



Identifiant de l'acte délivré par la préfecture :
083-248300543-20250120-lmc1362046A-DE-1-1
Date de validation par la préfecture : mardi 21 janvier 2025
Date de publication : 21/01/2025

**BUREAU METROPOLITAIN DU
LUNDI 20 JANVIER 2025**

NOMBRE D'ELUS METROPOLITAINS EN EXERCICE : 16		
QUORUM : 9		
PRESENTS	REPRESENTES	ABSENTS
15	0	1
OBJET DE LA DECISION		
N° 25/38		
APPROBATION DE LA CONVENTION-CADRE D'ECHANGE ET DE GEO- MUTUALISATION AVEC LES PARTENAIRES DE LA METROPOLE TOULON PROVENCE MEDITERRANEE 2024-2030		

Le Bureau Métropolitain de la Métropole TOULON PROVENCE MEDITERRANEE régulièrement convoqué, a été assemblé sous la présidence de Monsieur Jean-Pierre GIRAN.

PRESENTS :

M. Thierry ALBERTINI, Mme Hélène ARNAUD-BILL, M. Robert BENEVENTI, Mme Nathalie BICAIS, M. Robert CAVANNA, M. Jean-Pierre GIRAN, M. Arnaud LATIL, Mme Geneviève LEVY, M. Cheikh MANSOUR, Mme Josée MASSI, M. Jean-Louis MASSON, M. Ange MUSSO, M. Francis ROUX, M. Hervé STASSINOS, M. Gilles VINCENT.

ABSENT :

M. Jean-Sébastien VIALATTE.

DÉCISION MÉTROPOLITAINE

N° 25/38

BUREAU DU 20 JANVIER 2025

**O B J E T : APPROBATION DE LA CONVENTION-CADRE
D'ECHANGE ET DE GEO-MUTUALISATION AVEC LES
PARTENAIRES DE LA METROPOLE TOULON
PROVENCE MEDITERRANEE 2024-2030**

LE BUREAU MÉTROPOLITAIN,

VU le Code Général des Collectivités Territoriales,

VU le décret n°2017-1758 en date du 26 décembre 2017 portant création de la
Métropole Toulon Provence Méditerranée,

VU la délibération n°23/05/078 du 4 mai 2023 portant délégations au Président et au
Bureau,

VU la délibération n° 13/12/241 du 12 décembre 2013 portant mise en commun des services informatiques et systèmes informatiques géographiques et création d'une direction commune des systèmes d'information entre la Communauté d'Agglomération Toulon Provence Méditerranée et la ville de Toulon,

VU l'avenant n°1 acté par délibération n° 14/12/261 du 12 décembre 2014 précisant que l'ensemble des dépenses de la DCSI (commun, spécifique Ville, spécifique TPM) sont portés par la Communauté d'Agglomération Toulon Provence Méditerranée et la ville de Toulon,

VU la délibération n°18/12/390 du 18 décembre 2018 portant mise en commun des services informatiques et systèmes informatiques géographiques et création d'une Direction Ressources Numériques Mutualisées entre la Métropole TPM et la Ville de Toulon,

CONSIDERANT la démarche engagée par La Métropole Toulon Provence Méditerranée consistant à développer un système d'Information Géographique mutualisé avec ses partenaires,

CONSIDERANT qu'il convient de formaliser et poursuivre cette démarche de mutualisation en matière d'information géographique,

CONSIDERANT que cette mutualisation permet de :

- Favoriser les échanges, éviter les doublons, mobiliser et mutualiser prioritairement les connaissances disponibles sur le territoire métropolitain
- Réduire des coûts et utiliser aux mieux les fonds publics consacrés à la production de l'information géographique
- Partager l'expérience et les savoir-faire, et participer à l'enrichissement mutuel des informations géographiques
- Mettre à disposition des partenaires l'information géographique disponible sur le territoire,

CONSIDERANT que La Métropole Toulon Provence Méditerranée animera et coordonnera l'ensemble du dispositif de mutualisation et organisera une réunion à l'échéance de la présente convention,

CONSIDERANT que La Métropole Toulon Provence Méditerranée met à disposition des partenaires, adhérents à la convention cadre, les données géographiques référentielles, les données géographiques mutualisées ainsi qu'une plateforme extranet avec accès sécurisé en mode web,

CONSIDERANT que le portail DATA, outil d'accès aux données géographiques, mis à disposition par La Métropole Toulon Provence Méditerranée, est le fruit d'une première collaboration entre La Métropole Toulon Provence Méditerranée et ses partenaires suite aux travaux d'un groupe de travail constitué de volontaires,

CONSIDERANT que les partenaires adhérents à la convention cadre s'efforceront de rendre disponible aux membres du réseau, les informations géographiques dont ils sont dépositaires ; dans le respect des dispositions légales et réglementaires dont elles font l'objet, des principes énoncés et des droits éventuels de tiers,

CONSIDERANT que l'adhésion des personnes publiques à la présente convention cadre est soumise à l'autorisation préalable de leur assemblée délibérante, selon les règles propres à chacune d'elles,

CONSIDERANT que la réception par La Métropole Toulon Provence Méditerranée de la délibération prise par chaque personne publique acte son adhésion à la convention,

CONSIDERANT que tout partenaire adhérent peut se retirer de la convention. La demande de retrait du groupement est adressée à La Métropole Toulon Provence Méditerranée par lettre recommandée avec accusé de réception au plus tard un mois après que les instances compétentes du partenaire se soient prononcées en ce sens, en utilisant l'annexe 7,

CONSIDERANT que pour chaque commune de La Métropole Toulon Provence Méditerranée, cette convention cadre pourra être complétée de conventions spécifiques pour la réalisation d'échanges complémentaires dépassant les termes de la convention cadre,

CONSIDERANT que la mise en œuvre de cette convention d'échange et de géo-mutualisation est sans flux financier,

CONSIDERANT que cette convention est pour une durée de 6 ans, du 01/01/2024 au 31/12/2030,

Et après en avoir délibéré,

DECIDE

ARTICLE 1

D'ADOPTER l'exposé qui précède

ARTICLE 2

D'ADOPTER la convention cadre d'échange et de géo-mutualisation ci-annexée ainsi que tout document afférent à ce dossier.

ARTICLE 3

DE DIRE que cette décision est sans incidence financière.

Ainsi fait et délibéré les jours, ou mois et ans que dessus.
Pour extrait certifié conforme au registre.

Fait à Toulon, le 20 janvier 2025

Jean-Pierre GIRAN

Président de la Métropole
Toulon Provence Méditerranée



POUR	15
CONTRE	0
ABSTENTION	0



**CONVENTION CADRE
D'ÉCHANGES ET DE GEO-MUTUALISATION
2024-2030**

Au préalable, il est exposé ce qui suit :

Les partenaires publics de La Métropole Toulon Provence Méditerranée travaillent conjointement sur de nombreux projets en matière d'aménagement, de planification et de gestion des territoires. Ainsi, doivent-ils acquérir et utiliser de l'information numérique géolocalisée et se doter d'outils leur permettant d'exploiter ces informations.

Le présent document a pour objet de mettre en œuvre une convention cadre d'échange et de mutualisation autour de l'information géographique.

L'objectif est, d'une part, de mettre à disposition les données thématiques publiques par des technologies de l'information et de la communication, et, d'autre part, de favoriser leur utilisation et leur diffusion.

La mise en réseau des partenaires, proposée par la convention cadre, permettra de connaître, capitaliser et partager les données produites dans les organismes partenaires dans le cadre de leurs missions de service public. Il facilitera ainsi la connaissance du territoire.

Le présent document précise les modalités d'organisation de la mise en réseau des partenaires et de mise à disposition de données.

Dans le cadre de ses missions, La Métropole Toulon Provence Méditerranée dispose d'une plateforme d'échange d'information, de mutualisation d'expérience et d'exploitation des données : le Portail Data.

Afin de dynamiser les échanges et d'optimiser l'interopérabilité des systèmes, La Métropole Toulon Provence Méditerranée propose par le biais du réseau de mettre à disposition des partenaires du territoire ces outils.

En adhérant à la présente convention cadre chaque partenaire s'engage :

- À participer à la mise à disposition, sur la plateforme technique, de données mutualisables dont il dispose en veillant à leur qualité, leur actualisation et leur documentation. Le partenaire précisera le niveau de diffusion de ces données (accès restreint, grand public, ...),
- À indiquer les éventuelles erreurs qu'il constate en utilisant les données de partenaires,
- À respecter les conditions d'utilisation des données des partenaires (droits de propriétés, ...).

La mise en œuvre d'échanges et de mutualisation de l'Information Géographique pour le territoire de la Métropole Toulon Provence Méditerranée repose sur l'organisation entre les partenaires, de la mise en commun de données autour des axes complémentaires suivants :

- Le déploiement d'une plateforme technique d'échanges de données géographiques,
- L'alimentation des données géographiques par l'ensemble des partenaires.

L'objectif est de mettre à disposition, par les technologies de l'information et de la communication, les données publiques afin de faciliter l'accès et de favoriser leur utilisation et leur diffusion.

Considérant que, pour la définition, l'application et l'évaluation des politiques publiques qu'ils mettent en œuvre, les partenaires ayant une mission de service public, sont amenés à produire, et à utiliser des informations géographiques, cartographiques et sémantiques numériques, chacun des partenaires a également pour vocation de permettre l'accès le plus large possible de ses informations, la mise en commun des informations publiques contribue à la connaissance, la gestion et l'aménagement du territoire afin d'améliorer la cohérence de l'action publique, il est opportun, dans ces conditions, de favoriser l'accès et la réutilisation de ces informations de façon à faire jouer les synergies et à optimiser les fonds publics consacrés à leur production, ces échanges sont l'occasion d'améliorer la qualité des informations publiques produites et d'en maîtriser la connaissance,

Ceci exposé, il est convenu ce qui suit :

ARTICLE 1 – OBJETS, DEFINITIONS

Article 1.1 - Objet de la convention

La présente convention a pour objet de fixer les modalités de fonctionnement permettant la mutualisation et l'échange d'informations géographiques.

Cette mutualisation doit permettre de :

- Favoriser les échanges, éviter les doublons, mobiliser et mutualiser prioritairement les connaissances disponibles sur le territoire,
- Réduire des coûts et utiliser aux mieux les fonds publics consacrés à la production de l'information géographique,
- Partager l'expérience et les savoir-faire, et participer à l'enrichissement mutuel des informations géographiques,
- Mettre à disposition des partenaires l'information géographique disponible sur le territoire.

