPE_D12-004]

Chaque demande de maintenance évolutive fera l'objet d'une demande de la SGP formalisée le cas échéant au travers d'un outil mis à disposition par le Titulaire.

[FIN]

3.3.13 UO D13 - Support utilisateur et assistance technique

Voir paragraphe 5.6 - Support utilisateur et assistance technique

3.3.14 UO D14 - Monitoring de la plateforme de données

Voir paragraphe 5.7 - Monitoring de la plateforme de données

3.4 Prestations complémentaires sur devis

Dans le cadre du marché, le Titulaire pourra être amené à réaliser des missions complémentaires spécifiques restant en lien avec l'objet du marché.

Ces prestations complémentaires sont déclenchées par bon de commande. Chaque bon de commande précise les objectifs, le contenu de la prestation, les moyens déployés et les délais de réalisation via un planning. Elles peuvent être engagées en « jours », sur devis préalable, en

fonction du ou des profils nécessaires pour la réalisation de celles-ci et sur la base des prix renseignés dans le bordereau des prix unitaires.

La proposition de chiffrage est transmise deux (2) jours ouvrés après la demande la SGP. La SGP dispose de cinq (5) jours ouvrés pour répondre au Titulaire sur la commande de la prestation.

4 INFRASTRUCTURE ET SUITE LOGICIELLE

4.1 Exigences générales

La SGP attire l'intention du Titulaire sur l'importance accordée à la mise en place de services d'administration, d'exploitation et de support associés aux outils de la suite logicielle cloud proposée par Microsoft. Ce choix est motivé par la cohérence et l'importance accordée à l'infrastructure déjà existante et des objectifs à long terme de la SGP en matière de transformation numérique.

Néanmoins, le Titulaire a la possibilité de présenter des propositions alternatives qui pourraient tout autant répondre aux exigences du projet. Celles-ci seront évaluées de manière objective, en prenant en compte des critères techniques, fonctionnels, financiers, et stratégiques.

Par les outils et services Microsoft Azure, on inclut des composants et ressources nécessaires qui participent activement dans le cycle de vie des données. Ce dernier peut s'organiser en plusieurs briques :

- Une brique d'ingestion des données.
- Une brique de prétraitement, de transformation et d'intégration de ces données.
- Une brique de stockage massive des données structurées, semi structurées et non structurées.
- Une brique de traitement et d'analyse y compris l'analyse avancée en utilisant des algorithmes de Machine Learning et de Deep Learning...
- Une brique de visualisation et de restitution de ces données aux acteurs internes et externes.

Une brique de bonne gouvernance des données collectées, ingérées, traitées et restituées est également susceptible d'être intégrée.

À titre d'exemple, dans le cadre de la suite logicielle Microsoft Azure, des services tels que Azure Data Factory, Azure Databricks, Azure Synapse Analytics, Azure Data Lake Storage, Azure SQL Database, Azure Machine Learning... peuvent être impliqués dans ce processus, en offrant une vue d'ensemble complète pour gérer, traiter, analyser, et gouverner les données.

4.2 Exigences relatives à l'infrastructure de la plateforme

4.2.1 Exigences techniques

Ce chapitre traite les exigences techniques auxquelles doit satisfaire la plateforme de données de supervision GPE. Elle traite également les exigences et prestations que le Titulaire doit s'acquitter et honorer auprès de la SGP lors de l'exécution du marché.

[EXI:PDS_GPE_4-001]

Le Titulaire devra veiller et se charger de la maintenance logicielle de la plateforme de données GPE, il est responsable de l'ensemble des tâches techniques liées à la gestion, l'entretien, et l'évolution de la plateforme.

Cette plateforme va inclure des composants tels que des bases de données structurées, semi structurées, non structurées, des outils d'intégration et d'ingestion de données, des systèmes de traitement et d'analyse des données, ainsi que des interfaces utilisateurs pour l'accès et la visualisation de données.

Le Titulaire doit donc se charger des tâches non exhaustives suivantes :

- La gestion des correctifs (correction des anomalies liées au différents composants de la plateforme) ;
- La disponibilité des composants nécessaires au bon fonctionnement des services de la plateforme ;
- La mise à jour et évolution des composants et de la plateforme ;
- La supervision et de la surveillance de la plateforme ;
- La gestion des incidents et supports techniques ;
- L'optimisation de performance (le traitement de données massives avec des règles SSI et algorithme IA peut affecter la performance d'une plateforme de donnée) ;
- Sécurité et gestion des risques ;
- Gestion des sauvegardes et récupération ;
- Conformité et gouvernance des données ;
- Scalabilité et gestion de la charge.

[FIN]

4.2.1.1 Architecture

[EXI:PDS_GPE_4-002]

L'architecture de la plateforme de données GPE doit permettre la communication des zones de stockage, transformation et traitement et donc de différents fournisseurs de cloud (SaaS, PaaS, IaaS, CaaS). De plus, cette architecture doit être modulaire, afin de permettre l'ajout, la modification ou même le retrait de composants de données sans affecter le reste de la plateforme.

La plateforme doit prendre en charge des pipelines de données automatisés afin de permettre à l'ingénieur de données de gérer et suivre les pipelines de données.

[FIN]

[EXI:PDS_GPE_4-003]

Étant donné le choix effectué de recourir à la solution Outscale comme éditeur de cloud et d'infrastructure pour le stockage permanent des données, la configuration et la sécurisation de ces données basées sur une solution type Minio S3 pour la Zone (A), l'architecture proposée par le Titulaire doit être interopérable avec Outscale et doit fournir des connecteurs pour faciliter l'intégration des systèmes tiers.

[FIN]

[EXI:PDS_GPE_4-004]

Le Titulaire doit proposer une architecture cloud pouvant être hébergée sur fournisseur de cloud. Le Titulaire doit décrire et justifier des services cloud et technologies proposées.

[FIN]

[EXI:PDS_GPE_4-005]

L'architecture proposée doit prendre en compte l'entièreté du périmètre du marché (zone d'interface, de traitement, et de restitution de la donnée). L'architecture proposée doit pouvoir s'interfacer avec les applications du SI existant et à venir.

[FIN]

4.2.1.2 Supervision

[EXI:PDS_GPE_4-006]

La plateforme de données GPE doit avoir un outil de monitoring pour surveiller la santé de l'infrastructure, avec des alertes configurées pour les incidents critiques, elle doit également disposer d'un système de gestion des journaux mis en place par le Titulaire pour conserver des traces détaillées des événements de sécurité.

[FIN]

[EXI:PDS_GPE_4-007]

De plus, le Titulaire est amené à effectuer les tâches suivantes :

- Détection des coupures ou dégradations de service avec en résultante le déclenchement des actions correctives (application de consigne, escalade, déclenchement de l'astreinte...) ;
- Actions de contrôle ; disponibilité d'un service, d'un serveur, exécution des sauvegardes... ;

- Traitement des alertes suivant consignes (restauration du service ou diagnostic et escalade, correction préventive avant incident) ;
- Acquiescement des alarmes et 1er diagnostic à distance en 24 h/ 24 et 7 j/ 7 ;
- Arrêt et/ou relance des systèmes sur la base de consignes formalisées ;
- Gestion des passages des patchs sur les infrastructures sur la base de procédures ;
- Réalisation de travaux à la demande (sauvegarde, application de consignes de supervision...) sur la base de procédures formalisées ;
- Traitement des incidents sur procédures, escalade et alimentation de la base incident, gestion des problèmes, base de connaissance.

[FIN]

[EXI:PDS_GPE_4-008]

Dans le cadre de la gestion des consignes et procédures, le Titulaire collecte des consignes et des procédures fournies par les experts techniques vers l'exploitation et effectue une proposition de mise à jour des consignes et des procédures pour validation par les experts techniques avant transfert vers l'exploitation.

[FIN]

[EXI:PDS_GPE_4-009]

Il est également attendu du Titulaire l'analyse et le reporting sur les points suivants :

- Communication sur les indisponibilités et les arrêts programmés des infrastructures ;
- Communication sur les mises en production de type infrastructures ;
- Communication sur les événements (coupures de courant, travaux particuliers sur l'infrastructure...) ;
- Communication autour des bonnes pratiques.

[FIN]

La communication est unifiée au titre de la Gouvernance. Cette activité est réalisée sous la validation des éléments de communication et du choix des canaux de la SGP.

4.2.1.3 Environnements

4.2.1.3.1 Gestion du réseau

[EXI:PDS_GPE_4-010]

La plateforme des données du GPE doit garantir :

- une connectivité réseau stable et sécurisée.
- une connexion réseau à haut débit pour garantir la performance du traitement des données.

- un réseau redondant pour assurer la disponibilité en cas de panne du lien principal.

[FIN]

4.2.1.3.2 Protocoles

[EXI:PDS_GPE_4-011]

Les échanges de données entre client et serveurs ; serveur et serveur ; serveur et base de données doivent être chiffrés et à l'état de l'art.

[FIN]

[EXI:PDS_GPE_4-012]

Une matrice complète (ports, protocoles) des flux internes et externes nécessaires au fonctionnement de l'application est exigée.

[FIN]

4.2.1.3.3 Gestion des environnements et de leurs sécurités

[EXI:PDS_GPE_4-013]

La plateforme des données GPE doit permettre à un administrateur infrastructure d'allouer des ressources de types GPU à des environnements différents pour offrir une capacité de traitement en apprentissage à un Data Scientist selon le cas d'usage. Elle doit également offrir la possibilité d'utiliser des pipelines CI/CD pour l'automatisation des déploiements.

[FIN]

[EXI:PDS_GPE_4-014]

A minima, dans le cadre de cette plateforme, le Titulaire doit mettre à disposition trois environnements généralement appelés : développement, préproduction, production. D'autres environnements sont envisageables type : formation, recette. Les données métier ne doivent être accessibles qu'en production et préproduction. Les autres environnements doivent contenir des jeux de données désensibilisés.

[FIN]

[EXI:PDS_GPE_4-015]

Les environnements de production et de préproduction doivent être iso fonctionnels. Les différents types d'environnements ne doivent pas communiquer entre eux. Sauf dérogation explicite, il n'est pas possible d'avoir d'échange entre des machines d'environnements différents.

[FIN]

4.2.1.3.4 Performance

[EXI:PDS_GPE_4-016]

La plateforme des données GPE doit garantir une disponibilité de 99,95% pour les services critiques ; (accords de niveau de service (SLA) fournis par Azure et Outscale...).

[FIN]

[EXI:PDS_GPE_4-017]

La plateforme des données GPE doit permettre d'effectuer des tests de performance réguliers pour s'assurer que la plateforme supporte la charge de travail, plus particulièrement dans le cadre de traitement de données massive.

