Accusé de réception en préfecture
014-211407150-20240627-2024-65-DE
Date de télétransmission : 01/07/2024
Date de réception préfecture : 01/07/2024

cœur côte fleurie
COMMUNAUTÉ DE COMMUNES

ANNEXE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Partie I : Protection des données à caractère personnel :

La présente annexe s'applique pour les services indiqués en sous-traitance dans la colonne RGPD dédiée du catalogue des services. En fonction de l'introduction de nouveaux services, la présente annexe pourra éventuellement être complétée par les dispositions en matière de protection des données personnelles encadrant une responsabilité conjointe/distincte de traitement.

Cas de la sous-traitance

Tous les termes relatifs à la protection des Données Personnelles utilisés dans la présente annexe doivent être interprétés conformément au Règlement Général sur la Protection des Données 2016/679 du 27 avril 2016 abrogeant la directive 95/46/CE (ci-après le « Règlement Européen »).

1. Dans le cadre de l'exécution de la présente convention, LE COORDONNATEUR est amené à effectuer pour le compte de LA COMMUNE des opérations de traitement de données à caractère personnel. Pour toute opération de traitement effectuée par LE COORDONNATEUR pour le compte de LA COMMUNE, les MEMEBRES conviennent que LE COORDONNATEUR aura la qualité de sous-traitant et LA COMMUNE aura la qualité de responsable de traitement au sens du Règlement Européen.

Toutes les Données Personnelles traitées par LE COORDONNATEUR pour le compte de LA COMMUNE sont et demeurent sous la responsabilité exclusive de LA COMMUNE. LA COMMUNE conserve l'entière maîtrise de ses bases de Données, en particulier de ses Données Personnelles.

2. Pour les seuls besoins de l'exécution de la présente convention, LE COORDONNATEUR est autorisé à effectuer les opérations de traitement décrites en Partie II « Description des Traitements de Données confiés AU COORDONNATEUR » et conformément aux instructions documentées fournies par LA COMMUNE. LA COMMUNE se réserve le droit de modifier et/ou de compléter, par écrit et à tout moment, les instructions données.

Le refus DU COORDONNATEUR de se conformer à une instruction de LA COMMUNE constitue un manquement à une obligation essentielle, lequel pourra entraîner la résiliation de plein droit de la présente convention.

Si LE COORDONNATEUR considère qu'une instruction constitue une violation de la réglementation applicable au traitement concerné, elle en informe immédiatement LA COMMUNE qui donnera des instructions plus claires.

3. Les MEMBRES reconnaissent avoir pleine et entière connaissance des obligations de la réglementation relative à la protection des Données Personnelles qui s'appliquent à eux en leur qualité respective de responsable de traitement pour LA COMMUNE et de sous-traitant pour LE COORDONNATEUR.

Chaque MEMBRE indique dans la Partie III l'identité et les coordonnées du contact référent ou Délégué à la protection des données au sein de son organisme en matière de protection des données. Tout changement de contact référent doit être notifié par écrit à l'autre MEMBRE.

4. LE COORDONNATEUR s'engage notamment à respecter les obligations suivantes et à les faire respecter par son personnel, et ses sous-traitants le cas échéant :

Accusé de réception en préfecture
014-211407150-20240627-2024-65-DE
Date de télétransmission : 01/07/2024
Date de réception préfecture : 01/07/2024