Cette convention constitue un socle d'échange mutualisé d'information géographique entre les partenaires adhérents.

Article 1.2 - Nom du réseau

Le partenariat régi par la présente convention est intitulé « **Echanges et Géo-Mutualisation** »

Article 1.3 - Objet du réseau

L'ensemble du dispositif est animé par les principes de mutualisation et d'interopérabilité.

Les partenaires du réseau :

A) Dans le cadre de la mutualisation,

- S'efforcent de rendre disponible aux membres du réseau, les informations géographiques dont ils sont dépositaires ; dans le respect des dispositions légales et réglementaires dont elles font l'objet, des principes énoncés et des droits éventuels de tiers.

B) Dans le cadre de projets opérationnels,

- Mobilisent leurs moyens (humains, techniques et financiers) pour l'acquisition, la mise à jour, la constitution et la diffusion de nouvelles informations, qui seront disponibles.

C) Examinent la possibilité d'ouvrir l'accès aux informations mutualisables à des tiers bénéficiaires selon les conditions précisées au chapitre 2.

Article 1.4 : Principes généraux de fonctionnement

Article 1.4.1- Plateforme mise à disposition

La plateforme est mise à disposition en extranet, avec un accès sécurisé en mode WEB.

Cette plateforme comporte un portail (Portail Data) et un accès aux différents types d'applications. Elle est le fruit d'une première collaboration entre La Métropole Toulon Provence Méditerranée et ses partenaires suite aux travaux d'un groupe de travail constitué de volontaires.



Article 1.4.2 - Rôle de l'administrateur de la plateforme (Métropole Toulon Provence Méditerranée)

La mission confiée à l'administrateur consiste en :

- La gestion technique et organisationnelle du système d'information (*intégration et organisation des données, gestion des comptes utilisateurs*),
- La gestion des relations et des échanges de données avec les partenaires (*signataires de la convention*),
- La formation et l'assistance aux utilisateurs en s'appuyant pour ce dernier point sur le réseau de correspondants SIG,
- L'assistance concerne uniquement les aspects strictement liés à la plateforme et ses applications.

Article 1.4.3 - Rôle de l'utilisateur (Partenaires)

Les utilisateurs opérationnels ou décisionnels, peuvent utiliser la plateforme pour :

- L'utilisation à des fins d'information qui pourrait répondre à terme aux besoins du grand public,
- La consultation de localisation et/ou de gestion des données afin d'en connaître leur existence,
- L'utilisation pour des fins d'aide à la décision.

Responsabilités :

L'outil privilégié de consultation de l'information est l'accès à la plateforme.

Il n'y a pas de méthodes particulières.

Les seules méthodes consistent en l'application de bonnes pratiques :

- Faire remonter toutes les anomalies, du point de vue des données sur leur qualité et leur exhaustivité et de celui des fonctionnalités offertes (adéquation aux besoins, temps de réponse, bugs éventuels...),
- Concourir à l'évolution du système en participant à son évolution par des propositions,
- Participer à l'alimentation des données mutualisées.

Article 1.5 - Définitions

Mutualisation :

Dans la présente convention, le terme « mutualisation » s'entend comme une mise en commun entre les partenaires. Elle peut concerner des données et des informations de tout type, les expériences et savoir-faire, ainsi que des moyens humains, techniques et financiers.

Les données mutualisables sont définies comme telles par leur propriétaire qui en fixe les modalités d'accès, d'usage et de diffusion par les partenaires, en s'efforçant de mettre en œuvre les principes établis par la présente convention. La mise en commun ne modifie pas les droits de propriété des données et ne constitue pas une appropriation par le partenariat.

Géomatique :

Ensemble des applications liées à la gestion et au traitement informatique des données géographiques.

Systèmes d'Information Géographique (SIG) :

Les Systèmes d'Information Géographique (SIG) sont des outils de connaissance et de gestion des territoires dont le moteur est composé de matériel informatique et de logiciels dédiés, alimentés par des données géographiques. Grâce à leurs fonctionnalités d'analyse et de cartographie, les SIG sont de véritables outils d'aide à la décision et de communication.

Les SIG connaissent un développement important au sein des collectivités territoriales, leur intérêt étant de permettre :

- De mieux connaître les territoires grâce à l'utilisation de données mises à jour à différentes échelles, de les observer,
- De mener à bien des études et aider à prendre des décisions en répondant à des questions, en permettant de simuler l'impact de projet sur le territoire,
- D'optimiser la gestion du patrimoine grâce à des outils dédiés aux métiers des collectivités (urbanisme, gestion des réseaux, des déchets, de l'éclairage public, des cimetières...),

- De faciliter la communication sur les projets des collectivités mais aussi favoriser la promotion du territoire, notamment à travers l'édition de cartes.

Données géographiques : Données que l'on peut positionner sur un plan. Informations renseignant sur les objets observés à la surface de la Terre, y compris leur position géographique, leur forme et leur description. Les données géographiques peuvent se présenter sous différentes formes : données spatiales (localisées), données tabulaires (littérales) et données image

Administrateur SIG : Personne ayant en charge la gestion globale du Système d'Information Géographique : gestion des données et gestion des droits d'accès notamment.

Utilisateur : Personne issue des services des partenaires amenée à utiliser la plateforme et ayant reçu des codes d'accès de la part de l'administrateur afin de pouvoir s'y connecter.

Codes d'accès : Les codes d'accès sont composés de l'identifiant et du mot de passe. Ils permettent de se connecter à la plateforme. Ils sont uniques et propres à chaque utilisateur.

Identifiant : Lors d'une connexion à la plateforme, l'identifiant est le nom d'utilisateur unique. Aucun compte générique ne sera accepté. L'utilisateur devra créer son compte sur la plateforme. Celui-ci sera soumis à la validation de l'administrateur de la plateforme.

Droits « utilisateur » : Ensemble des droits d'exploitation des données attribués à chaque utilisateur par l'administrateur de la plateforme.

Poste client : Ordinateur du partenaire ayant accès à la plateforme mutualisée grâce à un accès Internet.

Couche : Un Système d'Information Géographique permet de gérer des données graphiques (cartographiques) et attributaires. Les données graphiques sont organisées en couches sur le principe d'un « mille-feuilles ».

Les données géographiques : Description d'objets géographiques (vecteurs ou rasters) localisés dans un système de coordonnées faisant référence au positionnement à la surface du globe terrestre. La description des entités spatiales est complétée par les données attributaires qui y sont rattachées (technologie SIG).

Les données attributaires (ou sémantiques) : Toute information alphanumérique qualitative ou quantitative complétant la description des objets géographiques tels que précédemment définis (technologie base de données).

Plateforme Open Data : il s'agit d'un site internet regroupant les couches géographiques mises à disposition par La Métropole Toulon Provence Méditerranée.

Métadonnées : Les métadonnées sont des données sur des données. Elles décrivent comment, quand et par qui un jeu particulier de données a été recueilli, et comment les données sont formatées. ...

ARTICLE 2 - CONDITIONS ET PRINCIPES GENERAUX D'UTILISATION DE LA PLATEFORME ET FONCTIONNEMENT DU RESEAU

Article 2.1 - Principe de mutualisation des données

Le principe de mutualisation vise à favoriser l'échange des données entre les partenaires du réseau, à permettre leur réutilisation et à contribuer à leur diffusion, notamment à destination du citoyen, dans le cadre d'une démarche dématérialisée (e-services).

L'outil de communication principal consiste en une plateforme "portail", accessible sur Internet, qui permet de favoriser la mutualisation des actions des institutions publiques en matière d'information géographique. En plus d'un accès libre à un certain nombre d'informations, elle comporte des espaces professionnels dédiés aux partenaires du réseau (identifiés par un nom d'utilisateur et un mot de passe) qui donnent accès à des outils collaboratifs visant à développer les échanges entre les différents contributeurs.

Afin d'enrichir nos bases de données et la plateforme Open Data, le service SIG préconise que lui soit fournies les données selon les préconisations de l'annexe 4.

L'accès au portail est ouvert à l'ensemble des membres selon une liste d'ayants droit dressée pour chaque donnée en concertation avec le "gestionnaire". L'administrateur de la plateforme veille notamment à ce que l'accès au portail soit réservé aux personnes autorisées, impose les niveaux de sécurité adaptées aux informations qui y sont présentes et fournit aux utilisateurs tous conseils utiles au bon usage des outils disponibles sur le portail.

Les transferts des données sont gratuits. Les échanges, organisés dans le cadre de la présente convention, ne constituent pas une vente mais une mise à disposition.

La fourniture des données ne constitue ni une cession, ni un droit d'utilisation exclusif pour le bénéficiaire.

Tout lot de données transmis reste la propriété de son producteur mais aussi de sa responsabilité. Il constitue une réalisation intellectuelle protégée par la loi N°92-597 du 1er juillet 1992 et par la loi N° 2006-961 du 1^{er} août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information.

Le principe de qualité des données est de règle pour l'alimentation de la plateforme. Par l'alimentation de la plateforme, les membres du réseau respectent les critères de qualité, préconisés par l'administrateur (voir Annexe 4).

Article 2.1.1 - Les données mises à disposition

Les données existantes sont listées dans le portail Open Data dont l'animation et l'administration sont assurées par La Métropole Toulon Provence Méditerranée. D'autres données mutualisables seront mises à disposition sous conditions.

Article 2.1.2 - Les données acquises et/ou produites dans le cadre des projets opérationnels

Tant que faire se peut, les données acquises et/ou produites dans le cadre des projets opérationnels figureront également dans le portail.

Les négociations pour l'acquisition et/ou la création de données nouvelles, dans le cadre des projets opérationnels, doivent conduire à la mutualisation de ces données pour l'ensemble des partenaires du réseau sans restriction ou contraintes liées aux droits d'usage ou de diffusion, sauf celles précisées dans le paragraphe suivant.

Article 2.1.3 - Exceptions aux principes de mutualisation

Les exceptions au principe de mutualisation doivent se comprendre dans un sens restrictif.