[FIN]

4.2.1.4 Gestion et optimisation de la capacité, de la disponibilité et de la performance globale

[EXI:PDS_GPE_4-018]

Il est attendu du Titulaire d'effectuer un suivi et des actions d'optimisation des capacités et des performances de l'infrastructure. À ce titre, le Titulaire doit effectuer un suivi de la disponibilité des composants de la plateforme comprenant des indicateurs classiques de disponibilité et une analyse des causes majeures (en fréquence ou en durée) d'indisponibilité. Seules les plages de service programmées à long terme peuvent être déduites du calcul de la disponibilité.

[FIN]

[EXI:PDS_GPE_4-019]

Le Titulaire doit également effectuer une analyse des causes majeures d'indisponibilité, et production d'un plan d'amélioration de la disponibilité avec des conseils sur l'optimisation du paramétrage des infrastructures ainsi que des propositions d'optimisation des seuils.

[FIN]

[EXI:PDS_GPE_4-020]

Il est également attendu du Titulaire :

- Un suivi régulier des performances et des charges des composants ;
- Une optimisation du paramétrage des composants ;
- Une optimisation des seuils définis et déclenchement d'un processus curatif en cas de franchissement de ces seuils (hors processus Plan de Capacité) ;
- La production d'un Plan d'évolutions des capacités et de la disponibilité incluant des propositions d'amélioration et stratégies d'évolutions, à moyen et/ou long terme.

[FIN]

[EXI:PDS_GPE_4-021]

Les documents à remettre lors des comités de suivi sont, notamment :

- Fichier de suivi de la disponibilité ;
- Fichier de suivi des performances ;
- Plan d'évolutions des capacités et de la disponibilité ;
- Rapport d'analyse.

[FIN]

4.2.1.5 Interfaces Homme-Machine (IHMs)

[EXI:PDS_GPE_4-022]

La plateforme des données GPE doit disposer d'une interface utilisateur intuitive pour le portail web, qui peut être personnalisée par les utilisateurs finaux.

[FIN]

[EXI:PDS_GPE_4-023]

L'interface doit être disponible en Français, tout en maintenant les termes techniques spécifiques à certains domaines ou métiers dans la langue d'origine (comme l'anglais) et ce pour garantir la cohérence avec les standards et pratiques du secteur (Ex ; expressions dans le domaine de la Data Science, Data Engineering ... à laisser en anglais pour éviter des confusions).

[FIN]

[EXI:PDS_GPE_4-024]

L'interface utilisateur doit permettre de travailler en mode "Bureau étendu" pour permettre à son utilisateur de gérer une surface de travail sur plusieurs écrans.

[FIN]

[EXI:PDS_GPE_4-025]

Les IHMs de la plateforme des données GPE doivent pouvoir garder la constance de l'affichage et de la qualité de l'image, et ce indépendamment de la résolution et de la configuration matérielle de la plateforme, à ce titre l'affichage doit s'ajuster automatiquement à la taille des terminaux utilisés afin de garantir la lisibilité des informations.

[FIN]

4.2.1.6 Gestion des sauvegardes

[EXI:PDS_GPE_4-026]

La plateforme des données GPE doit permettre l'exécution et la planification automatique de la sauvegarde des données critiques dans des services lors de l'attribution du marché (ex : Azure Backup), de même elle doit permettre la récupération granulaire (fichier individuel, base de données complète, etc.) des données à partir des sauvegardes

[FIN]

[EXI:PDS_GPE_4-027]

La plateforme des données GPE doit également gérer la rétention des sauvegardes selon des durées définies, à noter que des tests de restaurations doivent être effectués régulièrement pour s'assurer de l'intégrité des sauvegardes.

[FIN]

[EXI:PDS_GPE_4-028]

La plateforme des données GPE doit garantir la redondance des sauvegardes sur plusieurs régions géographiques, les sauvegardes ne peuvent pas être hébergées sur une location identique aux données sources.

[FIN]

[EXI:PDS_GPE_4-029]

La plateforme des données GPE doit garantir que toutes les sauvegardes sont chiffrées au repos et en transit (chiffrement avec des algorithmes conformes aux normes de sécurité actuelles...)

[FIN]

[EXI:PDS_GPE_4-030]

La plateforme des données GPE doit permettre la compression automatique des sauvegardes dans le but d'optimiser l'espace de stockage. Le Titulaire doit optimiser (compression, déduplication...) le volume de données pour le transit vers la plateforme de sauvegarde.

[FIN]

[EXI:PDS_GPE_4-031]

Plusieurs niveaux de service sont à identifier en fonction des politiques de sauvegardes (le type, la récurrence et la rétention) avec le Titulaire.

[FIN]

[EXI:PDS_GPE_4-032]

En fin de marché, les données sauvegardées doivent être restituées à la SGP ou au nouveau Titulaire lors de la phase de réversibilité (cf. §3.3.11 UO_D11 - Réversibilité).

[FIN]

4.2.1.7 Scalabilité et gestion de la charge

[EXI:PDS_GPE_4-033]

Le Titulaire doit s'assurer que la plateforme de données GPE soit capable de s'adapter à l'augmentation de volume de données et à l'augmentation du nombre d'utilisateurs et ce en mettant en place des mécanismes de scalabilité de contrôle (ex : mettre en place de bon GPU pour l'apprentissage automatique), de plus et dans ce contexte.

[FIN]

[EXI:PDS_GPE_4-034]

La plateforme de données GPE doit permettre également l'ajout de ressources horizontales et verticales pour supporter la croissance en fonction des besoins de traitement.

[FIN]

[EXI:PDS_GPE_4-035]

Les évolutions majeures impactant le coût du service, doivent être validées par la SGP.

[FIN]

4.2.2 Exigences de services

4.2.2.1 Gestion des Demandes et Incidents

[EXI:PDS_GPE_4-036]

La gestion des incidents comprend, notamment :

- Résolution des incidents, y compris, hors procédures et/ou hors consignes applicables ;
- Rétablissement des performances en cas de dégradation ;
- Résolution des incidents et mises en œuvre des procédures d'escalade ;
- Application des procédures d'escalade en vigueur ;
- Remontée d'alertes pertinentes.

[FIN]

Services attendus au titre des tickets :

[EXI:PDS_GPE_4-037]

Gestion des incidents de niveau 2

La prestation comprend, notamment l'analyse et diagnostic des incidents escaladés par les autres groupes de support ou identifiés via les télé distributions réalisées ou la surveillance périodique du parc.

[FIN]

[EXI:PDS_GPE_4-038]

Assistance et support niveau 3

La prestation comprend notamment l'analyse et le diagnostic des incidents escaladés par les autres groupes de support. Dans le cadre du traitement des incidents le Titulaire effectue :

- Mise à jour du dossier (domaine technique, cause, description, ...) ;
- Résolution d'incidents et notification au gestionnaire des référentiels le cas échéant ;
- Information de l'avancement des dossiers ;
- Clôture technique des dossiers traités conformément aux procédures SGP.

[FIN]

[EXI:PDS_GPE_4-039]

Dans le cadre du traitement des incidents majeurs et critiques, le Titulaire effectue :

- Analyse, communication, mise en place des solutions de contournements et résolution des incidents avec la réactivité nécessaire suivant la priorité de l'incident ;

[FIN]

[EXI:PDS_GPE_4-040]

Dans le cadre du traitement des incidents majeurs et critiques, le Titulaire effectue :

- Analyse, communication, mise en place des solutions de contournements et résolution des incidents avec la réactivité nécessaire suivant la priorité de l'incident ;
- Analyse collaborative avec d'autres groupes de support pour les incidents qui le nécessitent. La prestation comprend également la gestion et l'identification des problèmes ;
- Analyse des problèmes, si nécessaire avec d'autres groupes de support ;
- Mise en place de solution de contournement si nécessaire ;
- Proposition et gestion de solution.

[FIN]

[EXI:PDS_GPE_4-041]

Gestion des problèmes

La prestation comprend, notamment :

- Identification des problèmes ;

2024DC001 – PROGRAMME FONCTIONNEL
Code GED : DSTE_06_ACT_STE_002360_1

Ce document est la propriété de la Société des grands projets. Toute diffusion ou reproduction intégrale ou partielle est autorisée pour et dans la limite des besoins découlant des prestations ou missions du marché conclu avec le titulaire destinataire.

- Analyse des problèmes, si nécessaire avec d'autres groupes de support, pour identification des causes ;
- Mise en œuvre d'actions pour améliorer et corriger la situation.

[FIN]

4.2.2.2 Administration

[EXI:PDS_GPE_4-042]

L'administration courante comprend notamment :

- Maintien en condition opérationnelle (ex. : mise à jour des composantes infrastructures, systèmes et logiciels, dont antivirus et patches de sécurité sur les serveurs) ;
- Modification de paramétrage ;
- Gestion des espaces de stockage (Création, modification, retrait...) ;
- Gestion des systèmes de haute disponibilité ;
- Gestion de la virtualisation ;
- Sauvegarde ou restauration de composants et de données ;
- Gestion et génération des certificats et clés ;
- L'extraction d'information (système ou applicatif) ;
- La gestion des alertes (Création, modification...) ;
- Création et maintien de script d'administration (Powershell, etc...) ;
- Gestion des décommissions de ressources ;
- Toute autre demande de tâche d'administration ;
- Réalisation des contrôles quotidiennes et hebdomadaires ;
- Réalisation des opérations planifiées ;
- Planification et suivi des mises en production.

[FIN]

[EXI:PDS_GPE_4-043]

Cela comprend également la résolution des incidents non procédurés et la mise en œuvre des procédures d'escalade :

- Résolution d'incidents et satisfaction des demandes de services escaladés par le Pilotage de la SGP ;
- Escalade vers les entités de support (supports externes au Titulaire, Constructeur, Editeur...) ;
- Information du Pilotage de la SGP de l'évolution et de l'avancement des dossiers ;
- Clôture technique des incidents.
- Coordination avec les éditeurs et les mainteneurs applicatifs (titulaires de marché de TMA) pour assurer la compatibilité des systèmes ;
- Analyse des journaux d'évènement ;

- Mise en œuvre des mesures préventives à tout blocage par suite d'une alerte identifiée dans le cadre des activités de surveillance ;
- Mise en œuvre de chaînes de traitement ;
- Validation de la mise à jour antivirale ;
- Validation de la bonne exécution des sauvegardes ;
- Arrêt-reliance des systèmes, y compris hors horaires d'ouverture ;
- Maintenance des bases de données ;
- Opérations simples et tâches courantes identifiées au calendrier d'exploitation (renouvellement des informations d'identification, renouvellement de certificat, extension de volumétrie, création de ressources, ou tâches équivalentes).

