

Annexe 2 à la convention de gestion des services numériques communs Protection des données à caractère personnel

Préambule

- A. La Commune de Lavérune et Montpellier Méditerranée Métropole ont conclu une « Convention de gestion des services numériques communs » en date du (ci-après le « **Contrat** ») aux termes duquel Montpellier Méditerranée Métropole s'engage à mettre notamment à disposition une plateforme d'e-administration permettant à la Commune de proposer à ses usagers de bénéficier de services dématérialisés, notamment d'effectuer des démarches administratives en ligne, de répondre à des procédures de marchés publics en ligne, d'accéder à des données publiques.
- B. Dans le cadre de l'exécution du Contrat, Montpellier Méditerranée Métropole est amenée à collecter et traiter des données à caractère personnel pour le compte de la Commune, celle-ci revêtant la qualité de responsable de traitement et Montpellier Méditerranée Métropole celle de sous-traitant, au sens de l'article 4 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable entre les Parties à compter du 25 mai 2018 (ci-après dénommé le « **RGPD** »).
- C. Le RGPD impose de nouvelles obligations aux Parties, notamment celle de définir dans le cadre de leurs relations contractuelles les modalités de traitement des données à caractère personnel découlant de l'application de la présente convention

En conséquence dans le cadre de la présente annexe intégrée dans le dispositif contractuel conformément à l'article 12 de la convention de gestion des services numériques communs, il a été convenu ce qui suit :

I. Définitions et principes

- Les termes « **Responsable(s) de traitement** », « **Sous-traitant** », « **personne(s) concernée(s)** », « **donnée(s) à caractère personnel** », « **violation de données à caractère personnel** », « **autorité de contrôle** », et « **traitement(s)** » ont la même signification que celle qui leur est donnée par le RGPD, notamment en son article 4.
- Toute référence à la notion de « donnée » dans la présente annexe et la convention devra également s'entendre de toute donnée à caractère personnel traitée dans le cadre de l'exécution de la Convention.

- Dans le cadre de leurs relations contractuelles, les Parties s'engagent à respecter la réglementation en vigueur applicable aux traitements de données à caractère personnel, notamment le RGPD ainsi que toute réglementation française applicables, telle la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée.

II. Objet

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 découlant des prestations définies dans le Contrat conformément aux dispositions suivantes.

III. Description du traitement faisant l'objet de la sous-traitance

La Métropole, ayant la qualité de « Sous-traitant » au titre de la RPGD, est autorisée à traiter pour le compte de la Commune, ayant qualité de « Responsable de traitement » au titre de la RPGD, les données à caractère personnel nécessaires pour fournir des prestations aux usagers, aux agents et aux élus de la commune, conformément à, l'objet de la présente convention. La nature des opérations réalisées sur les données à caractère personnel consiste en une collecte et une transmission des informations personnelles fournies par les usagers des outils mutualisés.

La ou les finalité(s) du traitement sont

- Pour les e-services la transmission des demandes des usagers aux communes ou aux CCAS
- Pour le parapheur électronique et les outils élus, la mise à la signature électronique de documents et la préparation des conseils municipaux.

Les données à caractère personnel traitées sont :

- Pour les e-services, celles prévues à l'article 3 de l'arrêté du 4 juillet 2013 autorisant la mise en œuvre par les collectivités territoriales, les établissements publics de coopération intercommunale, les syndicats mixtes, les établissements publics locaux qui leur sont rattachés ainsi que les groupements d'intérêt public et les sociétés publiques locales dont ils sont membres de traitements automatisés de données à caractère personnel ayant pour objet la mise à disposition des usagers d'un ou de plusieurs téléservices de l'administration électronique:.
- Pour le parapheur et les outils numériques des élus : état-civil, adresse de contact, groupe politique dans l'assemblée correspondante.

Les catégories de personnes concernées sont :

- Les usagers demandeurs d'une prestation à la commune ou
- les élus et agents utilisateurs du parapheur électronique, des convocations dématérialisées et du porte-document nomade.

Pour l'exécution des obligations visées dans la présente annexe, le Responsable de traitement met à la disposition du Sous-traitant les informations nécessaires suivantes :

- Pour le parapheur et les outils numériques des élus : état-civil, adresse de contact, groupe politique dans l'assemblée correspondante.