Les données ayant les caractéristiques suivantes ne pourront pas être mises à disposition par les titulaires :

- Les informations nominatives sur des personnes privées ou couvertes par un secret, au sens des lois du 6 janvier 1978, modifiée par la loi N°2004-801 du 6 août 2004 relative à l'informatique, aux fichiers et aux libertés, du 17 juillet 1978 sur la liberté d'accès aux documents administratifs, et l'ordonnance du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques,
- Les données pour lesquelles le principe de mutualisation n'est pas conforme avec la réglementation en vigueur,
- Les données confidentielles ou sensibles,
- Les données soumises à des droits de diffusion à l'exception de celles pour lesquelles le producteur (qui n'est pas forcément le "gestionnaire" des

données), a indiqué de façon expresse par écrit, les conditions de mise à disposition de ces données fi des tiers.

- Les données produites par un des partenaires en collaboration avec un organisme extérieur, lorsque ce dernier s'y oppose.

Article 2.2 - Responsabilité du "gestionnaire" et du "bénéficiaire"

Article 2.2.1 - Le gestionnaire

Le "gestionnaire" met à disposition les données selon les dispositions énoncées dans l'article 2.1.

Le "gestionnaire" certifie que les fichiers transmis sont conformes aux fichiers utilisés pour ses propres besoins dans le cadre de son système d'information eu égard à leurs périodes de productions et de validité.

Le "gestionnaire" ne délègue pas sa compétence réglementaire avec la fourniture des données.

Le "gestionnaire" ne peut être tenu responsable de l'usage qui sera fait des fichiers fournis, ni des dommages directs et/ou indirects qui pourraient résulter de l'utilisation des données.

Le "gestionnaire" ne peut être tenu responsable des erreurs de localisation, d'identification, d'actualisation ou des imprécisions des données.

Lors de la mise à disposition des données dans la plateforme, le "gestionnaire" communique un descriptif précis de la structuration et de la qualité des données, en remplissant la fiche de métadonnées.

Le "gestionnaire" d'un lot de données s'engage à fournir toute documentation existante nécessaire ou utile.

Article 2.2.2 - Le bénéficiaire

"Le bénéficiaire" pourra télécharger la donnée sur le Portail Data, partie Open Data.

Si la donnée n'est pas directement téléchargeable, "le bénéficiaire" fait obligatoirement appel au "gestionnaire" pour disposer des données qu'il souhaite utiliser ou mettre à disposition de prestataires et de sous-traitants.

"Le bénéficiaire" constate, lors du transfert, la qualité des informations transférées et devient responsable des conséquences de leur utilisation, de leur modification et de leur mise à jour éventuelle dans un contexte différent de celui de leur production.

"Le bénéficiaire" ne rediffuse pas les données qu'il a reçues du "gestionnaire" sauf s'il les a transformées, enrichies ou dégradées (procédure de modification) pour des raisons et des besoins liés à l'exercice de ses compétences. Dans ce cas, il doit garantir l'engagement de prendre toutes les précautions nécessaires (techniques et juridiques) pour que toutes les données sources ne puissent être exploitées sans autorisation préalable.

"Le bénéficiaire" garantit la traçabilité des données (description des données sources et des traitements réalisés par rapport à la donnée d'origine).

"Le bénéficiaire" devra faire figurer sur tous les documents et/ou produits et services électroniques ayant pour origine partielle ou intégrale les données d'un partenaire, la mention "Source des données : suivi du "nom du service ou de l'organisme producteur" et de la "date", indiqués dans la fiche de métadonnées.

"Le bénéficiaire" (membre ou tiers bénéficiaire) du réseau ne pourra pas utiliser les données mises à sa disposition à des fins commerciales.

"Le bénéficiaire" garantit l'utilisation des données dans les conditions et les modalités d'exploitation telles qu'elles sont définies par le partenaire producteur dans la fiche de métadonnées (tout ce qui n'a pas été expressément autorisé est interdit).

Il appartient au "bénéficiaire" d'un lot de données de s'assurer :

- De l'adéquation des données demandées à ses propres besoins,
- Qu'il dispose de la compétence nécessaire à l'utilisation de ces données.

Article 2.3 - Mises à disposition d'informations à des prestataires et sous-traitants

La mise à disposition d'informations issues de la plateforme à des prestataires ou sous-traitants est strictement limitée à la réalisation des prestations effectuées pour le compte de l'un des partenaires du réseau.

Elle est subordonnée à la signature préalable d'un "Acte d'engagement" (modèle en Annexe 3), entre le partenaire du réseau et le prestataire de services, lui interdisant la conservation et l'utilisation des données transférées en dehors du cadre de la prestation concernée.

Article 2.4 - Mise à disposition de matériels

Le service SIG fournit à ces partenaires les outils SIG dont les applications mobiles compatibles Android et iOS mais ne fournit en aucun cas le matériel nécessaire à l'exploitation de ces outils.

Article 2.5 - Financement

La mise à disposition des données par les partenaires producteurs ou gestionnaires est gratuite.

Le cas échéant, les projets opérationnels sont financés selon des modalités définies entre les participants. Ils peuvent faire l'objet de conditions particulières d'exécution en listant en particulier les contributions de chaque partenaire.

Article 2.6 - Litiges

Dans le cas où l'interprétation ou l'exécution de la présente convention soulèverait un différend qui ne pourrait être résolu à l'amiable, les parties conviennent de rechercher une conciliation par un tiers choisi d'un commun accord, avant de porter éventuellement le différend devant le tribunal compétent.

Article 2.7 - Durée, modification, résiliation

La présente convention est établie pour une durée de 6 ans à effet du 01/01/2024.

A l'issue de ces 6 ans un bilan sera réalisé et présenté aux partenaires adhérents à cette convention.

La présente convention peut être résiliée par décision conjointe entre TPM et chaque partie à la présente, ou en cas de manquement aux obligations résultant de la présente par une partie, après mise en demeure restée sans effet pendant 1 mois, des avenants pourront être passés pour actualiser la convention.

ARTICLE 3 : FONCTIONNEMENT DU PARTENARIAT

Article 3.1 - Administration de la plateforme

La Métropole Toulon Provence Méditerranée assure le rôle d'administrateur pour la plateforme de mutualisation.

Le dispositif de la plateforme est un outil évolutif dont les objectifs de contenu dépendent en premier lieu de l'implication des services participants et par conséquent d'une culture commune en matière d'information géographique.

La Métropole Toulon Provence Méditerranée favorise et harmonise cette acculturation, en proposant notamment aux partenaires un outil d'accès à l'information géographique sur Internet et une assistance à l'utilisation de cet outil.

Les missions de l'administrateur sont de :

- Administrer l'infrastructure technique (maintenance, développements informatiques, ...) pour la plateforme,
- Administrer les bases de données (optimisation des bases, intégration de données...),
- Mutualiser les données de référence et les données métier.

Article 3.2 - Adhésion et retrait

L'adhésion des personnes publiques à la présente convention cadre est soumise à l'autorisation préalable de leur assemblée délibérante, selon les règles propres à chacune d'elles.

L'adhésion des autres institutions et organismes se fera dans le respect de leurs propres règles statutaires et des textes qui les régissent.

Dans tous les cas, une copie de la décision d'adhésion, complétée du formulaire « adhésion à la convention cadre d'échange et de géo-mutualisation » (modèle en Annexe 3) sera adressée par lettre recommandée avec accusé de réception à l'administrateur qui assure la coordination.

L'administrateur mettra alors en place les droits d'accès à la plateforme.

Cette autorisation sera donnée, sans réserve et de manière expresse, pour l'ensemble des clauses de la présente convention et des documents y étant annexés, et vaudra mandat pour que le coordinateur du groupement puisse agir dans le strict respect des missions qui lui sont reconnues par la présente convention.

Tout partenaire adhérent peut se retirer de la présente convention. La demande de retrait du groupement est adressée à l'administrateur par lettre recommandée. Le retrait sera effectif dans le délai de 6 mois à compter de la réception du courrier recommandé.

Liste des annexes

Annexe 1 : Adhésion à la convention cadrepage 14

Annexe 2 : Modèle de document de mise à disposition de données numériques du partenaire vers la Métropole TPMpage 16

Annexe 3 : Modèle d'acte d'engagement à fournir au prestataire en cas de livraison de donnéespage 18

Annexe 4 : Qualité des donnéespage 20

Annexe 5 : La protection des données (RGPD : Règlement général pour la protection des données)page 22

Annexe 6 : Charte informatique de la Métropole Toulon Provence Méditerranéepage 32

Annexe 7 : Résiliation à la convention cadrepage 44

ANNEXE 1 : Adhésion à la convention cadre

ADHESION A LA CONVENTION CADRE D'ECHANGES ET DE GEO-MUTUALISATION

Art. 1 : Engagement

Le <nom de l'organisme>, <statut juridique>, domicilié <adresse>, représenté par <nom du représentant> reconnaît avoir pris connaissances de la convention cadre d'Echanges et de Géo-Mutualisation et de ses annexes et décide de son adhésion à cette convention.

Chaque partenaire s'engage à désigner un correspondant et un suppléant.

En tant que relais entre son organisme et les autres partenaires, le correspondant de la plateforme de mutualisation doit pouvoir :

Vis-à-vis des partenaires de la plateforme :

- Représenter son organisme,
- Assurer la participation active de sa structure en l'impliquant,
- Définir et communiquer à l'administrateur de la plateforme les cellules et/ou les personnes de son organisme désignées comme utilisatrices de la plateforme (profil gestionnaire ou utilisateur), avec les droits associés,
- Garantir la validation interne et assurer l'actualisation des données mises à disposition par son service,
- Recueillir et traiter les remarques des autres participants,
- Informer l'administrateur de la plateforme des projets de son service en termes d'acquisition ou de numérisation d'informations géographiques,
- Informer les autres partenaires sur les données gérées par son service et qui ne sont pas mises à disposition.

Vis-à-vis de son organisme :

- Assurer en interne la rediffusion des informations liées à la plateforme, notamment les réflexions et travaux initiés dans le cadre de la convention concernant son organisme,
- Informer son organisme des données mises à disposition par les autres partenaires.

Le correspondant du réseau n'est pas nécessairement la personne unique réalisant l'ensemble de ces tâches, mais il doit être en contact avec les agents de sa structure qui les réalisent afin de suivre leur bon déroulement et de pouvoir rendre compte aux autres participants, le cas échéant. Il est notamment responsable de la diffusion interne

de la présente convention précisant les conditions d'utilisation des fichiers mis à disposition dans le cadre de la plateforme.

Chaque partenaire à la plateforme s'engage à garantir la représentativité de son correspondant dans le domaine de l'information géographique et à anticiper sur sa mobilité.