[FIN]

4.2.2.3 Exploitation courante des infrastructures systèmes et services

[EXI:PDS_GPE_4-044]

L'exploitation comprend, notamment :

- Installation et configuration des systèmes ;
- Déploiement de machines virtuelles ;
- Gestion des utilisateurs et identités, de l'authentification et des accès (généraux, de service et à privilèges, inclus création, modification, suppression...) ;
- Mise en œuvre de confiance (SSO, SAML, Oauth...) ;
- Arrêt-reliance des systèmes (avec validation de la SGP et procédure).
- Prise de mesures préventives à tout blocage (exemple : purge des logs avec validation de la SGP ou sur la base d'une consigne) ;
- Remontée d'alertes pertinentes aux autres groupes supports ;
- Surveillance des performances et diagnostic en cas de dégradation des temps d'accès ;
- Intervention pour rétablir les performances en cas de dégradation ;
- Traitement des tickets et incident éditeurs, constructeurs.
- Rédaction et maintien de documentations (techniques, opérationnelles...) ;
- Réalisation des tableaux de bord de fonctionnement ;
- Détection de la présence de vulnérabilités.

[FIN]

4.2.2.4 Priorités et engagements

[EXI:PDS_GPE_4-045]

Priorités des incidents

La priorité est basée sur l'impact (criticité du bien) et sur l'urgence (sévérité de l'incident). Elle sert à identifier le délai acceptable pour la mise en œuvre d'une action.

Il y a quatre niveaux de priorité :

- P1 - Impact sévère sur le métier des utilisateurs ;
- P2 - Impact majeur sur le métier des utilisateurs ;
- P3 - Impact mineur sur le métier des utilisateurs ;
- P4 - Pas d'impact sur le métier des utilisateurs.

En cas de désaccord entre les parties sur la priorité de l'incident, la qualification donnée par la SGP prévaudra durant l'incident. Après résolution, la priorité sera éventuellement analysée afin de valider correctement sa classification comme décrit ci-après :

Priorité	Description
P1	Impact sévère sur les processus métiers L'exécution du processus métier principal est bloquée : <ul style="list-style-type: none"> • Un outil est indisponible ou très gravement atteint • Des fonctions critiques de l'entreprise ne peuvent pas être exécutées
P2	Impact majeur sur les processus métiers <ul style="list-style-type: none"> • Une partie de l'outil n'est pas active, ou fonctionne mal • Une partie des fonctions critiques de l'outil ne peut pas être exécutée ou à des temps de réponse qui s'écartent de façon significative des niveaux convenus • Les utilisateurs finaux sont capables de travailler mais sont incapables d'atteindre un niveau de productivité normal en raison de l'incident
P3	Impact mineur sur les processus métiers <ul style="list-style-type: none"> • Priorité par défaut
P4	Pas d'impact sur les processus métiers <ul style="list-style-type: none"> • L'incident n'a guère de conséquences pour l'utilisateur final, mais l'outil ne répond pas pleinement aux accords conclus

La matrice de priorisation des incidents en fonction de l'urgence et de l'impact est la suivante :

Priorité des incidents		Urgence		
		Forte	Modérée	Faible
Impact	Fort	P1	P2	P3
	Modéré	P2	P3	P4
	Faible	P3	P4	P4

[FIN]

[EXI:PDS_GPE_4-046]

Temps garantis

Les niveaux de performance cible sont déterminés en fonction de la priorité des incidents et du niveau de service attendu (Bronze, Argent ou Or).

[FIN]

[EXI:PDS_GPE_4-047]

Lorsque le risque de non-respect d'un temps garanti P1 ou P2 est avéré et qu'une solution de contournement peut être proposée, son intégration se fera exclusivement avec l'accord avec la SGP.

[FIN]

[EXI:PDS_GPE_4-048]

Si une procédure de contournement est nécessaire, celle-ci doit être fournie et mise en œuvre afin de respecter les délais prévus par la GTR. Dans ce cas, la priorisation est revue au niveau P3 et le Titulaire est tenu de mettre en œuvre une solution définitive dans les délais associés à la priorité P3.

Temps garantis									
Priorité	Bronze			Argent			Or		
	GTD	GTI	GTR	GTD	GTI	GTR	GTD	GTI	GTR
P1	5 min	2 h	8 h	5 min	1h	4 h	5 min	30 min	2 h
P2	5 min	4 h	16 h	5 min	2h	8 h	5 min	1 h	4 h
P3	5 min	8 h	36 h	5 min	4h	16 h	5 min	2 h	8 h
P4	5 min	16 h	72 h	5 min	8h	32 h	5 min	4 h	16 h

- GTD : Garantie des Temps de Détection

- GTI : Garantie des Temps d'Intervention
- GTR : Garantie des Temps de Rétablissement

[FIN]

[EXI:PDS_GPE_4-049]

Autres sollicitations

La priorité des autres sollicitations (demandes de service, demandes d'informations, ...) est fixée par défaut à 20 minutes pour la prise en charge et 8 heures ouvrées pour le traitement sauf précision contraire à l'annexe à la convention de service.

[FIN]

4.3 Sécurité de la plateforme

4.3.1 Sécurité des prestations

[EXI:PDS_GPE_4-050]

Hum-01 - Sensibilisation des intervenants : Le Titulaire doit s'assurer que le personnel intervenant sur le périmètre de la prestation soit formé aux bonnes pratiques et aux bases de la sécurité au sein d'un système d'information.

[FIN]

[EXI:PDS_GPE_4-051]

Act-01 : Poste de travail : Le Titulaire doit s'assurer que le personnel intervenant sur le périmètre de la prestation utilise un poste de travail qui ne servira qu'à l'usage professionnel et dont la configuration de sécurité a été renforcée. Ces postes de travail doivent notamment être équipés d'un logiciel anti-virus.

[FIN]

[EXI:PDS_GPE_4-052]

Act-02 : Localisation des prestations : Le Titulaire s'engage à ce que les activités de développement de code et d'algorithmes spécifiques au Clint soient réalisées sur le territoire de l'Union Européenne.

[FIN]

[EXI:PDS_GPE_4-053]

Sde-01- Formation des développeurs : Le Titulaire s'engage à ce que le personnel mis à disposition pour réaliser des activités développement informatique soit formé sur le développement sécurisé et sur les vulnérabilités classiques.

[FIN]

[EXI:PDS_GPE_4-054]

Sde-02 - Utilisation d'outils d'analyse de code : Le Titulaire s'engage à utiliser des outils permettant de minimiser les erreurs introduites durant le développement informatique ainsi que les défauts de sécurité.

[FIN]

[EXI:PDS_GPE_4-055]

Sde-03 - Gestion du code et des algorithmes : Le code informatique et les algorithmes produits spécifiquement pour le Client doivent être documentés, historisés et maintenables. Ces éléments seront la propriété du Client.

[FIN]

[EXI:PDS_GPE_4-056]

Sde-04 - Confidentialités aux données : Le Titulaire ne doit en aucun cas copier de données de la Plateforme sur un autre système d'information que celui assurant son fonctionnement et sa sauvegarde. Le Titulaire ne doit pas communiquer les données de la Plateforme à un tiers, ni les exploiter en interne pour son propre compte.

[FIN]

[EXI:PDS_GPE_4-057]

Sde-05 - Incidents de sécurité : Le Titulaire s'engage à notifier immédiatement au Client tout incident relatif à la sécurité des systèmes d'information concernant le périmètre des prestations.

[FIN]

[EXI:PDS_GPE_4-058]

Sde-06 - Certification du Titulaire : Le Titulaire doit disposer d'une certification ISO 27001 concernant le périmètre des activités de ce marché.

[FIN]

[EXI:PDS_GPE_4-059]

Sde-07 - Gestion des incidents de sécurité : Le Titulaire doit disposer, sur le périmètre de la prestation, d'un processus formalisé et opérationnel de gestion des incidents de sécurité. Celui-ci doit tenir compte des phases suivantes : détection, analyse, traitement, alerte du Client.

[FIN]

[EXI:PDS_GPE_4-060]

Sde-08 - Gestion de crise : Sur le périmètre de la prestation sous sa responsabilité, le Titulaire doit disposer d'un plan de gestion de crise formalisé et opérationnel tenant compte des aspects SSI.

[FIN]

[EXI:PDS_GPE_4-061]

Sde-09 - Audits : Le Titulaire s'engage à autoriser le Client à conduire ou mandater des contrôles et audits de sécurité informatique des prestations, moyens utilisés et services proposés, et leurs éventuels sous-traitants.

[FIN]

[EXI:PDS_GPE_4-062]

Sde-10 - Réversibilité : Le Titulaire doit disposer d'une procédure permettant la restitution et la destruction définitive des données de la Passerelle. Cela concerne également le code informatique et les algorithmes qui auraient été créés pour le Client.

[FIN]

[EXI:PDS_GPE_4-063]

Sde-11 - Tableau de bord sécurité : Le Titulaire s'engage à mettre en place et tenir à jour un tableau de bord sécurité. Ce tableau de bord est communiqué mensuellement à la SGP, il liste et détaille les incidents, écarts aux règles de sécurité et plan d'actions associés.

[FIN]

[EXI:PDS_GPE_4-064]

Sde-12 - Gestion de l'obsolescence et des vulnérabilités : Le Titulaire est garant du maintien en conditions de sécurité de l'ensemble des composants informatique utilisés dans le cadre de la Prestation. Ces composants doivent être dans une version pour laquelle l'éditeur assure le support, ils doivent être à jour en matière de correctifs de sécurité.

[FIN]

4.3.2 Hébergement des données et des services

[EXI:PDS_GPE_4-065]

Le Titulaire doit garantir que les configurations de sécurité respectent les normes exigées, y compris le chiffrement des données, l'accès sécurisé, et la conformité aux réglementations en vigueur. À noter que les données manipulées ne rentrent a priori pas dans le champ d'application du règlement général de protection des données (RGPD).

[FIN]

[EXI:PDS_GPE_4-066]

Heb-01 - Certifications liées à l'hébergement : Le Titulaire doit s'assurer que l'hébergement des données et des services informatiques concernés par la prestation est certifié SOC 2 type 2 et ISO 27001.

[FIN]

[EXI:PDS_GPE_4-067]

Heb-02 - Localisation de l'hébergement : Le Titulaire doit s'assurer que l'hébergement des données et des services manipulant ces données sont situés exclusivement sur le territoire national.

[FIN]

[EXI:PDS_GPE_4-068]

Heb-03 - Redondance de l'hébergement : Le Titulaire doit s'assurer que l'hébergement des services et des données de la Passerelle est redondé sur au moins 2 sites distincts éloignés géographiquement. Cette redondance doit permettre de couvrir les risques environnementaux localisés.