- Traiter les Données Personnelles uniquement pour la ou les seules finalités qui font l'objet de la sous-traitance et s'abstenir de tout usage personnel, y compris à des fins prospectives ;
- Garantir la confidentialité des Données Personnelles traitées dans le cadre de la présente convention ;
- Veiller à ce que les personnes autorisées à traiter les Données Personnelles :
    - N'accèdent qu'aux seules Données Personnelles nécessaires à l'accomplissement de leurs activités dans le cadre de l'exécution de la présente convention,
    - Soient soumises à une obligation de confidentialité appropriée,
    - Aient reçu la formation nécessaire en matière de protection des Données Personnelles.
- Communiquer à LA COMMUNE sur simple demande et sans délai, l'ensemble des informations et documents démontrant sa conformité à ses obligations légales et contractuelles ;
- Assister LA COMMUNE dans le respect des obligations auxquelles elle est soumise en qualité de responsable de traitement, notamment à assurer la sécurité des Données Personnelles, à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées et à réaliser toute analyse d'impact relative à la protection des données nécessaire, avec la consultation de l'autorité de contrôle concernée le cas échéant ;
- Permettre la réalisation d'audits et d'inspections par LA COMMUNE ou par tout organisme tiers mandaté par elle à cet effet, afin de contrôler la conformité DU COORDONNATEUR à ses obligations légales et contractuelles en vertu de la présente convention, conformément aux dispositions de l'article **9** de la présente annexe ;
- Restituer ou détruire, à l'issue du traitement et au plus tard à l'expiration de la convention pour quelque raison que ce soit, selon des procédés et modalités convenus préalablement entre les MEMBRES, toutes les Données Personnelles traitées pour le compte de LA COMMUNE, à moins que la conservation desdites Données Personnelles au-delà de la durée du contrat soit justifiée par des dispositions légales ou réglementaires applicables auxdites Données Personnelles et/ou à la conservation de la preuve dans le cadre de tout litige, judiciaire ou extra judiciaire, directement ou indirectement lié à l'exécution des obligations d'un MEMBRE au titre de la présente convention.

  Au regard des contraintes techniques et organisationnelles, les Données à Personnelles traitées dans le cadre de la convention, ne pourront pas être détruites. LE COORDONNATEUR s'engage cependant à ne pas les restaurer depuis les supports sur bandes.

5. LE COORDONNATEUR s'engage également à recourir exclusivement à des sous-traitants ultérieurs présentant les garanties adéquates et sous réserve du respect des conditions suivantes :

- LE COORDONNATEUR peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques (cf Partie V). Dans ce cas, LE COORDONNATEUR informe préalablement et par écrit LA COMMUNE de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement concernées, l'identité et les coordonnées du sous-traitant ultérieur et les dates du contrat de sous-traitance ultérieure et une attestation garantissant la mise en œuvre des obligations relatives à la protection des données à caractère personnel par son sous-traitant ultérieur.
- LA COMMUNE dispose d'un délai de 21 jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ultérieure ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.
- Le sous-traitant ultérieur est tenu de respecter les obligations de la présente annexe pour le compte et selon les instructions de LA COMMUNE ;
- LE COORDONNATEUR demeure pleinement responsable envers LA COMMUNE de l'exécution par le sous-traitant ultérieur de ses obligations.

6. LE COORDONNATEUR s'engage également à recourir exclusivement à des moyens de traitement de données à caractère personnel situés sur le territoire de l'Union Européenne.

Toutefois, LE COORDONNATEUR pourra recourir à des moyens de traitement hors de l'Union Européenne sous réserve du respect des conditions suivantes :

- Elle a notifié LA COMMUNE du transfert envisagé avant le début de celui-ci ;
- Le pays de destination fait l'objet d'une décision d'adéquation par la Commission Européenne ou, à défaut d'une telle décision, le transfert est encadré par des garanties appropriées telles que la signature de clauses contractuelles types adoptées par la Commission Européenne ;
- Le transfert est sécurisé par des moyens techniques et organisationnels adaptés ;
- En tout état de cause, aucun transfert de Données Personnelles hors du territoire de l'Union Européenne ne doit diminuer d'une quelconque manière que ce soit la protection accordée aux personnes concernées par le Règlement Européen et par toute autre règlementation applicable en la matière.

7. LE COORDONNATEUR s'engage à mettre en œuvre et à maintenir les mesures techniques et organisationnelles requises par LA COMMUNE et toutes autres mesures nécessaires pour garantir un niveau de sécurité, d'intégrité et de confidentialité adapté au risque du ou des traitement(s) confié(s) AU COORDONNATEUR, de nature à protéger les Données Personnelles contre une destruction fortuite ou illicite, une perte accidentelle, une altération, une divulgation ou un accès non autorisé.

LE COORDONNATEUR s'engage à tester, analyser et évaluer périodiquement l'efficacité et l'adéquation des mesures techniques et organisationnelles définies en Partie IV et à fournir à LA COMMUNE le rapport d'audit établi ainsi que le plan de remédiation mis en œuvre le cas échéant.