En cas de changement du correspondant, ou de son suppléant, le service prendra les dispositions nécessaires pour assurer la continuité de la fonction et communiquera dans les meilleurs délais l'identité du nouveau correspondant à l'Administrateur de la plateforme.

Les organismes désigneront préférentiellement comme correspondant de la plateforme l'administrateur des données localisées de leur propre SIG.

Art. 2 : Correspondant

Le correspondant et son suppléant du <Nom du partenaire>, est :

- <Nom et fonction de la personne désignée,>
- <Suppléant : Nom et fonction>.

Art. 3 : Données mises à disposition

L'organisme établit une liste des données mises à disposition dans le cadre de la plateforme de mutualisation d'information Géographique. Cette liste indiquera les éléments précisés en annexe 2 suivant les préconisations de l'annexe 4.

Ces informations doivent être détaillées et complétées via l'annexe 4 (ci-après) et transmises à Toulon Provence Méditerranée, service SIG & Territoire Connecté.

Art. 4 : Dispositions particulières

Dispositions particulières concernant certains points tels que:

- Utilisation du logo de l'organisme
- Conditions spécifiques pour des copies
-

Fait à le

Lu et approuvé (mention manuscrite)

Signature

(Qualité du signataire pour une personne morale)

ANNEXE 2 : Modèle de document de mise à disposition de données numériques du partenaire vers la Métropole TPM

Ce document est à renseigner et à signer par le partenaire lors d'une livraison d'une donnée à la Métropole TPM pour une mise à disposition de cette dite-donnée.

Si plusieurs données sont fournies par le partenaire, il y aura autant de document de mise à disposition que de données.

A. Caractéristiques de la donnée

Nom de la donnée : à renseigner

Créateur de la donnée : à renseigner

Service responsable : à renseigner

Date de dernière mise à jour : à renseigner

Périodicité des mises à jour : à renseigner

Durée de validité : à renseigner

Format de la donnée : à renseigner

Emprise géographique : à renseigner

Système de coordonnées : à renseigner

B. Description de la donnée (explications sur son utilité et son mode de création)

À renseigner

C. Validation et utilisation de la donnée

Le service responsable de la donnée est chargé de contrôler les données en termes d'exhaustivité, de fiabilité et de précision. La responsabilité de la donnée revient donc au partenaire qui l'a fourni.

Suite au contrôle de ces données, plusieurs niveaux de validation sont définis pour traduire l'utilisation qui peut en être faite. La donnée mise à disposition doit être définie selon l'un des 2 niveaux suivants :

Niveau 1 : Information

Les données ont été jugées d'une qualité suffisante pour être mise en ligne à titre d'information. Cependant, elles ne sont pas jugées suffisamment abouties pour en faire une exploitation en l'état.

Niveau 2 : Exploitation données propriétaires

Les données proviennent d'une source interne à l'entité et leur contrôle a été quantifié par le service responsable de ces données. Elles sont jugées par celui-ci suffisamment aptes à une mise en ligne à la date de mise à jour pour une exploitation par les utilisateurs de la plateforme de la Métropole TPM.

À noter que la diffusion des données, quel que soit leur niveau de validation, à des tiers externes à l'entité, requiert l'accord du service responsables des données et doit faire l'objet de la signature de l'annexe 3 à la présente.

De fait, concernant la donnée.....

Le niveau de validation accordé est (cocher le niveau défini) : Niveau 1 ☐ Niveau 2 ☐

Service
responsable

Nom prénom du signataire

Qualité du
signataire

Date :

Signature :

ANNEXE 3 : Modèle d'acte d'engagement à fournir au prestataire en cas de livraison de données

Logo du producteur
de la donnée

ACTE D'ENGAGEMENT

Les fichiers désignés ci-après sont la propriété de

À indiquer: Libellé de la donnée - Projection - Format

Ces fichiers sont mis à la disposition :

Des concessionnaires, délégataires ou prestataires de service :

Nom, raison sociale :

Siège social :

N° de SIRET :

Code juridique de l'établissement :

Ci-après désigné " le dépositaire " ,

Par le bénéficiaire d'une licence Métropole TPM. Elle est issue de la convention cadre « Echanges et de Géo-mutualisation » :

Nom, raison sociale :

METROPOLE TOULON PROVENCE MEDITERRANEE
Direction Commune des Systèmes – Métropole TPM/Ville de Toulon
Service Système d'Information Géographique & Territoire Connecté

Siège social :

107, Boulevard Henri Fabre
CS 30536
83 041 TOULON

N° de SIRET :

248 300 543 00217

Ci-après désigné " le licencié ",

Dans le cadre de : **À indiquer: Libellé du marché de prestation**

Cette mise à disposition est strictement subordonnée à la signature par le dépositaire du présent acte d'engagement.

Par le présent acte, le dépositaire :

- 1)** Reconnaît avoir pris connaissance des spécifications techniques des fichiers préalablement à la signature du présent acte,
- 2)** S'engage à n'exploiter ces fichiers et les données des coéditeurs, sous toute forme et sous tout support, que pour autant que cette exploitation est strictement liée et s'exerce pour les seuls besoins des prestations qui lui ont été confiées par le licencié, et s'interdit tout autre utilisation des fichiers et des données qu'ils contiennent,
- 3)** S'engage à détruire les fichiers et tout document dérivé de ces fichiers qu'il n'aurait pas eu à restituer au licencié pour quelque motif que ce soit, dans le cadre de l'exécution du contrat de prestation, et à n'en conserver aucune copie,
- 4)** S'interdit notamment toute reproduction aux fins de divulgation, communication, mise à disposition, transmission des fichiers et des données à des tiers, sous toute forme, sur tout support, par quelque moyen et pour quelque motif que ce soit, à titre gratuit ou onéreux, sans l'autorisation expresse de l'éditeur,
- 5)** Reconnaît que tout manquement de sa part à ces dispositions engagera sa pleine et entière responsabilité à l'égard de l'éditeur.

Par le présent acte, le licencié :

S'engage à informer le service SIG de la Métropole Toulon Provence Méditerranée de tout prêt à un concessionnaire, délégataire ou prestataire de service par mail : sig@metropoletpm.fr.

Fait à , le

Le **dépositaire** (nom et qualité), Signature :

ANNEXE 4 : Qualité des données

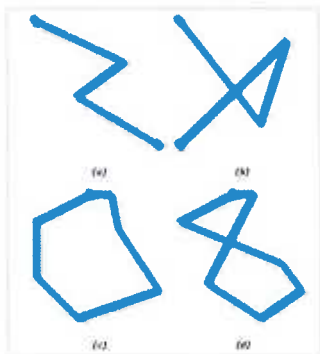
Cette annexe porte sur la qualité des données pour rendre possible les échanges de données géographiques ; celles-ci devront respecter quelques prérequis :

- Présence de métadonnées qui indiquent comment, quand, où et par qui les données ont été recueillies, mentionnent leur disponibilité et leur mode de distribution, le système de projection et de coordonnées qui les caractérisent, l'échelle de suivi, la résolution et la précision. En Europe, les métadonnées doivent se conformer à une norme de métadonnées géospatiale (Norme ISO 19139 - INSPIRE).
- Formats de données définis à l'Open Geospatial Consortium (OGC) et pouvant ainsi être transformés par les bibliothèques GDAL/OGR (dans le cas de web service, les protocoles à privilégier sont WMS et WFS).
- Plus particulièrement sur les données « vecteur », sont à privilégier les entités géométriques **simples et valides**.
Selon les spécifications de l'OGC, une géométrie **simple** est une géométrie qui ne comporte pas de points géométriques anormaux, comme des auto-intersections ou des auto-tangences, ce qui concerne essentiellement les points, les multipoints, les polylignes et les multi-polylignes.
La notion de géométrie **valide** concerne principalement les polygones et les multi-polygones et le standard définit les caractéristiques d'un polygone valide.

** POINT **

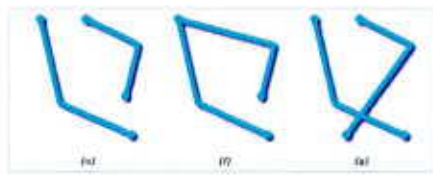
Un point est par nature simple, ayant une dimension égale à 0. Un objet multipoints est simple si tous les points le composant sont distincts.

** POLYLIGNE **



Une polyligne est simple si elle ne se recroise pas (les extrémités peuvent être confondues, auquel cas c'est un anneau et la polyligne est fermée).

Les polygones (a) et (c) sont simples, mais pas les polygones (b) et (d)

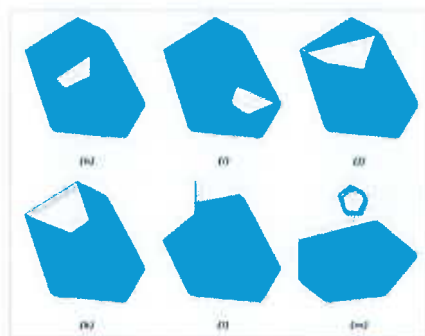


Une multi-polyligne est simple si toutes les polygones la composant sont elles-mêmes simples et si les intersections existantes entre 2 polygones se situent à une extrémité de ces éléments.

(e) et (f) sont des multi-polygones simples, mais pas (g)

**** POLYGONE ****

Les limites d'un polygone peuvent être constituées par un unique anneau extérieur (polygone plein) ou par un anneau extérieur et un ou plusieurs anneaux intérieurs (polygone à trous).



Un polygone est valide s'il ne comporte pas d'anneaux se croisant.

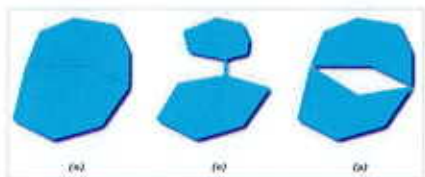
Un anneau peut intersecter la limite mais seulement en un point (pas le long d'un segment).

Un polygone ne doit pas comporter de lignes interrompues (les limites doivent être continues) ou de point de rebroussement (pic).

Les anneaux intérieurs doivent être entièrement contenus dans la limite extérieure du polygone.

(h) et (i) sont des polygones valides, (j), (k), (l), (m) sont des polygones ni simples ni valides mais (j) et (m) sont des multi-polygones valides

Un multi-polygone est valide si et seulement si tous les polygones le composant sont valides et si aucun intérieur d'un polygone ne croise celui d'un autre.



Les limites de 2 polygones peuvent se toucher, mais seulement par un nombre fini de points (pas par une ligne).