[FIN]

4.3.3 Disponibilité de la Plateforme

[EXI:PDS_GPE_4-069]

Dis-01 - Supervision : Le Titulaire doit procéder à la supervision informatique de la Passerelle afin d'identifier au plus vite toute indisponibilité ou dysfonctionnement de celle-ci.

[FIN]

[EXI:PDS_GPE_4-070]

Dis-02 - Taux de disponibilité : Le Titulaire doit garantir une disponibilité de la plateforme d'au moins 95%. Ce taux est calculé sur une base mensuelle.

[FIN]

[EXI:PDS_GPE_4-071]

Dis-03 - Indisponibilités non planifiées : Le Titulaire s'engage à informer rapidement le Client en cas d'incident impactant la disponibilité ou le bon fonctionnement de la Passerelle.

[FIN]

[EXI:PDS_GPE_4-072]

Dis-04 - Indisponibilités planifiées : Les opérations impliquant une indisponibilité de tout ou partie de la Plateforme doivent être notifiée au Client au moins 2 jours ouvrés à l'avance. Le délai de prévenance est porté à 2 semaines en cas d'indisponibilité planifiée de plus de 6 heures. Le Titulaire s'engage à limiter les impacts des indisponibilités planifiées, notamment en réduisant la fréquence et la durée d'indisponibilité.

[FIN]

[EXI:PDS_GPE_4-073]

Dis-06 - Sinistre majeur : Le Titulaire doit être en capacité de rétablir les fonctionnalités essentielles de la plateforme en moins de 72 heures après un sinistre majeur. Cette exigence s'applique notamment aux cas suivants : perte ou défaillance d'un centre de données, cyber-attaque, catastrophe humaine ou naturelle sur un périmètre géographique limité.

[FIN]

[EXI:PDS_GPE_4-074]

Les exigences précédentes s'appliquent au périmètre global de responsabilité du Titulaire, cela intègre les interfaces, applications, et socles techniques à sa charge. Tout écart avec l'une de ces exigences pourra donner lieu à l'application d'une pénalité.

[FIN]

4.3.4 Sauvegardes

[EXI:PDS_GPE_4-075]

Sau-01 - Sauvegarde : Le Titulaire s'assure que les données de la Passerelle sont sauvegardées. Ces sauvegardes sont traitées de manière à garantir leur confidentialité et leur intégrité. Les sauvegardes de données ne doivent pas être soumises aux mêmes risques de sinistres que les données sauvegardées. Les sauvegardes doivent permettre de garantir une perte de données maximale admissible de 72 heures (PDMA).

[FIN]

[EXI:PDS_GPE_4-076]

Sau-02 - Supervision des sauvegardes : Le Titulaire s'assure que les opérations relatives aux sauvegardes sont supervisées. Cette supervision doit permettre d'identifier au plus vite tout dysfonctionnement relatif à la gestion des sauvegardes.

[FIN]

[EXI:PDS_GPE_4-077]

Sau-03 - Tests de restauration : Le Titulaire s'assure qu'un test de restauration des sauvegardes est effectué au moins une fois par an. Ce test de restauration de sauvegarde est à réaliser avant l'ouverture effective du service pour le Client.

[FIN]

4.3.5 Chiffrement des flux et gestion des certificats

[EXI:PDS_GPE_4-078]

A1 : Sécurisation du flux de récupération des données sources

Le flux de récupération des données de la zone A1 doit être sécurisé par l'usage d'un tunnel VPN de type IPsec. Ce tunnel VPN doit être configuré de sorte à assurer la confidentialité et l'intégrité des données transférées, et à empêcher toute altération des données à leur source.

[FIN]

[EXI:PDS_GPE_4-079]

A2 : Chiffrement des flux d'échanges inter-applicatifs

Les échanges de fichiers et de données entre applications s'appuient sur des protocoles chiffrés et à l'état de l'art. L'utilisation de protocoles ne permettant pas le chiffrement est prohibée (ex : SMBv1, HTTP).

[FIN]

[EXI:PDS_GPE_4-080]

A3 : Privilégier TLS 1.3 et accepter TLS 1.2

La version TLS 1.3 doit être prise en charge et privilégiée. La version TLS 1.2 est également acceptée sous condition de suivre les exigences ci-dessous.

[FIN]

[EXI:PDS_GPE_4-081]

A4 : Ne pas utiliser SSLv2, SSLv3, TLS 1.0 et TLS 1.1

Les versions SSLv2, SSLv3, TLS 1.0 et TLS 1.1 sont interdites.

[FIN]

[EXI:PDS_GPE_4-082]

A5 : Authentifier le serveur à l'échange de clé

Au cours d'un échange de clé, le serveur doit être authentifié par le client. Les alternatives anonymisées de ces échanges ou reposant sur l'utilisation de certificat brut définies dans la RFC 7250 sont proscrites.

[FIN]

[EXI:PDS_GPE_4-083]

A6 : Échanger les clés en assurant toujours la PFS

La propriété de confidentialité persistante doit être assurée (PFS). Il faut pour cela employer une suite cryptographique reposant sur un échange Diffie-Hellman éphémère (ECDHE ou, à défaut, DHE).

[FIN]

[EXI:PDS_GPE_4-084]

A7 : Utiliser SHA-2 comme fonction de hachage

Les fonctions de hachage de la famille SHA-2 doivent être utilisées.

[FIN]

[EXI:PDS_GPE_4-085]

A8 : Préférer l'ordre de suites du serveur

L'ordre des suites cryptographiques qui figure dans sa configuration du serveur doit prévaloir sur l'ordre des suites signalées par les clients.

[FIN]

[EXI:PDS_GPE_4-086]

A9 : Utiliser des clés de taille suffisante

Pour une protection des communications, les clés RSA doivent avoir une taille minimale de 2048 bits, et les clés ECDSA doivent avoir une taille minimale de 256 bits.

[FIN]

[EXI:PDS_GPE_4-087]

A10 : Recourir à un processus sécurisé de fourniture des certificats

Les certificats présentés doivent être valides, leur processus de renouvellement doit s'effectuer sans action humaine.

[FIN]

4.3.6 Développement sécurisé

[EXI:PDS_GPE_4-088]

B1 : Vérifier l'échappement des contenus inclus

Les données externes employées dans quelque partie que ce soit de la réponse envoyée au navigateur doivent avoir fait l'objet d'un « échappement » adapté au contexte d'interprétation.

[FIN]

[EXI:PDS_GPE_4-089]

B2 : Vérifier la conformité des données issues de sources externes

Il est nécessaire de vérifier, chaque fois que c'est possible, que les données ont bien la forme attendue. Lorsque cela est possible, une approche par liste d'autorisations est recommandée : par exemple une donnée censée être numérique ne doit être composée que de chiffres.

[FIN]

[EXI:PDS_GPE_4-090]

B3 : Proscrire l'usage de la fonction *eval()*

La fonction eval permettant la transformation de chaîne de caractères en code représente un risque important. L'usage de cette fonction (ou équivalente) doit être proscrit.

[FIN]

[EXI:PDS_GPE_4-091]

B4 : Proscrire l'accès en JavaScript à un cookie de session

Pour un cookie de session, il est nécessaire de positionner l'attribut HttpOnly.

[FIN]

[EXI:PDS_GPE_4-092]

B5 : Limiter le transit des cookies aux flux sécurisés

Dès lors que des cookies sont nécessaires le flag Secure doit être utilisé.

[FIN]

[EXI:PDS_GPE_4-093]

B6 : Limiter les composants logiciels tiers

La liste des composants applicatifs tiers employés doit être limitée au strict nécessaire. Les composants non nécessaires doivent faire l'objet d'une suppression. Si leur suppression n'est

pas envisageable, il est recommandé de les désactiver. Les composants tiers doivent être stockés localement afin de ne pas impliquer l'accès à un autre hébergeur.

[FIN]

[EXI:PDS_GPE_4-094]

B7 : Maintenir à jour les composants logiciels tiers utilisés

Les composants applicatifs tiers employés doivent être recensés et maintenus à jour. Cela impose que les composants sélectionnés pour une production soient évalués sur leur pérennité lors des phases de conception et que les vulnérabilités publiées soient suivies pour chacun d'eux. Le recours à des composants logiciels tiers doit respecter leur condition d'utilisation.

[FIN]

[EXI:PDS_GPE_4-095]

B8 : Gestion de l'obsolescence

L'ensemble des outils et composants utilisés est dans une version pour laquelle l'éditeur assure le support, et tenu à jour.

[FIN]

[EXI:PDS_GPE_4-096]

B9 : Minimiser la divulgation d'informations liées aux composants techniques

Les versions des composants techniques utilisés ne doivent pas être rendu accessibles. Tout entête ou fichier permettant d'identifier un composant technique ou sa version (ex : header « Server », changelog) ne doit pas être divulgué.

[FIN]

[EXI:PDS_GPE_4-097]

B10 : Gestion des empreintes de mots de passe

Lorsqu'une application doit vérifier elle-même les mots de passe renseignés, celle-ci met en œuvre des mesures comme le hachage et le salage permettant de se prémunir contre les attaques documentées : attaques par dictionnaire, attaques par tables arc-en-ciel, attaques par force brute, etc.

[FIN]

4.3.7 Emails

[EXI:PDS_GPE_4-098]

C1 : Chiffrer les emails en transport

Si le service procède à l'envoi d'emails, un chiffrement opportuniste doit être proposé. Celui-ci doit s'appuyer sur les protocoles à l'état de l'art (STARTTLS en mode opportuniste avec chiffrement TLS 1.2 minimum).

[FIN]

[EXI:PDS_GPE_4-099]

C2 : Signer les emails sortants

Si le service procède à l'envoi d'emails, une signature DKIM à l'état de l'art doit être apposée (1024 bits minimum). L'enregistrement DNS associé doit être correctement déclaré.

[FIN]

[EXI:PDS_GPE_4-100]

C3 : Permettre le contrôle de l'authenticité des emails

Si le service procède à l'envoi d'emails, un enregistrement SPF doit être configuré de sorte que l'authenticité des emails puisse être vérifiée. Cet enregistrement doit être configuré en « soft fail » ou « hard fail » et complété d'un contrôle DMARC « reject » ou « quarantine ».

[FIN]

4.3.8 Nom de domaine et hébergement

[EXI:PDS_GPE_4-101]

D1 : Enregistrer les noms de domaines par la DSI de la SGP

Tout nouveau nom de domaine qui serait nécessaire dans le cadre de l'implémentation du service doit être réservé par la Client.

[FIN]

[EXI:PDS_GPE_4-102]

D2 : Héberger le service sur le territoire national

L'hébergement doit être effectué sur le territoire national, cette exigence concerne les différents environnements utilisés (production, préproduction...) ainsi que les sauvegardes.