8. Si LE COORDONNATEUR a connaissance ou suspecte la survenance d'une faille de sécurité susceptible d'être qualifiée de violation de Données Personnelles, il s'engage à notifier à LA COMMUNE ladite violation, qu'elle soit avérée ou non, dans un délai maximum de quarante-huit (48) heures après en avoir pris connaissance par le(s) moyen(s) suivant(s) : courriel au contact référent de LA COMMUNE.

Cette notification doit contenir l'ensemble des informations connues sur la faille, conformément aux dispositions du Règlement européen, et doit être accompagnée de toute documentation utile afin de permettre à LA COMMUNE si nécessaire, de notifier cette violation à l'autorité de contrôle compétente et aux personnes concernées. LE COORDONNATEUR s'engage à :
- investiguer l'origine et l'étendue de la faille ;
- informer régulièrement LA COMMUNE des résultats de l'investigation ;
- à définir et adopter, à ses frais, toutes mesures permettant de remédier aux manquements visés ci-dessus dans les plus brefs délais, ainsi que les mesures permettant d'éviter leur survenance dans le futur.

9. LE COORDONNATEUR tient à la disposition de LA COMMUNE la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits (1 audit maximum par an), y compris des inspections, par LA COMMUNE ou un autre auditeur qu'elle a mandaté à ses seuls frais, et contribuer à ces audits. Afin d'être recevable, toute demande d'audit devra être adressée par écrit AU COORDONNATEUR moyennant un préavis de 45 jours avant la date prévisionnelle d'audit.

10. LE COORDONNATEUR s'engage à inscrire le traitement qui lui est confié dans un registre sous-traitant et à le tenir à la disposition de LA COMMUNE et communiquer toutes les informations qui y sont inscrites sur demande.

Accusé de réception en préfecture
014-211407150-20240627-2024-65-DE
Date de télétransmission : 01/07/2024
Date de réception préfecture : 01/07/2024

cœur côte fleurie
COMMUNAUTÉ DE COMMUNES

Partie II : Description des traitements de données à caractère personnel confiés AU COORDONNATEUR :

Traitement : Cloud privé SYSCLOUD

Finalité (objet) du traitement [1]	Mise à disposition d'un serveur own cloud
Catégories de données à caractère personnel [2] [à cocher]	☐ Données d'identification ☐ Données sur la vie personnelle ☐ Informations d'ordre économique et financier ☐ Informations d'ordre professionnel ☒ Données de connexion ☐ Données de localisation ☐ Données de navigation ☐ Données sensibles ☐ NIR ☐ Autres
Catégories de personnes concernées [3]	personnes ayant un compte utilisateur (agents et élus des communes)
Nature des opérations de traitement [4]	Accès, stockage, suppression
Durée du traitement	Durée de la convention + 1 mois

Traitement : Messagerie électronique SYSMSGEX, SECAS

Finalité (objet) du traitement [1]	Mise à disposition d'une boîte mail
Catégories de données à caractère personnel [2] [à cocher]	☒ Données d'identification ☐ Données sur la vie personnelle ☐ Informations d'ordre économique et financier ☒ Informations d'ordre professionnel ☒ Données de connexion ☐ Données de localisation ☐ Données de navigation ☐ Données sensibles ☐ NIR ☐ Autres
Catégories de personnes concernées [3]	personnes ayant un compte utilisateur (agents et élus des communes)
Nature des opérations de traitement [4]	Collecte, conservation, suppression
Durée du traitement	Durée de la convention + 1 mois

Traitement : Accès aux applications SYSAUTHCTRL, SYSPRESTA (AUTHENTIFICATION)

Finalité (objet) du traitement [1]	Administration des accès utilisateurs, habilitations
Catégories de données à caractère personnel [2] [à cocher]	☒ Données d'identification ☐ Données sur la vie personnelle ☐ Informations d'ordre économique et financier ☒ Informations d'ordre professionnel ☒ Données de connexion ☐ Données de localisation ☐ Données de navigation ☐ Données sensibles ☐ NIR ☐ Autres
Catégories de personnes concernées [3]	personnes ayant un compte utilisateur (agents et élus des communes)
Nature des opérations de traitement [4]	Collecte, conservation, suppression
Durée du traitement	Durée de la convention + 1 mois