(n) et (o) ne sont pas des multi-polygones valides, par contre (p) est valide

ANNEXE 5 : La protection des données (RGPD : Règlement général pour la protection des données)

Déléguée à la protection des données du partenaire :

Nom

Adresse mail

Numéro de téléphone

Délégué à la protection des données Métropole TOULON PROVENCE MEDITERRANEE

Christian DURAND

donnees_personnelles@metropoletpm.fr

04 94 36 34 24

SOMMAIRE

ANNEXE 5 : LA PROTECTION DES DONNEES (RGPD : REGLEMENT GENERAL POUR LA PROTECTION DES DONNEES)	1
I. GENERALITES	3
1.1 QUALIFICATION DES PARTIES.....	3
1.2 OBJET DE L'ANNEXE.....	3
II. DUREE DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL	3
III. OBLIGATIONS DU SOUS-TRAITANT VIS-A-VIS DU RESPONSABLE DE TRAITEMENT	3
3.1 OBLIGATIONS DU SOUS-TRAITANT ET DESCRIPTION DU TRAITEMENT FAISANT L'OBJET DE LA SOUS-TRAITANCE	3
3.2 SOUS-TRAITANCE ULTERIEURE	4
3.3 DROIT D'INFORMATION DES PERSONNES CONCERNEES	5
3.4 EXERCICE DES DROITS DES PERSONNES	5
3.5 VIOLATION DE DONNEES	5
3.6 DOCUMENTATION - AUDITS	5
3.7 AIDE DU SOUS-TRAITANT	6
3.8 MESURES TECHNIQUES ET ORGANISATIONNELLES	6
3.9 SORT DES DONNEES	9
3.10 DELEGUE A LA PROTECTION DES DONNEES	9
3.11 TENUE DU REGISTRE	9
IV. OBLIGATIONS DU RESPONSABLE DE TRAITEMENT VIS-A-VIS DU SOUS-TRAITANT	9

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « **le règlement européen sur la protection des données** » ou « **le RGPD** »).

I. GENERALITES

1.1 Qualification des parties

La Métropole TPM et le partenaire signataire reconnaissent revêtir la qualité de « responsable du traitement », c'est-à-dire être les seules entités personnes habilitées à déterminer la finalité du traitement des données personnelles recueillies.

La Métropole reconnaît revêtir la qualité de « sous-traitant », c'est-à-dire traiter les données personnelles recueillies pour le compte, sur instruction ou sous l'autorité du responsable de traitement, sans pouvoir déterminer la finalité du traitement des dites données.

1.2 Objet de l'annexe

La présente annexe a pour objet de définir :

- Les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies au sens du RGPD ci-après.
- Les obligations du responsable de traitement vis-à-vis du sous-traitant.

Les dispositions ci-après définies s'appliqueront à chaque fois que les prestations de services du sous-traitant peuvent le conduire à accéder à des données à caractère personnel provenant du responsable de traitement dans le cadre des traitements visés dans la présente.

II. DUREE DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Le traitement par les parties engagées n'est autorisé que pendant la durée d'exécution de la convention cadre de géomutualisation et au maximum 4 ans, à partir de la date du dernier signataire.

III. OBLIGATIONS DU SOUS-TRAITANT VIS-A-VIS DU RESPONSABLE DE TRAITEMENT

3.1 Obligations du sous-traitant et description du traitement faisant l'objet de la sous-traitance

Le sous-traitant s'engage à :

- 3.1.1 Traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/ont l'objet de la sous-traitance ;
- 3.1.2 Ne traiter les données à caractère personnel **que sur instructions documentées** du responsable de traitement tel que prévu dans le présent contrat ;
- 3.1.3 **Informier immédiatement** le responsable de traitement, s'il considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des États membres relative à la protection

des données. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

3.1.4 Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat, notamment :

- Ne prendre aucune copie des documents et supports d'informations comportant des données à caractère personnel ou des données à caractère personnel elles-mêmes, à l'exception de celles nécessaires pour les besoins de l'exécution de sa prestation, objet du Contrat ;
- Ne pas utiliser les documents et données à caractère personnel à des fins autres que celles spécifiées au Contrat ;
- Ne pas divulguer ces documents ou données à caractère personnel à des tiers non autorisés.
- Veiller à ce que **les personnes autorisées à traiter les données à caractère personnel** en vertu de la présente convention :
 - S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité
 - Reçoivent la formation nécessaire en matière de protection des données à caractère personnel
- Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de **protection des données dès la conception** et de **protection des données par défaut**.

3.2 Sous-traitance ultérieure

Le sous-traitant peut également faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le responsable de traitement dispose d'un délai de quinze (15) jours à compter de la date de réception de cette information pour présenter par écrit ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant est autorisé à faire appel à d'autres sous-traitants dans le cadre des services de maintenance et d'hébergement fournis à la personne publique responsable de traitement.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par son sous-traitant ultérieur de ses obligations.

3.3 Droit d'information des personnes concernées

Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

3.4 Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données à caractère personnel, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées exercent directement auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique au Délégué à la Protection des Données du responsable de traitement.

3.5 Violation de données

En cas de faille de sécurité avérée ou suspectée susceptible de compromettre la sécurité des données à caractère personnel auxquelles le sous-traitant a accès (destruction, perte, altération, divulgation, accès non autorisé à des données à caractère personnel, de manière accidentelle ou illicite), le sous-traitant devra immédiatement :

- Prendre toutes mesures nécessaires pour en atténuer les conséquences et pour empêcher qu'une telle violation puisse perdurer et/ou se reproduire.
- Notifier au responsable de traitement dans les meilleurs délais à compter de la découverte de la faille de sécurité et par tous moyens écrits y compris les correspondances électroniques :
 - a) Une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d'enregistrements de données à caractère personnel concernés) ;
 - b) Les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel ;
 - c) Ses conséquences probables et les mesures prises ou les mesures que le sous-traitant propose de prendre pour remédier à la violation, y compris pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

3.6 Documentation - Audits

Le sous-traitant met à la disposition du responsable de traitement les informations nécessaires pour démontrer le respect de ses obligations prévues à l'article 28 du RGPD et pour lui permettre de réaliser des audits, y compris des inspections, aux frais du responsable de traitement. Ils

doivent permettre notamment de s'assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées sans que cela ne soit détecté et notifié.

L'audit sera mené par le responsable du traitement ou un auditeur qu'il aura mandaté, non-concurrent du sous-traitant, et soumis à une obligation de confidentialité.

Le responsable de traitement s'engage à notifier avec un préavis minimum de quinze (15) jours au sous-traitant tout audit, en lui communiquant notamment l'objet de la mission, la date de l'audit, la durée envisagée, et le nom du ou des auditeur(s).

Le sous-traitant ne pourra pas refuser, sans motif légitime, l'auditeur choisi par le responsable de traitement pour réaliser cet audit.

Le sous-traitant mettra en place les moyens raisonnables pour permettre à l'auditeur de mener à bien son audit. Les opérations d'audit et les demandes d'information devront être effectuées pendant les heures normales d'ouverture du sous-traitant et ne devront pas perturber le bon fonctionnement des activités de ce dernier.

Au titre de cette assistance fournie au responsable de traitement par le sous-traitant, ce dernier interviendra sans frais supplémentaire pour le responsable de traitement dans la limite de deux (2) jours/homme par an. Toute mobilisation complémentaire de ressource du sous-traitant pour cette assistance sera facturée au responsable de traitement.

Un exemplaire du rapport d'audit sera remis gracieusement au sous-traitant. Les parties examineront de bonne foi ce rapport dans le cadre d'un comité de pilotage, et identifieront, le cas échéant, les actions qui devront être engagées par l'une ou l'autre des parties pour mettre en œuvre les décisions prises lors de ce comité. Ce rapport est confidentiel et strictement réservé aux parties. Si le rapport fait apparaître un manquement aux obligations du sous-traitant, ce dernier s'engage à mettre en œuvre, à ses frais, toute mesure corrective appropriée dans un délai de 3 mois. En cas de contestation du rapport d'audit par le sous-traitant, ce dernier proposera à ses frais un nouvel audit par un autre cabinet de son choix.

Le responsable de traitement ne pourra pas réaliser plus d'un audit du sous-traitant sur une période glissante de 12 mois, sauf accord de ce dernier.

3.7 Aide du Sous-traitant

Sur demande du responsable de traitement, et après accord sur la proposition technique et financière du sous-traitant, ce dernier peut apporter son aide au responsable de traitement pour l'assister dans la réalisation d'analyses d'impact relatives à la protection des données à caractère personnel, ainsi que pour la préparation de la consultation préalable de l'autorité de contrôle.

La personne publique responsable du traitement demeure seule maître de la finalité du traitement et de la décision de soumettre ou non le traitement, après conseil du sous-traitant, à une analyse d'impact ou une consultation préalable de l'autorité de contrôle nationale.

3.8 Mesures techniques et organisationnelles

Le sous-traitant s'engage conformément à la réglementation applicable à la protection des données à caractère personnel, à mettre en œuvre les mesures techniques et organisationnelles appropriées au regard de la nature des données et des risques présentés par le traitement, afin de préserver la confidentialité, la sécurité et l'intégrité des données à caractère personnel auxquelles il pourra avoir accès à l'occasion de la réalisation des prestations, et notamment empêcher toute déformation, altération, endommagement, destruction de manière fortuite ou illicite, perte, divulgation et/ou tout accès par des tiers non autorisés préalablement.

Afin de garantir un niveau de sécurité adapté, le sous-traitant mettra notamment en œuvre, en tenant compte des risques pour la sécurité des données à caractère personnel et pour la vie

privée des personnes, selon les besoins, les mesures de sécurité appropriées définies par la Métropole TPM.