[FIN]

4.3.9 Lutte contre les intrusions

[EXI:PDS_GPE_4-103]

E1 : Restreindre les ports en écoute

Seuls les ports 80 (http) et 443 (https) peuvent être ouverts en écoute sans restriction d'origine des flux. Aucun autre port ne doit être ouvert sans restriction d'origine (ex : base de données, FTP, SSH).

[FIN]

[EXI:PDS_GPE_4-104]

E2 : Rediriger ou bloquer le trafic non chiffré

Toute tentative connexion non chiffrée (http) doit être bloquée ou automatiquement redirigée vers un protocole chiffré (https).

[FIN]

[EXI:PDS_GPE_4-105]

E3 : Mettre en place un pare-feu applicatif (WAF)

Un outil tiers permettant d'intercepter les flux avant qu'ils arrivent au serveur web doit être configuré afin de détecter et bloquer les tentatives d'intrusions les plus fréquentes (top 10 OWASP).

[FIN]

[EXI:PDS_GPE_4-106]

E4 : Utiliser des composants faisant l'objet d'un support et exempt de vulnérabilités

L'ensemble des logiciels et matériels utilisés dans le cadre du service est dans une version pour laquelle l'éditeur assure le support. De plus ces logiciels et matériels doivent être à jour en matière de correctifs de sécurité.

[FIN]

4.3.10 Lutte contre les attaques

[EXI:PDS_GPE_4-107]

F1 : Réduire le risque de déni de service

Un outil ou mécanisme doit être mis en place afin de lutter contre les attaques par déni de service.

[FIN]

[EXI:PDS_GPE_4-108]

F2 : Protection contre les codes malveillants

Des logiciels de protection contre les codes malveillants, appelés communément antivirus, sont installés sur les serveurs d'interconnexion, serveurs applicatifs et postes de travail utilisés pour l'administration.

[FIN]

4.3.11 Administration et gestion des accès

[EXI:PDS_GPE_4-109]

G1 : Restreindre les interfaces d'administration

Les interfaces d'administrations, qu'elles s'appuient sur le protocole HTTPS ou non doivent être accessibles qu'après une authentification à deux facteurs. Lorsque cela n'est pas possible, elles ne doivent être accessible que depuis un tunnel VPN sécurisé ou une liste d'adresses IP validées.

[FIN]

[EXI:PDS_GPE_4-110]

G2 : Utilisation d'identifiant de connexion nominatifs

Des comptes d'administration individuels sont attribués à chaque administrateur. Les comptes natifs d'administration ne sont pas utilisés pour les actions courantes d'administration et les secrets associés ne sont accessibles qu'à un nombre très restreint de personnes.

[FIN]

[EXI:PDS_GPE_4-111]

G3 : Révision périodique des droits d'accès

Les comptes utilisés doivent être gérés d'une façon à ce que leur revue périodique soit possible. Cette revue doit pouvoir porter les droits d'accès associés et les ressources ou les fonctionnalités qui en font l'objet.

[FIN]

[EXI:PDS_GPE_4-112]

G4 : Confidentialité des informations d'authentification

Les mots de passe ne sont pas stockés en clair, ils ne transitent pas en clair sur le réseau.

[FIN]

[EXI:PDS_GPE_4-113]

G5 : Gestion du départ d'un administrateur

La gestion des accès doit permettre qu'un compte nominatif d'un administrateur soit désactivé sans impacter le fonctionnement du service. Lorsque des comptes génériques sont utilisés, la modification de leur secret doit être possible facilement, notamment à la suite du départ d'un administrateur.

[FIN]

[EXI:PDS_GPE_4-114]

G6 : Caractéristiques des mots de passe

Les mots de passe des comptes respectent les critères précisés ci-dessous :

- Compte utilisateur : 8 caractères minimum (avec 3 types de caractères différents parmi : majuscule, minuscule, chiffre, caractère spécial). Blocage de l'accès après 4 tentatives successives en échec.
- Compte administrateur : 15 caractères minimum (avec 4 types de caractères différents). Blocage automatique de l'accès après 3 tentatives en échec.
- Compte de service : 25 caractères minimum (avec 4 types de caractères différents)

[FIN]

[EXI:PDS_GPE_4-115]

G7 : Renforcer la sécurité des identifiants de connexion

Les interfaces utilisateur et d'administrations ne doivent être accessibles que depuis un tunnel VPN sécurisé ou une liste d'adresses IP préalablement validées, ou protégées par une authentification à deux facteurs.

[FIN]

[EXI:PDS_GPE_4-116]

G8 : Identification, authentification et contrôle d'accès logique

L'accès à la plateforme et ses données nécessite une identification et une authentification individuelle de l'utilisateur.

[FIN]

[EXI:PDS_GPE_4-117]

G9 : Contrôle d'accès à base de profils

Une gestion fine par profils d'accès doit être configurable. Les principes du besoin d'en connaître et du moindre privilège s'appliquent.

[FIN]

[EXI:PDS_GPE_4-118]

G10 : Gestion des comptes par défaut

Les comptes par défaut qui ne sont pas requis pour le fonctionnement du système ou son administration sont supprimés, ou à défaut désactivés. Les comptes par défaut requis pour le fonctionnement d'un système ou qui ne peuvent pas être supprimés ni désactivés sont configurés avec un nouveau mot de passe conforme à cette politique.

[FIN]

[EXI:PDS_GPE_4-119]

G11 : Limitation des droits des comptes de service

Les comptes de service font l'objet d'une restriction des droits, en suivant le principe du moindre privilège.

[FIN]

[EXI:PDS_GPE_4-120]

G12 : Centralisation du contrôle d'accès

Une architecture d'authentification centralisée doit être utilisée en lieu et place d'une gestion locale des mots de passe. Le système doit permettre imposer l'authentification des utilisateurs en s'appuyant sur un annuaire Active Directory ou Azure Active Directory.

[FIN]

4.3.12 Traçabilité des accès et supervision

[EXI:PDS_GPE_4-121]

H1 : Gérer un historique inaltérable des accès

Un journal des accès et tentatives d'accès doit être alimenté automatiquement. Ce journal doit être stocké d'une façon à ce qu'il ne puisse être altéré et doit couvrir l'ensemble des accès (utilisateur final, administrateur, interfaces...). Il doit indiquer a moins : adresse IP d'origine, URL accédée, horodatage, code de la réponse fournie par le serveur.

[FIN]

[EXI:PDS_GPE_4-122]

H2 : Conserver un historique des accès

Le journal des accès doit être conservé au moins 1 an.

[FIN]

4.3.13 Sécurité des interfaces de programmation d'applications (API)

[EXI:PDS_GPE_4-123]

K1 : Restriction des services et méthodes API strictement nécessaires

De façon à réduire la surface d'attaque, les services de type API doivent être activés uniquement lorsque nécessaire.

[FIN]

[EXI:PDS_GPE_4-124]

Une attention particulière doit être portée concernant :

- Les services de type API activés par défaut lors de la mise en place d'un nouveau service ou application informatique alors qu'ils ne seraient pas nécessaires.
- Les méthodes de type API activées par défaut lors de la mise en place d'un nouveau service ou application informatique alors qu'elles ne seraient pas nécessaires (ex. verbes *PUT*, *POST* ou *DELETE* lorsque qu'il est seulement nécessaire d'avoir un accès en consultation).

[FIN]

4.4 Intégration et orchestration des données

[EXI:PDS_GPE_4-125]

Le Titulaire peut s'appuyer sur Azure Data Factory pour l'orchestration des flux de données entre les différentes sources et destinations, assurant ainsi l'intégration fluide des données dans les environnements Big Data.

[FIN]

[EXI:PDS_GPE_4-126]

Le Titulaire doit utiliser des connecteurs de différentes bases de données afin de permettre l'ingestion de ces données provenant de diverses sources (bases de données, APIs, fichiers...).

[FIN]

[EXI:PDS_GPE_4-127]

En complément de certaines fonctions personnalisées dans les flux de données déjà proposées par Azure Data Factory, le Titulaire doit mettre en place d'autres briques en fonction des cas d'usages étudiés.

Une liste non exhaustive de ces UDFs (user define function) doit être déterminée, proposée et réalisée par le Titulaire en fonction du besoin métier.

[FIN]

4.5 Stockage des données traitées

[EXI:PDS_GPE_4-128]

Pour le stockage des données traitées, le Titulaire peut s'appuyer sur les services Azure que ce soit pour les données structurées et non structurées.

Les solutions et moyens de stockages doivent être disponibles, sécurisées, ils doivent intégrer des mécanismes de backup et de restauration.

[FIN]

4.6 Visualisation et reporting

[EXI:PDS_GPE_4-129]

Pour l'analyse et la visualisation des données, le Titulaire peut par exemple utiliser Power BI. Cela comprend la création de tableaux de bord interactifs et de rapports dynamiques.

[FIN]

4.7 Gouvernance des données

[EXI:PDS_GPE_4-130]

Pour une meilleure prise de décision, la gouvernance de données est nécessaire dans le cadre de cette plateforme. Cette gouvernance permet de sécuriser les données, d'assurer le respect des réglementations et des lois sur la confidentialité de ces données, d'améliorer la qualité des données manuelles. Afin de répondre à ce besoin et de maîtriser la donnée, le Titulaire doit donc proposer une solution interopérable avec les autres composants de la plateforme des données GPE.

[FIN]

4.8 Documentation, formation et support

[EXI:PDS_GPE_4-131]

Le Titulaire fournit une description détaillée de l'utilisation prévue des outils de la suite logicielle, en démontrant comment ces outils seront utilisés pour atteindre les objectifs du Marché. Des rapports réguliers sur l'utilisation et la performance de ces outils sont également proposés durant l'exécution du Marché.

[FIN]

[EXI:PDS_GPE_4-132]

Le Titulaire doit s'assurer que les utilisateurs finaux disposent des compétences nécessaires pour utiliser les outils de la suite logicielle, en organisant des sessions de formation appropriées. Un

support technique devra être mis en place pour répondre aux questions relatives à l'utilisation de ces outils.

[FIN]

5 MAINTIEN EN CONDITION OPERATIONNELLE (MCO)

[EXI:PDS_GPE_5-001]

Le Titulaire est responsable du **Maintien en Condition Opérationnelle (MCO)** des systèmes et infrastructures de la plateforme de données de la SGP, garantissant ainsi leur disponibilité, leur performance, et leur sécurité. Cela inclut la surveillance continue des systèmes pour détecter et résoudre rapidement les anomalies, la gestion proactive des mises à jour logicielles et des correctifs de sécurité, ainsi que l'optimisation des performances pour répondre aux besoins d'évolution de la SGP.