Traitement : Gestion des incidents SYSPRESTA (AUTHENTIFICATION, SERVEUR APPLICATION), SYSTELEMAINT, SYSCONSEIL

Finalité (objet) du traitement [1]	Gestion des tickets d'incidents, mise en place de services divers, étude, prise de main à distance
Catégories de données à caractère personnel [2] [à cocher]	☒ Données d'identification
	☒ Données sur la vie personnelle
	☒ Informations d'ordre économique et financier
	☒ Informations d'ordre professionnel
	☒ Données de connexion
	☐ Données de localisation
	☐ Données de navigation
	☐ Données sensibles
	☐ NIR
	☒ Autres
Catégories de personnes concernées [3]	personnes ayant un compte utilisateur (agents et élus des communes)
Nature des opérations de traitement [4]	Collecte, accès, stockage, extraction, envoi/communication, suppression
Durée du traitement	Durée de la convention + 1 mois

Traitement : Mise à disposition de machine virtuelle (SYSSRVFILE, SYSSRVAPPWIN, SYSSRVAPPLINUX, SECSUP, SECFWDEDIE, SECFWMUT, SECAV)

Finalité (objet) du traitement [1]	Mise à disposition d'une plateforme d'accueil
Catégories de données à caractère personnel [2] [à cocher]	☐ Données d'identification
	☐ Données sur la vie personnelle
	☐ Informations d'ordre économique et financier
	☐ Informations d'ordre professionnel
	☒ Données de connexion
	☐ Données de localisation
	☐ Données de navigation
	☐ Données sensibles
	☐ NIR
	☐ Autres
Catégories de personnes concernées [3]	personnes ayant un compte utilisateur (agents et élus des communes)
Nature des opérations de traitement [4]	accès, organisation, conservation, suppression
Durée du traitement	Durée de la convention + 1 mois

Traitement : Service d'interconnexion activé (TELBOSITE, O-TELBOWEBMUT, O-TELBOWEBDEDIE)

Finalité (objet) du traitement [1]	Mise à disposition de service d'interconnexion de données de niveaux 2 et 3
Catégories de données à caractère personnel [2] [à cocher]	☐ Données d'identification
	☐ Données sur la vie personnelle
	☐ Informations d'ordre économique et financier
	☐ Informations d'ordre professionnel
	☒ Données de connexion
	☐ Données de localisation
	☐ Données de navigation
	☐ Données sensibles
	☐ NIR
	☐ Autres
Catégories de personnes concernées [3]	personnes ayant un compte utilisateur (agents et élus des communes)
Nature des opérations de traitement [4]	Stockage, routage, filtrage
Durée du traitement	Durée de la convention + 1 mois

Traitement : Service de sauvegarde et de duplication (SYSBKPHL, SYSBKPREPVM)

Finalité (objet) du traitement [1]	Service de mise à disposition de volumétrie de stockage affecté aux sauvegardes
Catégories de données à caractère personnel [2] [à cocher]	☒ Données d'identification
	☒ Données sur la vie personnelle
	☒ Informations d'ordre économique et financier
	☒ Informations d'ordre professionnel
	☒ Données de connexion
	☐ Données de localisation
	☐ Données de navigation
	☐ Données sensibles
	☐ NIR
	☒ Autres
Catégories de personnes concernées [3]	personnes ayant un compte utilisateur (agents et élus des communes)
Nature des opérations de traitement [4]	Accès, conservation, suppression
Durée du traitement	Durée de la convention + 1 mois

[1] : il s'agit de répondre à la question « dans quel but récolte-t-on des données personnelles ? ». Exemple : gestion du recrutement, gestion du foncier, gestion de la demande des usagers, gestion des courriers, …

[2] : données d'identification : état civil, identité, images, etc ;
données sur la vie personnelle : habitude de vie, type de logement, situation familiale, etc ;
informations d'ordre économique et financier : revenus, situation financière, fiscale, etc ;
informations d'ordre professionnel : poste, fonction, etc ;
données de connexion : adresse IP, log, etc ;
données de localisation : déplacement, données GPS, GMS, etc ;
données sensibles : origine raciale ou ethnique, opinion politique, conviction religieuse ou philosophique, orientation sexuelle, santé, appartenance syndicale, données génétiques, données biométriques ;
numéro NIR : numéro d'inscription au répertoire (=numéro de sécurité sociale).