- La pseudonymisation ou le chiffrement des données à caractère personnel :
 - Les données de production ne sont pas utilisées dans les environnements de développement.
 - Si les données livrées sont dites « normales », l'envoi se fait par mail et si données sont dites sensibles, livraison avec un zip chiffré.
- Les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
 - Sécurité physique des locaux
 - L'accès aux locaux nécessitent la possession d'un badge physique nominatif et actif. Selon la sensibilité des zones, des droits spécifiques sont fournis aux badges. Un système de vidéo surveillance est également mis en œuvre, avec une centralisation sur un serveur sécurisé. La vidéo surveillance couvre les accès et/ou zones sensibles.
 - L'accès visiteur est strictement contrôlé. Lors de l'arrivée d'un visiteur, celui-ci est accompagné tout au long de sa présence au sein des locaux par son interlocuteur. Le visiteur n'est jamais laissé sans surveillance au sein des locaux. Chaque visiteur s'enregistre lors de son arrivée dans les locaux et un badge visiteur à mettre en évidence lui est remis. Dès que le visiteur quitte les locaux, l'horodatage du départ est enregistré. Le badge visiteur ne permet aucun accès.
 - L'accès aux salles hébergeant les équipements réseaux sont protégés au moyen de badge. L'accès est autorisé uniquement pour le responsable et les personnels de la DSI.
 - Transfert de l'information
 - Les informations sensibles et confidentielles ne sont communiquées qu'au travers de canaux sécurisés et chiffrés. À défaut, les informations sont chiffrées avant d'être communiquées. Le moyen de déchiffrement de l'information est communiqué au travers d'un media de communication tiers (ex : envoi du contenu chiffré par mail et envoi de la clef de déchiffrement par SMS).
 - Tous les échanges de données entrants, sortants et internes sont analysés par des solutions antivirus/antimalware et de détection de fuite de données (DLP) afin de prévenir toutes atteintes à la sécurité de l'information.
 - L'infrastructure repose sur un ensemble d'équipements redondés (électricité, climatisation, réseau et serveur). Les systèmes mis en œuvre sont de type actifs-actifs afin de répartir la charge. Si toutefois les briques techniques ne le permettent pas, la redondance est à minima de type actif-passif. Les données SIG sont stockées dans une base de données. La gestion des flux entrants et sortants est réalisée par un système de double pares-feux, certifiés ou qualifiés par l'ANSSI. Un système de surveillance 24h/24 7/7 de l'espace hébergé et du serveur est installé permettant la remontée d'alertes par e-mail et SMS vers le sous-traitant
- Les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

- Les données, sous formes de bases de données ou de fichiers, sont sauvegardées et stockées sur un support sur site. Elles sont aussi chiffrées pour être exportées sur un site externe. L'infrastructure virtuelle est sauvegardée localement et exportées sur un site de PRA.
- Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.
 - Revue régulière de l'ensemble des briques techniques et organisationnelle afin d'améliorer constamment la qualité de la sécurité du système d'information
 - Audits automatisés réalisés régulièrement afin de mettre en évidence les éventuelles failles connues non patchées
 - Tests de pénétration menés au moins une fois par an en interne. Une copie du dernier test peut être obtenue sur demande écrite du responsable de traitement.
- Sécurité des traitements de support.
 - Le personnel ne peut pas apporter son propre appareil (BYOD), sauf dans le cas des appareils de téléphonie mobile, qui ne peuvent accéder aux outils de messagerie et de collaboration Office qu'avec l'utilisation de l'authentification multi facteur (MFA).
 - Des contrôles de sécurité sont en place pour permettre une main-d'œuvre distante sécurisée, y compris des politiques d'accès conditionnel.
 - La mise au rebut des actifs (quel que soit la confidentialité de ceux-ci) est soumise à la procédure de suppression des informations confidentielles. Cette procédure oblige une suppression logique sécurisée ou une destruction physique des médias ayant contenu des informations confidentielles. Lors de leurs mises au rebut, les médias (disques durs, bandes magnétiques) sont obligatoirement détruits physiquement et de manière sécurisée.
 - En cas de réattribution d'un actif, les données sont supprimées conformément à la procédure de suppression des informations confidentielles. La DSI supprime les données des actifs avant réattribution de ces actifs, à l'occasion d'un renouvellement de matériel. Le sous-traitant fait appel à un prestataire externe spécialisé dans la destruction des données et des actifs physiques, cette destruction est alors matérialisée par un certificat de destruction.
- Sécurité des traitements de reprise de données et répartition des responsabilités.
 - Mise à disposition d'outils d'échanges de données sécurisés : espace sur un serveur FTP accessible en FTPs, espace de stockage accessible (HTTPs) via l'espace privé réservé à chaque client... Suite à la mise à disposition des données par la collectivité, le responsable de la reprise des données s'assurera de la suppression de celles-ci sur l'ensemble des supports de stockage intervenant dans la chaîne de reprise. Les données d'origine pourront toutefois être archivées le temps de l'exécution de la prestation.

3.9 Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à :

- À renvoyer toutes les données à caractère personnel au responsable de traitement dans les conditions spécifiées par celui-ci,
- Détruire, et à en justifier par écrit la destruction, toutes les données à caractère personnel présentes dans ses systèmes d'information, sauf si leur conservation est exigée en vertu de l'article 28 du RGPD.

3.10 Délégué à la protection des données

Les parties engagées communiqueront à chaque signataire les nom et les coordonnées de leur délégué à la protection des données, s'ils en ont désigné un, conformément à l'article 37 du règlement européen sur la protection des données.

3.11 Tenue du registre

Le sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, conformément aux dispositions du RGPD, comprenant :

- Le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
- Les catégories de traitements effectués pour le compte du responsable du traitement ;
- Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- Une description générale des mesures de sécurité techniques et organisationnelles.

Le sous-traitant donnera accès au registre au responsable de traitement sur demande.

IV. OBLIGATIONS DU RESPONSABLE DE TRAITEMENT VIS-A-VIS DU SOUS-TRAITANT

Le responsable de traitement s'engage à respecter le RGPD et toute norme législative ou réglementaire applicable aux données à caractère personnel traitées, et notamment à :

- Donner au Sous-traitant des instructions et finalités de traitement de ses données à caractère personnel conformes au RGPD,

ANNEXE 6 : Charte informatique de la Métropole Toulon Provence Méditerranée

Charte TIC

**Charte pour l'utilisation des technologies d'information et de communication
(TIC).**

Sommaire

ANNEXE 6 : Charte informatique de la Métropole Toulon Provence Méditerranée	1
1.1 Préambule	2
1.2 Application	2
1.3 Principes généraux	3
1.3.1 Responsabilité	3
1.3.2 Confidentialité	3
1.4 Propriété intellectuelle	3
1.5 Contrôle d'accès au système d'information	3
1.6 Système anti-virus et de protection du poste de travail	4
1.7 Terminaux mobiles	4
1.8 Configuration de l'installation informatique	5
1.9 Infrastructure de stockage de fichiers	5
1.10 Espaces Collaboratifs	6
1.11 Connexion Internet	7
1.11.1 Principes	7
1.11.2 Systèmes de tracabilité	8
1.12 Messagerie électronique, documents et poste de travail	8
1.12.1 Principes	8
1.12.2 Contenu des messages électroniques	9
1.12.3 Conditions d'usage	9
1.12.4 Systèmes d'audit	10
1.13 Archivage électronique	10
1.14 Administrateurs Système et Réseau informatique	10
1.15 Sanctions	11
1.16 Avis des représentants du personnel	11
1.17 CNIL	11
1.18 Evolution de la charte	12

1.1 Préambule

La Métropole TPM met à disposition des agents territoriaux, élus et certains intervenants externes habilités, des outils informatiques (système d'information) et de communication (Internet, intranet, messagerie, espaces collaboratifs) essentiels à son activité à des fins professionnelles.

L'information ainsi accessible représente un capital immatériel précieux qui relève de la responsabilité de chacun de protéger.

Un usage inapproprié des outils informatiques et de communication peut entraîner la divulgation d'informations essentielles ou faussées ou peut les rendre indisponibles.

A plus ou moins long terme, ceci peut engendrer par exemple des pertes d'informations, une atteinte à l'image de marque, ou encore une dégradation de la qualité du service public rendu par la collectivité.

Enfin, les infractions aux lois, dont l'essentiel est rappelé en annexe, du fait du comportement répréhensible des utilisateurs dans l'utilisation des outils informatiques et de communication peuvent engager leur responsabilité civile ou pénale en plus de celle de la collectivité.

L'utilisation de ces outils nécessite d'adopter une attitude vigilante et responsable en respectant des règles de conduite et de sécurité que la présente charte vise à définir.

Les raisons qui justifient le renforcement des contraintes d'utilisation sont nombreuses :

- ▶ Maintenir la sécurité du système d'information de la Métropole TPM;
- ▶ Maintenir les performances du système d'information de la Métropole TPM ;
- ▶ Garantir l'intégrité du système d'information de la Métropole TPM;
- ▶ Préserver la confidentialité des données de la Métropole TPM telles que contenues ou accessibles via le système d'information ;
- ▶ Garantir la sécurité des droits privatifs tant de la collectivité que de ses utilisateurs.

Pour ces raisons, la Métropole TPM a défini une charte qui spécifie les règles qui doivent être respectées lors de l'utilisation du système d'information mis à disposition dans le cadre de l'exercice de l'activité professionnelle.

1.2 Application

La présente charte s'applique à toutes les personnes ayant accès aux outils informatiques et de communication, qu'il s'agisse des agents territoriaux, des élus ou de toute personne travaillant pour la Métropole TPM sans être liées à elle par un contrat de travail (sous-traitants, intérimaires, stagiaires, collaborateurs occasionnels).

Toutes ces personnes seront dénommées utilisateurs du SI (Système d'Information) dans ce document.

La Métropole TPM veille à leur donner connaissance de la présente charte et à attirer leur attention sur les conséquences qui s'attacheraient au non-respect de celle-ci.

Même s'il est indispensable de limiter l'utilisation privée des outils informatiques et de communication, la Métropole TPM tolère un usage ponctuel et

raisonnable de l'informatique à des fins personnelles, dans la limite où cela n'impacte ni le temps, ni la qualité du travail et n'expose l'outil informatique à aucune menace virale, attaque malveillante ou fuite d'information.

1.3 Principes généraux

1.3.1 Responsabilité

L'utilisateur est responsable de ses écrits et de ses actes à l'égard des tiers et à l'égard de la Métropole TPM. L'utilisation des outils informatiques et de communication doit donc se faire dans le respect des lois et réglementations en vigueur (dont les principales sont rappelées en annexe), et sans porter atteinte, notamment, à l'ordre public, aux bonnes mœurs et aux droits des tiers.

En particulier, l'utilisateur doit veiller à ne pas tenir de propos diffamatoires. Il ne doit pas transmettre d'informations susceptibles de nuire à l'image de la collectivité ou accéder à des sites internet de même nature ni promouvoir de tels sites.