[FIN]

[EXI:PDS_GPE_5-002]

Le Titulaire doit également assurer la gestion des sauvegardes régulières, la validation des procédures de reprise d'activité en cas d'incident, et la documentation systématique des interventions réalisées. Il est chargé d'assurer la conformité aux normes de sécurité tout en garantissant une continuité de service sans interruption. Le MCO comprendra également l'assistance aux utilisateurs, la gestion des accès, et l'amélioration continue des systèmes pour anticiper les futurs besoins opérationnels.

[FIN]

[EXI:PDS_GPE_5-003]

Pour chacune des sections ci-dessous, le Titulaire est tenu de fournir un document détaillant de manière exhaustive l'approche méthodologique qu'il entend adopter pour traiter ces différents aspects. Ce document doit inclure une description des étapes envisagées, des outils et des technologies utilisés, ainsi que des livrables prévus. De plus, il est attendu que le Titulaire précise les critères d'évaluation des résultats obtenus pour chaque partie, afin d'assurer une transparence et une traçabilité optimale du processus.

[FIN]

5.1 Maintenance corrective, mise à jour et évolution des logiciels

[EXI:PDS_GPE_5-004]

Le Titulaire doit garantir que les logiciels utilisés par la SGP sont régulièrement mis à jour pour intégrer les dernières fonctionnalités, correctifs de sécurité, et améliorations de performance. Pour cela, le Titulaire doit assurer la mise en place d'une organisation permettant l'intervention rapide pour corriger les anomalies et les dysfonctionnements signalés par les utilisateurs ou détectés par les systèmes de surveillance.

[FIN]

[EXI:PDS_GPE_5-005]

Il est attendu du Titulaire une description détaillée des éléments ci-dessous :

Temps de réponse : Voir paragraphe 5.2 ci-dessous (SLA) et tableau associé sur les engagements sur un temps de réponse selon le niveau de criticité de l'anomalie.

Processus de résolution : Description du processus de résolution des incidents, y compris l'analyse, la correction, les tests et le déploiement.

De manière générale, ces éléments doivent constituer le plan de reprise d'activité que mettra en place le Titulaire. Ce plan vise à restaurer les services et les opérations après un incident majeur ou une panne qui a interrompu le fonctionnement normal des systèmes. Le PRA est activé après qu'un événement perturbateur a eu lieu, pour récupérer les données et relancer les activités.

Patch Management : Le Titulaire doit assurer une gestion complète des patchs qui permettent à la plateforme de données d'être performante et à jour d'un point de vue technique, fonctionnelle et de sécurité. À ce titre, le Titulaire doit assurer une surveillance régulière des systèmes pour identifier les nouvelles mises à jour de sécurité, correctifs logiciels et patches publiés par les fournisseurs.

[FIN]

[EXI:PDS_GPE_5-006]

Comme pour la gestion des évolutions, le Titulaire a la charge de réaliser les macro-activités ci-dessous :

Planification des mises à jour : Établir un calendrier de mises à jour pour les logiciels, incluant l'identification des nouvelles versions disponibles, des correctifs de sécurité, et des mises à jour majeures. La planification doit prendre en compte les priorités de la SGP et ses contraintes opérationnelles.

Exécution des mises à jour : Mettre en œuvre les mises à jour logicielles conformément au plan établi, incluant l'installation des nouvelles versions, l'application des correctifs de sécurité, et la gestion des dépendances. Cette activité comprend également la vérification de la compatibilité des mises à jour avec l'infrastructure existante et la résolution des éventuels conflits ou problèmes post-mise à jour.

Évaluation et documentation des évolutions : Après chaque mise à jour, évaluer l'impact des modifications sur les performances et la sécurité des logiciels. Documenter les nouvelles fonctionnalités, les améliorations apportées, et les instructions spécifiques pour les utilisateurs et les administrateurs. Cette documentation doit également inclure un suivi des versions et des changements pour assurer une traçabilité complète des évolutions logicielles.

[FIN]

5.2 SLA

[EXI:PDS_GPE_5-007]

Les SLAs (Service Level Agreement ou Engagements de Services) attendus en fonction des types d'anomalie sont les suivants :

Type	Définition	Durée de résolution (en jours ouvrés)	Délai de contournement
Bloquante	Anomalie qui rend la plateforme complètement inopérante et pour laquelle il n'existe aucune solution palliative ou de contournement	2 jours	1 jour
Majeure	Anomalie qui dégrade de manière significative le fonctionnement général de la plateforme ou altère de manière significative les fonctions essentielles du logiciel mentionnées dans la documentation	5 jours	/
Mineure	Anomalie ayant pour effet d'altérer le fonctionnement du service, mais n'empêchant pas son utilisation	10 jours	/

Ces éléments sont proposés par la SGP mais le Titulaire pourra proposer une autre démarche au sein de sa réponse technique. En ce sens, la nouvelle démarche et éléments associés seront précisés et amandés à l'issu du choix du Titulaire.

[FIN]

[EXI:PDS_GPE_5-008]

Exemples de livrables qui pourront être produits. La liste précise est convenue en amont avec la SGP :

Prestations	Livrables
Planification des mises à jour	<ul style="list-style-type: none"> Calendrier des mises à jour Rapport d'analyse des versions disponibles et des besoins Plan de gestion des interruptions de service
Exécution des mises à jour	<ul style="list-style-type: none"> Rapport de mise à jour des logiciels

Prestations	Livrables
	<ul style="list-style-type: none"> Journal des correctifs appliqués et des nouvelles versions installées Plan de reprise d'activité en cas d'échec de la mise à jour
Évaluation et documentation des évolutions	<ul style="list-style-type: none"> Rapport d'évaluation post-mise à jour Documentation des nouvelles fonctionnalités et des améliorations Historique des versions et suivi des modifications
Intervention rapide pour corriger les anomalies et les dysfonctionnements signalés par les utilisateurs ou détectés par les systèmes de surveillance	<ul style="list-style-type: none"> Registre des incidents Rapports d'intervention Documentation de correction

[FIN]

5.3 Sécurité et sauvegarde des données

[EXI:PDS_GPE_5-009]

Le Titulaire doit tout mettre en œuvre pour assurer la sécurité de l'infrastructure de la plateforme de données de la SGP, tout en assurant la disponibilité et l'intégrité des données grâce à des stratégies de sauvegarde robustes. Cette prestation vise à mettre en place des mesures de sécurité et à garantir que les données peuvent être restaurées de manière fiable en cas d'incident.

[FIN]

[EXI:PDS_GPE_5-010]

Il est attendu du Titulaire une description détaillée des éléments ci-dessous :

Évaluation de la sécurité : Identifier les vulnérabilités potentielles et les risques de sécurité. Cela inclut la réalisation de tests de pénétration et l'évaluation de la conformité aux normes de sécurité.

Mise en place des mesures de sécurité : Implémenter des contrôles de sécurité pour protéger les données et l'infrastructure.

Sauvegarde et restauration : Mettre en œuvre des stratégies de sauvegarde régulières pour garantir la protection des données. Cela comprend la configuration des solutions de sauvegarde, la planification des cycles de sauvegarde, la gestion des sauvegardes externes, et la réalisation de tests de restauration pour s'assurer que les données peuvent être récupérées.

[FIN]

[EXI:PDS_GPE_5-011]

Exemples de livrables qui pourront être produits. La liste précise est convenue en amont avec la SGP :

Activités	Livrables
Évaluation de la sécurité	<ul style="list-style-type: none">• Rapport d'évaluation des vulnérabilités et des risques• Plan de sécurité et de conformité• Résultats des tests de pénétration
Mise en place des mesures de sécurité	<ul style="list-style-type: none">• Documentation des configurations de sécurité• Politique de gestion des accès et des autorisations• Plan de réponse aux incidents de sécurité
Sauvegarde et restauration	<ul style="list-style-type: none">• Plan de sauvegarde des données, incluant les fréquences et les méthodes• Procédures de restauration des données et de reprise après sinistre• Rapport de test des procédures de sauvegarde et de restauration

[FIN]

5.4 Gestion des utilisateurs et des accès

[EXI:PDS_GPE_5-012]

Le Titulaire doit mettre en place des systèmes et des procédures pour contrôler l'accès aux ressources et aux données de la plateforme de données de la SGP. Cela inclut la gestion des identités, l'assignation des permissions appropriées, et la surveillance des activités des utilisateurs.

[FIN]

[EXI:PDS_GPE_5-013]

Il est attendu du Titulaire une description détaillée des éléments ci-dessous :

Processus de gestion des accès : Procédures pour l'ajout, la modification et la suppression des accès

Audit des accès : Réalisation d'audits trimestriels pour vérifier la conformité des accès.

[FIN]

[EXI:PDS_GPE_5-014]

Le Titulaire a la charge de réaliser les macro-activités ci-dessous :

Cadrage des politiques d'accès : Établir des politiques pour la gestion des accès, définissant les rôles et les permissions associés. Cette activité inclut l'analyse des besoins d'accès des différents utilisateurs, la définition des niveaux d'accès requis, et la mise en place de procédures de création, de modification et de suppression des comptes utilisateurs.

Implémentation des contrôles d'accès : Mettre en œuvre des mécanismes de contrôle d'accès. Cette phase comprend également la configuration des systèmes de gestion des identités pour automatiser et sécuriser les processus de gestion des utilisateurs et des droits d'accès.

Surveillance et audit des accès : Mettre en place des systèmes de surveillance pour enregistrer et analyser les activités des utilisateurs sur la plateforme, afin de détecter les comportements anormaux ou non autorisés. Cette activité comprend la génération de rapports d'accès, la réalisation d'audits de sécurité réguliers et l'application de mesures correctives en cas de violation des politiques d'accès.

[FIN]

[EXI:PDS_GPE_5-015]

Exemples de livrables qui pourront être produits. La liste précise est convenue en amont avec la SGP :

Activités	Livrables
Cadrage des politiques d'accès	<ul style="list-style-type: none">Politique de gestion des identités et des accèsMatrice des rôles et des permissionsProcédures de gestion des comptes utilisateurs
Implémentation des contrôles d'accès	<ul style="list-style-type: none">Documentation de l'implémentation des contrôles d'accèsGuide d'utilisation du système de gestion des identitésProcédures de gestion des accès et d'authentification
Surveillance et audit des accès	<ul style="list-style-type: none">Rapports de surveillance des activités des utilisateursRésultats des audits de sécurité et de conformité des accèsRapport de suivi des incidents d'accès et mesures correctives appliquées

[FIN]

5.5 Suivi financier de la consommation du cloud

[EXI:PDS_GPE_5-016]

Le Titulaire doit garantir une gestion efficace des ressources cloud utilisées par la plateforme de données de la SGP. Cette prestation implique la surveillance continue de la consommation des

services cloud, l'analyse des dépenses pour identifier les tendances et les opportunités d'optimisation, et la mise en œuvre de stratégies visant à minimiser les coûts tout en maximisant l'efficacité des ressources.