[3] : usager, agent, utilisateur du site internet, candidat à un poste, etc

[4] : il s'agit de répondre à la question « comment vont être exploitées les données personnelles récoltées ? ». Exemple: collecte, stockage, accès, extraction, envoi communication, modification, transfert (hors UE), suppression, …

Accusé de réception en préfecture
014-211407150-20240627-2024-65-DE
Date de télétransmission : 01/07/2024
Date de réception préfecture : 01/07/2024

cœur côte fleurie
COMMUNAUTÉ DE COMMUNES

Partie III : Coordonnées des contacts référents

Contact référent chez LE COORDONNATEUR	Contact référent chez LA COMMUNE
Nom : Agnès MEURIN	Nom : A compléter
E-mail : dpo@coeurcotefleurie.org	E-mail : A compléter
Numéro de téléphone : 0231885449	Numéro de téléphone : A compléter

Partie IV : Mesures techniques et organisationnelles mises en place chez LE COORDONNATEUR :

Dans le cadre de la prestation, LE COORDONNATEUR s'engage à mettre en place des mesures techniques et organisationnelles:

Contrôle d'accès physiques aux sites et installations utilisés pour les Prestations
Objectif : prévenir l'accès non autorisé aux sites et installations utilisés pour / dans le(s) traitement(s) de données

- ☒ Dispositif anti-intrusion (verrouillage des portes, alarmes anti-intrusion)
- ☒ Alimentation électrique de secours garantie des dispositifs physiques de sécurité
- ☒ Dispositif d'authentification à l'entrée des sites (badge, clé, etc.)
- ☐ Procédure d'octroi / retrait des dispositifs d'authentification à l'entrée des sites
- ☒ Stockage des supports de sauvegarde dans un lieu sécurisé
- ☐ Vidéosurveillance
- ☐ Service de gardiennage 24/7
- ☐ Terminaux mobiles rangés dans un lieu sécurisé en dehors des heures de travail
- ☐ Modalités d'accès spécifiques pour les visiteurs (signature d'un registre, badge temporaire, etc.)
- ☐ Certification des *datacenters*
- ☒ Mesures de restriction d'accès supplémentaires aux espaces techniques critiques
    - Salles fermées à clé
    - Vidéosurveillance avec / sans enregistrement
    - Badge avec habilitation spécifique justifiée par un besoin professionnel légitime
- ☒ Politique d'accompagnement des visiteurs dans les locaux
- ☐ Environnement de travail chez le prestataire dédié au client (zone dédiée) avec contrôles d'accès spécifique
    - Badge avec habilitation d'accès spécifique
    - Journalisation de l'activité des badges
    - Isolement (au sein d'une zone dédiée) des collaborateurs travaillant sur des applications / sujets sensibles

Contrôles d'accès logique aux systèmes et outils utilisés pour les Prestations
Objectif : prévenir l'accès non autorisé aux systèmes IT sur lesquels sont traitées les données

- ☒ Journalisation des accès aux systèmes IT
- ☒ Identification des utilisateurs via des comptes utilisateurs nominatifs
- ☒ Limitation du nombre de tentatives d'accès à un compte (blocage du compte utilisateur)
- ☒ Politique robuste de mot de passe (utilisateurs / administrateurs)
- ☒ Politique d'accès aux systèmes IT avec procédure de gestion des habilitations et revue régulière
- ☐ Accès aux systèmes IT uniquement après authentification à double facteur

☒ Sécurisation de l'accès distant aux systèmes IT (VPN, authentification forte, etc.)
☒ Sécurisation du réseau sans fil par le protocole WPA2 ou WPA2-PSK
☐ Terminaux mobiles protégés par chiffrement
☒ Verrouillage automatique des sessions en cas d'inactivité
☒ Mise à jour régulière (automatique ou manuelle) des antivirus et pare-feu
☒ Installation des mises à jour critiques des systèmes d'exploitation sans délai
☒ Installation des mises à jour des applications en cas de faille critique
☐ Procédure d'oubli de mot de passe obligatoire et auditable
☐ Console spécifique d'administration des serveurs sécurisée
☒ SIEM / SOC
☒ Sécurité des interfaces inter-applications (authentification, chiffrement…)