1.3.2 Confidentialité

L'utilisation des outils informatiques et de communication doit se faire dans le respect de l'obligation générale et permanente de confidentialité et de discrétion qui est demandée à tout utilisateur à l'égard des informations concernant la Métropole TPM. L'utilisateur doit donc veiller, notamment, à ne pas divulguer d'informations sensibles (informations financières, politiques, ressources humaines, marchés publics...).

1.4 Propriété intellectuelle

Tous documents accessibles, notamment sur Internet, quels qu'ils soient, sont susceptibles d'être protégés par un droit de propriété intellectuelle. Il convient donc, pour éviter tout risque de violation des droits d'un tiers, d'être particulièrement vigilant et d'obtenir au préalable l'autorisation de l'auteur ou de ses ayants droit pour toute reproduction ou numérisation de document.

Il est également rappelé que tous les logiciels installés sur le poste de travail doivent respecter le droit de propriété intellectuelle.

1.5 Contrôle d'accès au système d'information

L'accès individuel attribué à l'utilisateur, concrétisé par un nom d'utilisateur et un mot de passe, est strictement personnel.

L'utilisateur est d'une part responsable de la confidentialité de son mot de passe, lequel ne peut en aucun cas être transmis. Il peut être, d'autre part, tenu personnellement responsable de l'utilisation qui sera faite de son accès ou de son compte utilisateur au moyen de son mot de passe.

Le mot de passe ne doit être communiqué à personne, pas même à un agent DRNM (Direction Commune des Systèmes d'Information).

Si un technicien DRNM a besoin, à des fins de dépannage le plus souvent, d'accéder à la session personnelle de l'utilisateur, il doit, avec l'accord de celui-

ci, réinitialiser le mot de passe puis lui permettre de le changer à sa prochaine ouverture de session.

Si par nécessité de service, il est demandé à la DRNM d'intervenir sur la session personnelle d'un utilisateur en son absence, une autorisation formelle sera demandée au DGS.

Le système imposera un changement régulier du mot de passe, qui devra respecter des exigences de complexité et/ou de longueur.

Ces exigences seront communiquées par la DRNM avant application et peuvent évoluer en fonction de l'état de l'art et des recommandations en la matière.

De manière générale, aucune information technique concernant le matériel informatique ou téléphonique de la Métropole TPM ne doit être communiquée à des tiers.

1.6 Système anti-virus et de protection du poste de travail

Le poste de travail (micro-ordinateur fixe ou portable) de chaque utilisateur est équipé d'un logiciel anti-virus. Cependant, l'utilisation des outils de communication (Internet, messagerie) et des supports de stockage (CD-ROM, Clé USB, disque dur externe...) peut, malgré les précautions prises, provoquer la transmission et l'installation sur le poste de travail de l'utilisateur, à l'insu de ce dernier, des programmes ou fichiers qui altèrent ou pillent les données ou logiciels qu'il contient. En cas d'anomalie, l'utilisateur doit stopper l'action en cours et prévenir immédiatement la DRNM.

L'utilisateur ne doit jamais désactiver le ou les systèmes de protection installé(s) par la Métropole TPM.

L'utilisation de médias de stockage amovible type clés USB ou disques durs externes est tolérée sur vos postes de travail, sous réserve de suivre ces recommandations :

- Utilisation de ces périphériques pour transférer des fichiers et non comme stockage, car ils ne sont pas très pérennes dans le temps et peuvent facilement être perdus ou volés.
- Stockage de fichiers non sensibles et non confidentiels : risque de fuite de données en cas de vol
- Scan antivirus systématique de vos clés avant utilisation sur vos ordinateurs professionnels et personnels
- Cryptage systématique des périphériques amovibles hébergeant des données professionnelles (se rapprocher de la DRNM).

1.7 Terminaux mobiles

L'usage des appareils mobiles (smartphones, tablettes, pc portables etc.) permet, en plus d'être joignable, de consulter ses courriels et de naviguer sur internet. Plus encore, il rend possible la connexion au réseau de la collectivité pour travailler sur des applications métier ou accéder à des documents comme tout un chacun le ferait depuis son poste de travail professionnel.

Les terminaux mobiles stockent des données qui sont enregistrées volontairement (courriels, agenda, contacts, photos, documents, SMS, etc.) ou involontairement (cache de navigation, historique de déplacements datés et géo-localisés, etc.). Dans le contexte professionnel de la collectivité, ces données peuvent être sensibles qu'il s'agisse d'un appareil privé ou fourni par nos services.

En complément des mesures de sécurité, la DRNM peut appliquer sur les terminaux mobiles un profil de configuration non modifiable à l'aide d'une solution de « gestion de terminaux mobiles ».

Les mesures de sécurisation peuvent porter sur le contrôle d'accès, la sécurité des applications, la sécurité des données et des communications, la sécurité du système d'exploitation et de l'appareil et la sécurisation du cycle de vie du terminal.

En outre, l'affectation de ce type d'équipement est liée aux besoins de l'utilisateur par rapport à ses fonctions actuelles, la DRNM pourra récupérer ce matériel en cas de changement de service ou de fonctions de l'agent.

1.8 Configuration de l'installation informatique

De manière générale, il est interdit à l'utilisateur de modifier la configuration des outils informatiques installés par la Métropole TPM. A ce titre, l'utilisateur ne doit pas, de son propre chef, ajouter un ou des logiciels supplémentaires ni supprimer des outils implantés sur son poste de travail.

L'utilisateur ne doit pas supprimer les éventuels messages de sécurité prévus pour apparaître en pied de message sur tout message électronique envoyé à partir du poste de travail.

1.9 Infrastructure de stockage de fichiers

Outre les éventuels dispositifs de stockage externes disponibles avec les ordinateurs attribués par la DRNM (graveurs de support magnétique ou optiques, clés USB mémoires, disques durs externes...), d'autres espaces de stockage sont accessibles sur le réseau interne, en fonction des configurations et des situations.

Ces espaces, tels que les serveurs de fichiers, permettent le partage de documents professionnels au sein d'une même entité ou d'un même service, ou encore pour certains d'entre eux, le stockage de documents professionnels confidentiels (stockage dans un espace individuel sur ces serveurs de fichiers). Pour ces raisons, ces espaces sont sauvegardés automatiquement et régulièrement par la DRNM.

Chaque utilisateur doit ainsi veiller à ce que les informations utiles à son service d'appartenance soient stockées dans ces espaces, pour lesquels des dispositions de sauvegarde sont assurées.

Les utilisateurs ne doivent en aucun cas utiliser ces espaces et les serveurs partagés pour stocker et/ou partager tout fichier multimédia (musiques, photos, vidéos) ou autre, qui ne serait pas strictement professionnel.

En tout état de cause, tout stockage de fichier extraprofessionnel ne pourra s'opérer que sur les équipements individuels de l'utilisateur à l'exclusion de tout espace partagé.

Il est rappelé que le disque local du poste de travail de l'utilisateur n'est en général pas sauvegardé et que tout fichier stocké uniquement sur ce média sera perdu en cas de problème matériel. Il est recommandé de stocker ses fichiers sur les serveurs mis à disposition par la DRNM, car ils sont sauvegardés quotidiennement.

L'utilisateur devra s'assurer de la parfaite innocuité de ces fichiers pour les ressources de la collectivité. Il ne devra pas perturber ou limiter les capacités techniques mises à sa disposition à une fin professionnelle et devra respecter l'ensemble des dispositions réglementaires applicables aux contenus stockés ou utilisés (droit d'auteur, droit à l'image, etc.) Ces fichiers ne doivent en aucun cas être susceptibles de porter atteinte à l'image de la Métropole TPM.

En cas de suspicion de non-respect de l'une des dispositions de la Charte concernant les fichiers extraprofessionnels, la Métropole TPM se réserve notamment la possibilité de retirer et/ou d'effacer les contenus stockés, après avoir prévenu l'utilisateur, sauf si ces contenus sont considérés dangereux pour le SI.

L'ensemble des outils informatiques doit être utilisé conformément aux règles et recommandations techniques pouvant émaner de la DRNM de la Métropole TPM. L'utilisateur doit se rapprocher de cette dernière en cas de difficulté ou d'obstacle à l'utilisation des outils et lui déclarer tous les dysfonctionnements suspects.

1.10 Espaces Collaboratifs

La DRNM peut autoriser l'accès à des espaces collaboratifs hébergés sur Internet (Hubic, Dropbox, GoogleDrive etc.), dans la mesure où les conditions suivantes sont respectées :

Pas d'outil professionnel équivalent mis à disposition par la DRNM

Utilisation de la double authentification (couple compte utilisateur/mot de passe + code reçu par SMS ou mail) si proposé par la solution

- Changement des codes d'accès tous les 6 mois minimum
- Respect des principes généraux de responsabilité et de confidentialité exposés au chapitre 1.3 et communication de ces principes aux utilisateurs extérieurs à la collectivité.
- Publication d'information (fichier partagé, article etc.) si possible pour une durée limitée

De même, les espaces collaboratifs professionnels mis à disposition par la DRNM permettront une délégation des droits à des administrateurs fonctionnels qui seront garants des principes énoncés ci-dessus.

1.11 Connexion Internet

1.11.1 Principes

Seuls ont vocation à être consultés les sites présentant un lien direct et nécessaire avec l'activité professionnelle.

Une consultation ponctuelle et dans les limites raisonnables, pour un motif personnel, des sites Internet dont le contenu n'est pas contraire à l'ordre public, aux bonnes mœurs, ne mettant pas en cause l'intérêt et la réputation de la Métropole TPM, ni interdit par la loi, est tolérée.

Les activités exposées ci-dessous, sans que cette liste ne soit exhaustive, sont interdites :

- ▶ La consultation de sites interdits ou dangereux,

Sauf autorisation expresse de la Direction Générale des Services :

- ▶ Les conversations interactives en ligne (« Chat »), sauf pour une utilisation professionnelle.
- ▶ L'écoute de radios ou le visionnage de vidéo en streaming, en dehors de plages horaires éventuellement autorisées ou justification d'utilité dans le cadre professionnel.
- ▶ L'abonnement à des sites payants personnels.
- ▶ L'utilisation de sites de stockage personnel pour entreposer des fichiers,
- ▶ L'accès aux programmes ou sites d'échange de fichiers (dits « peer to peer »).

L'accès à des messageries personnelles est toléré, mais uniquement via webmail.

L'utilisateur doit néanmoins s'assurer de ne pas ouvrir de mails ou de pièces jointes suspects, sa responsabilité pourra être engagée en cas de propagation d'un virus par ce biais.