[FIN]

[EXI:PDS_GPE_5-017]

Il est attendu du Titulaire une description détaillée des éléments ci-dessous :

Stratégie visant à minimiser les coûts : Détailler les approches et les outils utilisés pour réduire les dépenses liées aux services cloud tout en maintenant les performances requises.

Méthode de surveillance continue : Expliquer les processus et les technologies mis en place pour surveiller en temps réel l'utilisation des ressources cloud et détecter toute anomalie ou dérive.

Plan de communication pour le suivi de la consommation : Présenter le plan de communication prévu pour informer régulièrement les parties prenantes de la consommation des ressources, des coûts associés, et des mesures correctives si nécessaire.

Surveillance de la consommation : Mettre en place des outils et des processus pour surveiller en temps réel l'utilisation des ressources cloud, incluant le suivi des services consommés, des volumes de données stockés, et des instances de calcul utilisées. Cette activité inclut également l'identification des services surutilisés ou sous-utilisés pour optimiser les ressources.

Analyse des coûts : Analyser les coûts associés à la consommation des services cloud par brique fonctionnelle de la plateforme de données. Cette analyse permet d'identifier les postes de dépense les plus élevés et les tendances de consommation.

Optimisation et recommandations : Proposer des stratégies et des actions pour optimiser l'utilisation des ressources cloud. Fournir des recommandations pour réduire les coûts, améliorer l'efficacité et ajuster les budgets en conséquence.

[FIN]

[EXI:PDS_GPE_5-018]

Exemples de livrables qui pourront être produits. La liste précise est convenue en amont avec la SGP :

Activités	Livrables
Surveillance de la consommation	<ul style="list-style-type: none">Tableau de bord de surveillance de la consommation cloudRapports mensuels de consommation des ressources cloud

Activités	Livrables
	<ul style="list-style-type: none"> Liste des ressources sous-utilisées ou inutilisées
Analyse des coûts	<ul style="list-style-type: none"> Rapports détaillés des coûts par brique fonctionnelle Analyse comparative des dépenses réelles par rapport aux prévisions budgétaires Identification des tendances de consommation et des coûts associés
Optimisation et recommandations	<ul style="list-style-type: none"> Plan d'optimisation des coûts cloud Recommandations pour la réduction des coûts Stratégie de gestion des ressources et ajustements budgétaires proposés

[FIN]

5.6 Support utilisateur et assistance technique

[EXI:PDS_GPE_5-019]

Le Titulaire doit fournir un support réactif et efficace aux utilisateurs de la plateforme, ainsi qu'une assistance technique pour résoudre les incidents, répondre aux questions et faciliter l'usage optimal de la plateforme.

[FIN]

[EXI:PDS_GPE_5-020]

Il est attendu du Titulaire une description détaillée des éléments ci-dessous :

Niveaux de support : Distinguer les différents niveaux de support (niveau 1, 2, 3) avec des descriptions claires de ce qui est couvert à chaque niveau.

Canaux de communication : Décrire les différents moyens de contacter le support (téléphone, email, chat, portail web) et les horaires de disponibilité.

[FIN]

[EXI:PDS_GPE_5-021]

Exemples de livrables qui pourront être produits. La liste précise est convenue en amont avec la SGP :

Activités	Livrables
Support utilisateur	<ul style="list-style-type: none"> Guide d'utilisation Documentations des bonnes pratiques et FAQ

	<ul style="list-style-type: none"> • Rapport de satisfaction utilisateur
Assistance technique	<ul style="list-style-type: none"> • Rapport mensuel des incidents et des résolutions • Processus de gestion des tickets

[FIN]

5.7 Monitoring de la plateforme de données

[EXI:PDS_GPE_5-022]

Le Titulaire doit assurer le monitoring de la plateforme de données en fournissant une surveillance en temps réel, une gestion des alertes, des rapports, et une prise en charge des incidents.

[FIN]

[EXI:PDS_GPE_5-023]

Il est attendu du Titulaire une description détaillée des éléments ci-dessous :

Outils et technologies utilisés : Les outils de monitoring que le Titulaire prévoit d'utiliser et préciser les méthodes d'intégration de ces outils avec les composants de la plateforme.

Stratégie de surveillance : La stratégie de monitoring, y compris les métriques surveillées, la fréquence des vérifications et les seuils d'alerte définis.

Reporting et analyse : Les types de rapports que vous fournirez (rapports quotidiens, hebdomadaires, mensuels, etc.). Les indicateurs clés de performance (KPI) utilisés pour évaluer la santé de la plateforme. Les outils ou tableaux de bord utilisés pour le reporting et leur accessibilité pour les équipes de supervision.

[FIN]

[EXI:PDS_GPE_5-024]

Exemples de livrables qui pourront être produits. La liste précise est convenue en amont avec la SGP :

Activités	Livrables
Outils et technologies utilisés	<ul style="list-style-type: none"> • Schéma d'intégration des outils avec les composantes de la plateforme • Documentation des capacités de chaque outil en termes de détection, performance et sécurité
Stratégie de surveillance	<ul style="list-style-type: none"> • Plan de surveillance détaillé avec les métriques surveillées • Fréquence des vérifications et seuils d'alerte documentés

	<ul style="list-style-type: none"> • Tableau de bord de surveillance en temps réel
Reporting et analyse	<ul style="list-style-type: none"> • Rapports périodiques (quotidiens, hebdomadaires, mensuels) sur l'état de santé de la plateforme • Analyse des incidents détectés et des actions correctives • Indicateurs clés de performance (KPI) pour l'évaluation continue

[FIN]

6 EXIGENCES RELATIVES AU MANAGEMENT DE PROJET

6.1 Organisation projet

[EXI:PDS_GPE_6-001]

Exigence : Le Titulaire décrit l'organisation projet qu'il va mettre en place pour prendre en charge l'administration technique de la plateforme de donnée.

[FIN]

[EXI:PDS_GPE_6-002]

Il est attendu du Titulaire une description détaillée des éléments ci-dessous :

Structure de l'équipe : Présentation de l'équipe dédiée avec les rôles et responsabilités de chaque membre

Outils de gestion de projet : Liste des outils utilisés

Procédures de communication : Fréquence des réunions de suivi, canaux de communication utilisés, rapport de statut mensuel

[FIN]

6.2 Participation aux ateliers collaboratifs à la demande de la SGP

[EXI:PDS_GPE_6-003]

Exigence : Le Titulaire doit participer aux ateliers collaboratifs à la demande de la SGP pour accompagner à l'identification et à la priorisation des cas d'usage métier en s'appuyant sur toutes les parties prenantes pertinentes. La participation du Titulaire à ces ateliers est comprise dans le prix global et ne donne pas lieu à une rémunération complémentaire.

[FIN]

[EXI:PDS_GPE_6-004]

Les livrables attendus sont :

Agenda des ateliers : Doit être fourni au minimum une semaine avant chaque atelier.

Comptes rendus des ateliers : À remettre dans les 48 heures suivant chaque atelier.

Liste des cas d'usage identifiés : Mise à jour après chaque atelier.

Matrice de priorisation des cas d'usage : Revue et validée par les parties prenantes dans la semaine suivant l'atelier.

[FIN]

6.3 Reporting et suivi des indicateurs

[EXI:PDS_GPE_6-005]

Exigence : Le Titulaire fournit des rapports réguliers sur l'avancement du projet et le respect des indicateurs de performance.

[FIN]

[EXI:PDS_GPE_6-006]

Il est attendu du Titulaire une description détaillée des éléments ci-dessous :

Fréquence des rapports : Rapports hebdomadaires et mensuels.

Contenu des rapports : Avancement des tâches, respect des délais, gestion des risques, et points bloquants.

Indicateurs de performance : Définition et suivi des KPIs pertinents.

[FIN]

6.4 Proposition technique pour le développement, le maintien ou l'optimisation de la plateforme de données

[EXI:PDS_GPE_6-007]

Exigence : Tout au long de la prestation et sur demande de la SGP, le Titulaire doit fournir des propositions techniques détaillées couvrant les aspects suivants :

Architecture de la plateforme : Description de l'architecture et des modifications proposées.

Améliorations fonctionnelles : Propositions d'améliorations fonctionnelles en réponse aux besoins métiers évolutifs.

Optimisations de performance : Techniques et outils pour optimiser les performances de la plateforme.

Sécurité : Mesures de sécurité mises en place pour protéger les données.

[FIN]

6.5 Pipeline de livraison

[EXI:PDS_GPE_6-008]

Le Titulaire s'engage à assurer des livraisons régulières et fonctionnelles en s'appuyant sur les expressions de besoin métiers et en respectant les contraintes techniques définies. Cette exigence inclut :

Livraisons incrémentales : Le Titulaire doit planifier et effectuer des livraisons régulières.

Respect des délais : Chaque livraison doit être effectuée dans les délais définis et validés par la SGP.

Qualité des livrables : Chaque livraison doit être fonctionnelle, testée et répondre aux critères de qualité définis dans les spécifications techniques.

Amélioration continue : Le Titulaire doit organiser des revues régulières avec les parties prenantes pour valider les livraisons, recueillir les retours et ajuster les développements futurs en conséquence.

[FIN]

6.6 Qualité des livrables

[EXI:PDS_GPE_6-009]

Le Titulaire doit s'assurer que tous les livrables fournis respectent les standards de qualité définis par la SGP. Cette exigence inclut :

Conformité : Les livrables doivent être conformes aux spécifications techniques et fonctionnelles validées.

Documentation : Chaque livraison doit être accompagnée de la documentation nécessaire (manuel utilisateur, documentation technique, guides de déploiement, etc.)

Tests : Chaque livrable doit être testé et validé avant livraison, avec les rapports de tests fournis à la SGP.

Validation SGP : Les livrables doivent être validés par la SGP avant leur mise en production.

[FIN]

7 MODALITES D'EXECUTION DES PRESTATIONS

7.1 Organisation au sein de la Société des grands projets

L'interlocuteur privilégié du Titulaire au sein de la Maîtrise d'Ouvrage est le Directeur des Systèmes de Transport et Exploitation ou la personne qu'il désigne.

Des référents métiers peuvent également être amenés à communiquer avec le Titulaire.

7.2 Organisation attendue du Titulaire

[EXI:PDS_GPE_7-001]

Le Titulaire affecte à la mission un chef de projet qui sera l'interlocuteur unique de la SGP. Le chef de projet du Titulaire mobilise au moment opportun les ressources nécessaires en qualité et en quantité afin de pouvoir réaliser toutes les prestations prévues au titre de la mission et garantir leur qualité ainsi que le respect du planning déterminé dans le cadre des bons de commandes.