Contrôle de l'accès aux données du Client
Objectif : prévenir tout accès et activité illicites / non autorisés sur les données

☐ Pseudonymisation
☒ Accès restreint aux données aux seules personnes justifiant d'un besoin opérationnel
☒ Accès justifié par un ticket d'assistance ouvert par le Client
☒ Enregistrement des connexions et accès aux données
☐ Formalisation des habilitations d'accès dans une politique

Mesures relatives à la sécurité des transmissions de données connectée
Objectifs : assurer une transmission sécurisée des données et prévenir toute transmission non autorisée

☒ Chiffrement des données transmises par Internet (chiffrement des courriels, connexion sécurisée en transit par cryptage SSL)
☐ Accès à distance via une connexion VPN

Mesures relatives à la sécurité des transmissions de données non connectée
Objectifs : assurer une transmission sécurisée des données et prévenir toute transmission non autorisée lors de l'usage de supports amovibles

☐ Chiffrement des fichiers
☐ Chiffrement des supports

Mesures relatives au contrôle de l'intégrité des données
Objectif : protéger les données contre toute altération et assurer la traçabilité de toute saisie, modification et suppression de données

☒ Journalisation de l'activité des administrateurs systèmes
☒ Journalisation de l'activité des utilisateurs des outils de traitement de données personnelles
☒ Journaux collectés et monitorés par le Cyber SOC, avec scénarios suspects définis
☒ Effacement des données sur les matériels mis au rebut

Mesures relatives à la disponibilité de la Solution et des données
Objectif : prévenir toute perte / destruction, même momentanée, des données, que ce soit accidentel ou intentionnel

☒ Sauvegarde régulière des données avec contrôle de réalisation et de vérification des sauvegardes
☐ Procédure de restauration de sauvegarde avec test régulier

☐ Stockage des supports de sauvegarde sur un site extérieur
☒ Sécurisation des installations techniques :
- Alimentation UPS avec onduleurs
- Détecteurs de fumée
- Contrôle de la température

☒ Utilisation conforme à l'état de l'art de solutions de protection des systèmes
☐ Plan de continuité d'activité avec test régulier
☐ Plan de reprise d'activité avec test régulier

Mesures relatives à la séparation des données du Client
Objectifs : Séparer les données afin d'éviter la propagation d'un éventuel incident à d'autres bases de données ou fichiers

☐ Segmentation logique / physique des données
☐ Sandboxing

Mesures relatives à la sécurité des développements
Objectifs : Éviter une violation de données personnelles en utilisant des données fictives pour effectuer les tests et développements d'applications

☐ Test de développement informatique sur des données fictives ou anonymisées
☐ Formation des développeurs aux principes de la protection des données par défaut et dès la conception et à la sécurité des environnements de développement et recette
☐ Charte de la sécurité dans les développements
☐ Revue de code
☐ Environnements dédiés de développement et test / préproduction
☐ Anonymisation des bases de données de test et recette

Mesures organisationnelles

☒ Procédure de test, d'analyse et d'évaluation de l'efficacité des mesures techniques et organisationnelles (test d'intrusion, scans de vulnérabilité internes et externes, etc.)
☒ Procédure de gestion des incidents de sécurité et des violations de données personnelles
☐ Politique de sécurité formalisée
☐ Charte informatique avec une valeur contraignante pour les salariés
☒ Sensibilisation des utilisateurs à la sécurité
☐ Formation des collaborateurs amenés à travailler sur le(s) traitement(s) de données confié(s) au prestataire
☐ Évaluation régulière des sous-traitants ultérieurs et leurs mesures de sécurité
☐ Plan d'assurance sécurité
☐ Charte informatique administrateur
☐ Le contrat avec des tiers inclut des clauses de sécurité, des SLA et les clauses adéquates en matière de protection des données personnelles
☒ Procédure en cas d'utilisation de supports amovibles

cœur côte fleurie
COMMUNAUTÉ DE COMMUNES

Partie V : Liste des Sous-traitants ultérieurs DU COORDONNATEUR :

Nom du Sous-traitant	Nature de la prestation	Localisation des Données
NEANT	NEANT	NEANT