La DRNM se réserve le droit de couper l'accès au webmails, voire l'accès à Internet lors de pics d'attaque virale

Toute utilisation abusive à des fins personnelles ou toute utilisation interdite peut donner lieu à des sanctions, comme précisé au paragraphe 1.15.

1.11.2 Systèmes de traçabilité

La Métropole TPM a mis en place un système de contrôle permettant notamment :

- L'enregistrement des temps de connexion à Internet par poste et par utilisateur
- L'enregistrement des sites les plus consultés depuis les postes de travail de la Métropole TPM

Ces informations seront conservées pendant 12 mois et ces traitements de contrôle seront déclarés à la CNIL, conformément aux dispositions de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

En outre, la Métropole TPM a installé des systèmes de filtrage de sites, notamment ceux dont le contenu peut être contraire à l'ordre public ou aux bonnes mœurs.

Ce système, obligatoire à mettre en œuvre pour la collectivité, a pour but de protéger la propriété intellectuelle en empêchant le téléchargement d'œuvres contrefaites, d'empêcher l'accès à des sites interdits (apologie du terrorisme, pédopornographie, vente de drogue, d'armes etc).

Cette traçabilité est active pour tous les utilisateurs du SI.

1.12 Messagerie électronique, documents et poste de travail

1.12.1 Principes

L'attribution d'un compte de messagerie électronique ou d'une boîte aux lettres est du ressort de la Direction Générale des Services.

L'attribution d'un compte de messagerie électronique ou d'une boîte aux lettres personnelle est réservée à un usage professionnel.

Un usage ponctuel et raisonnable de la messagerie à titre privé est toléré.

L'agent a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée et, par conséquent, au respect du secret de ses correspondances.

Ainsi, sauf risque ou événement particulier¹ et sous réserve des dispositions relatives au contenu des messages électroniques ci-dessous, la collectivité ne peut ouvrir les messages identifiés par les agents comme personnels et les contenus sur le disque dur du serveur de fichiers ou de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou si celui-ci a dûment été prévenu et convoqué.

¹ Il s'agirait d'une alerte donnée par un centre de veille et d'alerte (CERTA), une autorité compétente de police ou de justice ou d'une commission rogatoire d'un juge à la direction de la Métropole Toulon Provence Méditerranée, ou un fait grave justifiant l'urgence et/ou la mise en danger de la collectivité.

En revanche, la Métropole TPM peut accéder aux messages et fichiers non identifiés comme personnels par les utilisateurs, par exemple dans le cadre d'une absence pour maladie, pour répartition du travail ou continuité du service public.

Remarque : Pour distinguer les documents à caractère privé et ainsi bénéficier du secret des correspondances privées, l'utilisateur doit systématiquement indiquer la mention « personnel » ou « privé » sur les fichiers ou messages envoyés. A défaut d'identification manifeste de cette mention, tout message envoyé ou reçu depuis le poste de travail sera présumé revêtir un caractère professionnel.

Il est également rappelé que tout document, message, donnée, etc. produit à l'aide des outils professionnels mis à disposition par la collectivité est et reste la propriété de celle-ci.

Aussi, tout document, message, etc. ainsi produit doit rester accessible et dans un format compatible à une utilisation ou modification future par la collectivité. Par exemple, il doit être possible d'accéder à tout moment ou à la demande, au document au format word qui a donné naissance à son document équivalent au format pdf.

1.12.2 Contenu des messages électroniques

Un message électronique permet d'échanger des informations à vocation professionnelle et liées à l'activité directe de la collectivité.

Un message électronique peut contenir des textes, des images fixes ou animées à l'exclusion des films, vidéos, sons ou musiques, sauf autorisation expresse de la hiérarchie.

Un message électronique peut contenir des télécopies. Toutes les règles établies par la présente charte s'appliquent à un tel document dès lors qu'il est transmis par la messagerie.

L'utilisateur devra s'assurer que les messages et les pièces jointes respectent les capacités tolérées.

Les messages à caractère injurieux, insultants, dénigrants, dégradants, politiques, religieux ou portant atteinte à la vie privée des personnes et à l'image et à la réputation de la Métropole TPM constituent une faute professionnelle justifiant des sanctions appropriées pour l'utilisateur qui les a produits.

1.12.3 Conditions d'usage

Les activités exposées ci-dessous, sans que cette liste ne soit exhaustive, sont interdites, sauf autorisation expresse de la DGS :

- ▶ la participation à des « chaînes de messages »,
- ▶ l'ouverture de fichiers exécutables « .exe », « .bat », « .cmd »

Toujours prévenir la DRNM en cas de doute sur l'origine d'un mail.

1.12.4 Systèmes d'audit

En raison d'exigences de sécurité particulières, le système d'information ainsi que l'ensemble des moyens de communication qu'il contient et notamment la messagerie électronique doivent être audités à des fins statistiques, de traçabilité, d'optimisation et de détection des abus.

A cet effet, les administrateurs informatiques de la Métropole TPM disposent des droits et pouvoirs spécifiques pour accéder au système d'information.

Lors de l'accès, les administrateurs sont tenus de respecter la confidentialité des informations auxquelles ils accèdent, vis-à-vis des tiers.

Ces informations seront conservées pendant 12 mois et ces traitements de contrôle seront déclarés à la CNIL, conformément aux dispositions de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

1.13 Archivage électronique

Les données (applications métiers, bureautique, messagerie) produites par les utilisateurs dans le cadre de leurs fonctions constituent des archives électroniques.

Elles obéissent à la même réglementation que les archives sur support papier et doivent à ce titre être conservées pendant des délais réglementaires.

Avant de procéder à la suppression de leurs données, il est donc demandé aux utilisateurs de contacter le Service des Archives afin de se renseigner sur leur durée d'utilité et leur sort final.

Enfin, un document validé et donc dans sa version finale est considéré comme archive et ne peut donc pas être stocké en dehors du territoire français : il ne peut donc être archivé que sur un espace propre à la collectivité ou dans un cloud souverain.

1.14 Administrateurs Système et Réseau informatique

Les administrateurs systèmes et réseau sont conduits de par leurs fonctions même à avoir accès à l'ensemble des informations relatives aux utilisateurs.

L'administrateur active sur les systèmes dont il a la responsabilité les journaux nécessaires à l'identification et à la reconstitution des séquences d'événements qui pourraient constituer un incident de sécurité, ou qui pourraient faire l'objet d'une commission rogatoire émise par les autorités judiciaires. Il archive les

données ainsi recueillies dans des conditions propres à en assurer l'intégrité, la disponibilité, l'authenticité et la confidentialité.

Il mène cette activité dans des conditions qui garantissent le respect des lois et des règlements relatifs aux libertés publiques et privées, au secret des correspondances, au droit d'accès à l'information, et il veille notamment à détruire tous les journaux qui comportent des données nominatives à l'expiration d'un délai qui ne peut excéder un an

Plus généralement, les administrateurs sont soumis à une obligation de secret professionnel et à ce titre, ils ne sont pas tenus d'investiguer pour le compte de tiers ou de leur hiérarchie dans les systèmes de contrôle pour des motifs autres que strictement professionnels ou liés à un événement grave concernant la sécurité du système d'information.

Ils sont soumis à une charte spécifique définissant précisément leurs prérogatives, et encadrés par le RSSI (Responsable Sécurité du Système d'Information)

Les responsables d'entités qui voudraient passer outre ces règles de sécurité du système d'information, ou entreprendre des actions qui dérogeraient à ces règles, doivent remettre au RSSI un document écrit et signé par lequel ils assument explicitement la responsabilité de cette dérogation, des risques qui en découlent, et de leurs conséquences.

1.15 Sanctions

Toute violation des règles générales de conduite et d'utilisation des outils informatiques et de communication peut entraîner des sanctions disciplinaires proportionnelles à la gravité des faits, et des poursuites en cas d'actions illégales, dans le respect des lois en vigueur.

Au premier manquement mineur à ces règles, un mail d'avertissement sera envoyé par la DRNM à l'utilisateur.

La Métropole TPM se réserve notamment le droit d'interdire à tout utilisateur l'accès à Internet et aux outils de communication électronique, et de bloquer à tout moment l'accès à ces outils.

1.16 Avis des représentants du personnel

La présente charte a été soumise à l'avis des représentants du personnel, conformément aux dispositions du statut de la fonction publique territoriale.

1.17 CNIL

Conformément à la loi informatique et libertés du 6/01/78, les utilisateurs sont informés que les données collectées font l'objet d'un traitement automatisé. Les utilisateurs disposent d'un droit d'accès et de rectification aux informations les concernant. Ce droit peut s'exercer auprès de la personne ou du service responsable de la protection des données personnelles.

Les nouvelles technologies et notamment les nouveaux périphériques mobiles, permettent de se connecter à son environnement de travail informatique depuis n'importe où et à n'importe quelle heure, il est fortement conseillé de n'utiliser ces fonctionnalités qu'avec parcimonie et pendant ses horaires de travail régulier, à l'exception d'une situation de crise ou d'astreinte.

1.18 Evolution de la charte

La présente charte est rédigée dans l'intérêt de chacun des utilisateurs et manifeste la volonté de la Métropole TPM d'assurer un développement et une utilisation harmonieux et homogènes de son système d'information.

Les évolutions mineures seront notifiées par un message d'actualité dans l'intranet.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiés par la loi 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

Loi 86-1067 du 30 septembre 1986 relative à la liberté de communication

Loi n° 88-19 du 5 janvier 1988 (fraude informatique dite « loi Godfrain »)

Loi n°98-536 du 1er juillet 1998 (protection des bases de données),

Loi n°2000-230 du 13 mars 2000 (adaptation du droit de la preuve aux technologies de l'information et signature électronique),

Loi n°2004-575 du 21 juin 2004 (confiance dans l'économie numérique -LCEN),

Loi du 29 juillet 1881, modifiée (Infraction de presse)

Loi n°84-53 du 26 janvier 1984 (dispositions statutaires relatives à la FPT)

ANNEXE 7 : Résiliation à la convention cadre

DEMANDE DE RESILIATION A LA CONVENTION CADRE D'ECHANGES ET DE GEO-MUTUALISATION

Le correspondant et son suppléant du *<Nom du partenaire>*, est :

- *<Nom et fonction de la personne désignée,>*
- *<Suppléant : Nom et fonction>.*

Fait à le

Signature
(Qualité du signataire pour une personne morale)

.....