[FIN]

[EXI:PDS_GPE_7-002]

Le chef de projet est le garant du bon déroulement de la mission dans son ensemble. Son expertise dans le traitement des données, dans les problématiques liées aux systèmes de transport et de l'infrastructure cloud, sa force de proposition et son niveau de responsabilité doivent lui permettre de prendre toutes les décisions nécessaires pour le bon déroulement du planning ou l'engagement de ressources adéquates.

[FIN]

[EXI:PDS_GPE_7-003]

À ce titre, il a pour responsabilité :

- Le pilotage opérationnel des différentes phases du projet ;
- Définir les charges, le planning et l'organisation des différentes phases du projet ;
- Contrôler l'état d'avancement de chaque phase ;
- Proposer ou prendre les mesures nécessaires pour que l'avancement et la charge soient cohérents avec les objectifs du projet ;
- Veiller au bon déroulement de toutes les phases du projet ;
- Coordonner ses équipes et celle de l'éditeur ;
- Suivre les études et les développements qui lui sont confiés ;
- Alerter le responsable SGP le plus en amont possible en cas de problème.

[FIN]

7.3 Gouvernance et comitologie

7.3.1 Gouvernance

[EXI:PDS_GPE_7-004]

Dès la notification du marché, le Titulaire désigne un responsable de compte qui deviendra l'interlocuteur privilégié de la SGP. Le responsable de compte doit être muni des pouvoirs nécessaires pour prendre toutes décisions utiles, signer tout document, donner toutes instructions au personnel de son entreprise, assister aux réunions, etc...

[FIN]

[EXI:PDS_GPE_7-005]

Le responsable de compte a pour rôle d'assurer la mise en place et le suivi du marché. À ce titre, il doit coordonner l'action de ses intervenants et s'assurer que ces derniers respectent les spécifications du marché, ainsi que les éventuelles consignes qui pourraient être données par la SGP.

[FIN]

7.3.2 Comitologie

[EXI:PDS_GPE_7-006]

Les instances à organiser et le reporting associé à fournir sont :

Comité	Fréquence	Objectifs	Participants	Livrables attendus du Titulaire	Durée
Comité de projet	Bi mensuelle	Revue des devis en cours Premier niveau d'escalade Informations spécifiques sur les éditeurs couverts Évaluation de la conformité SGP (notamment en cas d'évolution des métriques de licence) Prendre les décisions sur les orientations en cours Revu des objectifs en cours Planning en cours	Titulaire : Chef de projet Invitation ad hoc d'experts si nécessaire. SGP : Chef de projet Gestionnaire de marché	Support de comité Compte-rendu de réunion	2h
Comité de pilotage	Trimestrielle	Point sur les Coûts, Qualité et Délais Gestion d'escalades le cas échéant Calendrier prévisionnel de renouvellement de contrat de licence	Titulaire : Responsable de compte, Directeur commercial et Directeur des Opérations SGP : Chef de projet Gestionnaire de marché	Support de comité Compte-rendu de réunion	2h

		Évolutions des programmes de licences des éditeurs	DSI		
Comité Stratégique	Annuelle	Revue de l'activité de la période écoulée : bilan annuel Prospective sur les évolutions d'organisation/besoins réciproques Consolidation des mesures de performance Échange sur les Best Practices, innovations, améliorations possibles Synthèse des KPI	Titulaire : DG Titulaire SGP : Responsable de STE Idem comité de revue de pilotage	Support de comité Compte-rendu de réunion	2h

[FIN]

[EXI:PDS_GPE_7-007]

Les instances et la description du contenu des livrables est précisé au PAQ. Il est attendu du Titulaire qu'il fournisse certaines informations nécessaires au pilotage des actifs logiciels par la SGP.

[FIN]

7.4 Outil mis à disposition de la SGP dans le cadre du suivi de projet

7.4.1 Journal des modifications

[EXI:PDS_GPE_7-008]

Dans le cadre du suivi de projet, le Titulaire doit fournir un outil/document de suivi de l'ensemble des modifications apportées au systèmes, les nouvelles fonctionnalités, les corrections de bugs, les améliorations.

[FIN]

[EXI:PDS_GPE_7-009]

À chaque nouvelle version majeure déployée, un document de l'état du journal des modifications doit être enregistré dans l'outil de Gestion Documentaire de la SGP.

[FIN]

7.4.2 Suivi des expressions de besoin et recueil des anomalies

[EXI:PDS_GPE_7-010]

Le Titulaire propose à la SGP un outil permettant aux utilisateurs d'exprimer de nouveaux besoins et/ou de remonter des anomalies logicielles. Le suivi des besoins et des anomalies est réalisé au cours des comités projets.

[FIN]

7.5 Exigences qualités au titre du marché

7.5.1 Plan d'assurance sécurité (PAS)

[EXI:PDS_GPE_7-011]

Un Plan d'Assurance sécurité (PAS) traduit la mise en application de la politique sécurité. Ce document doit être rédigé en version opérationnelle par le Titulaire et validé par la SGP à l'issue de la phase de prise de connaissance.

[FIN]

[EXI:PDS_GPE_7-012]

En matière de sécurité, le Titulaire doit garantir une maîtrise totale des règles applicables en matière de droit d'accès, confidentialité et l'ensemble de la gestion des droits applicables aux différents périmètres du présent accord cadre.

[FIN]

7.5.2 Plan d'assurance qualité (PAQ)

[EXI:PDS_GPE_7-013]

Un Plan d'Assurance Qualité (PAQ) traduit la mise en application de la politique qualité de la SGP. Ce document doit être rédigé en version opérationnelle par le Titulaire et validé par la SGP à l'issue de la phase de prise de connaissance.

[FIN]

[EXI:PDS_GPE_7-014]

Le PAQ peut faire l'objet d'adaptation lors de l'émission d'un bon de commande. Le contenu du document ne pourra pas s'écarter du cadre initial. Le Titulaire ne pourra soustraire de contenu au document ou le modifier d'une manière contraire au présent programme fonctionnel.

[FIN]

[EXI:PDS_GPE_7-015]

La SGP attend du Titulaire des orientations, recommandations, proposition de solutions, des méthodes, qui démontrent la prise en compte des exigences telles que formulées dans le présent document et qui seront reprises et complétées dans le PAQ.

[FIN]

[EXI:PDS_GPE_7-016]

La qualité des prestations du Titulaire et la satisfaction du maître d'ouvrage seront appréciées, au regard des critères suivants (à détailler dans le PAQ) :

- Le respect des coûts ;
- Le respect des délais ;
- Le respect de la complétude de la fourniture ;
- La qualité des livrables ;
- L'apport de valeur (innovation, inspiration, créativité, ...) ;
- Le respect de la démarche qualité telle que décrite dans le PAQ ;
- Le respect des normes et processus en vigueur au sein de la Société des grands projets ;
- L'expertise et le dimensionnement de la Société des grands projets ;
- La clarté, la lisibilité et la complétude de la documentation produite en langue française.

L'appréciation de la qualité des prestations permet de déterminer les axes d'amélioration à mettre en œuvre en cours d'exécution.

[FIN]

7.6 Niveaux de séniorité des profils

[EXI:PDS_GPE_7-017]

Les niveaux de séniorité associés à chaque profil sont les suivants :

- **Junior** : 1 à 3 ans dans un poste associé au profil sur un projet similaire correspondent à un profil junior sur l'activité ;
- **Confirmé** : supérieur à 3 ans et jusqu'à 7 ans dans un poste associé au profil correspondant sur un projet similaire correspondant à un profil confirmé sur l'activité ;
- **Sénior** : supérieur à 7 ans dans un poste associé au profil sur un projet similaire et correspondant à un profil senior sur l'activité ;

[FIN]

8 LISTE DES SIGLES ET ABREVIATIONS

Les acronymes utilisés dans ce document sont les suivants :

Acronyme	Description
2D / 3D	en 2 Dimensions / en 3 Dimensions
AC	Automatismes de Conduite
BD	Base(s) de Données
BIM	Building Information Model/Modeling/Management
BPU	Bordereau des Prix Unitaires
CAO	Conception Assistée par Ordinateur
CC	Commandes Centralisées
CCAP	Cahier des Clauses Administratives Particulières
CCTP	Cahier des Clauses Techniques Particulières
CTEVP	Commission Technique Essais Vérification & Performance
DCE	Dossier de Consultation des Entreprises
DMARC	Message Authentication Reporting et Conformance
DMZ	Zone démilitarisée (sous-réseau informatique sécurisé)
DSI	Direction des Systèmes d'Informations (SGP)
EF	Expert Fonctionnel (DSI)
ETL	Extract Transform Load (Extraction, transformation, chargement)
EXE	Phase « Exécution » du Marché
FMDs	Fiabilité, Maintenabilité, Disponibilité et Sécurité
FdQ	Façades de quai
FRACAS	Failure Reporting, Analysis, and Corrective Action System
GED / GDC	Gestion Électronique de Documents / Gestion De Configuration
GMAO	Gestion de la Maintenance Assistée par Ordinateur
GO	Groupe d'Ouvrage
GPE	Grand Paris Express
GTD	Garantie des Temps de Détection
GTI	Garantie des Temps d'Intervention
GTR	Garantie des Temps de Rétablissement
IdFM	Île-de-France Mobilités

Acronyme	Description
IHM	Interface Homme-Machine
MCO	Maintien en Condition Opérationnelle
MOA	Maitrise d’Ouvrage
MOES	Maîtrise d’Œuvre des Systèmes
MR / AC	Matériel Roulant / Automatismes de conduite
MRV	Matériel Roulant Voyageurs
PAQ	Plan d’Assurance Qualité
PAS	Plan d’Assurance Sécurité
PCC	Poste de Commandes Centralisées
PDMA	Perte de données maximale admissible
PFS	Perfect Forward Secrecy - Confidentialité persistante
RATP-I	RATP Infrastructures
RGPD	Règlement Général sur la Protection des Données
RTPGP	Réseau de Transport Public du Grand Paris
SGP	Société des grands projets
SLA	Service Level Agreement (Engagements de Services)
STE	Systèmes de Transport et Exploitation
UO	Unités d’Œuvre
VA	Vérification d’Aptitude
VSR	Vérification de Service Régulier

9 LISTE DES DOCUMENTS ANNEXES

- **Annexe 1** : Matrice des exigences numérotées (DSTE_06_ACT_STE_002361_1)
- **Annexe 2** : Note d'Information sur le suivi opérationnel FMD (PN2030-1_06_HPH_NOT_000027_3)
- **Annexe 3** : Référentiel des données du GPE (UMQO_02_HPH_DRF_000003_5)
- **Annexe 4** : Délais et jalons (DSTE_06_ACT_LIS_002402_1)