IV. Obligations du Sous-traitant vis-à-vis du Responsable de traitement

Le Sous-traitant s'engage à :

- Traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/ont l'objet de la sous-traitance ;
- Traiter les données conformément aux instructions documentées et écrites du Responsable de traitement en application des articles 1 et 2 de la présente convention et de son annexe 1.
- Informer immédiatement le Responsable de traitement si le Sous-traitant considère qu'une instruction donnée par le Responsable de traitement constitue une violation du RGPD ou de toute autre disposition du droit de l'Union Européenne ou du droit des Etats membres relative à la protection des données.
- Dans le cas où 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 Européenne ou du droit de l'Etat membre auquel il est soumis, informer le Responsable de traitement de cette obligation juridique préalablement à la mise en œuvre du traitement considéré, sauf si le droit concerné interdit une telle information pour des motifs d'intérêt public ;
- Garantir la confidentialité des données à caractère personnel traitées dans le cadre du Contrat ;
- Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du Contrat :
 - 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.

V. Sous-traitance

Le Sous-traitant peut faire appel à un autre sous-traitant (ci-après dénommé 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 de Sous-traitants ultérieurs. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du Sous-traitant ultérieur et les dates du contrat de sous-traitance.

Le Responsable de traitement dispose d'un délai minimum de trente (30) jours ouvrés à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le Responsable de traitement n'a pas émis d'objection pendant le délai susvisé.

Le Sous-traitant ultérieur est tenu de respecter les obligations de la Convention et de la présente annexe pour le compte et selon les instructions du Responsable de traitement. Il appartient au Sous-traitant de s'assurer que le Sous-traitant ultérieur présente les mêmes garanties suffisantes que le Sous-traitant lui-même, quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD.

En tout état de cause, si le Sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données à caractère personnel, le Sous-traitant demeure pleinement responsable à l'égard du Responsable de traitement de l'exécution par le Sous-traitant ultérieur de ses obligations.

VI. Droit d'information des personnes concernées

Il appartient au Responsable de traitement de fournir l'information requise par les lois applicables et notamment par le RGPD aux personnes concernées par les opérations de traitement au moment de la collecte des données.

VII. Exercice des droits des personnes

Dans la mesure du possible, le Sous-traitant aidera 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, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Le Sous-traitant s'engage à assister le Responsable de traitement à mettre en œuvre les moyens techniques et organisationnels appropriés pour permettre à la Commune en sa qualité de Responsable de Traitement, de répondre aux demandes reçues des personnes concernées, conformément notamment aux dispositions du RGPD.

Lorsque les personnes concernées exercent auprès du Sous-traitant des demandes d'exercice de leurs droits, il s'engage à adresser ces demandes dès réception au Responsable de traitement par courrier électronique à l'adresse suivante : donneespersonnelles@montpellier3m.fr

VIII. Notification par le Sous-traitant des violations de données à caractère personnel et des failles de sécurité

Le Sous-traitant notifie au Responsable de traitement toute violation de données à caractère personnel dans un délai maximum de quarante-huit [48] heures après en avoir pris connaissance.

Cette notification doit être accompagnée de toute documentation utile afin de permettre au Responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

IX. Aide et assistance du Sous-traitant dans le cadre du respect par le Responsable de traitement de ses obligations

Le Sous-traitant s'engage à aider et assister le Responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.

Le Sous-traitant s'engage à aider et assister le Responsable de traitement pour la réalisation de consultations préalables de l'autorité de contrôle compétente.

X. Mesures de sécurité du Sous-traitant

Le Sous-traitant s'engage, avant tout traitement, à mettre en œuvre les mesures de sécurité techniques et organisationnelles garantissant un niveau de sécurité en conformité avec le référentiel général de sécurité (RGS) en application du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives.

Références : <https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/>

XI. Sort des données

A la cessation des effets de la Convention, pour quelque cause que ce soit, le Sous-traitant s'engage, au choix et selon les instructions du Responsable de traitement, à :

- Détruire toutes les données à caractère personnel ;
- Renvoyer toutes les données à caractère personnel au Responsable de traitement, ou ;
- Renvoyer les données à caractère personnel à un autre sous-traitant désigné par le Responsable de traitement.

Dans cette dernière hypothèse, le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du Sous-traitant. Une fois détruites, le Sous-traitant justifiera par écrit de la destruction.

XII. Délégué à la protection des données

Le Sous-traitant communiquera au Responsable de traitement le nom et les coordonnées de son Délégué à la Protection des Données (ci-après dénommé le « DPD »), s'il en a désigné un conformément à l'article 37 du RGPD.

Nom et coordonnées du DPD:
Eric LEDOUX
Montpellier Méditerranée Métropole
50, place Zeus CS 39556
34961 MONTPELLIER CEDEX 2

XIII. Registre des catégories d'activités de traitement

Le Sous-traitant s'engage à tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du Responsable de traitement comprenant :

- Le nom et les coordonnées du Responsable de traitement, des éventuels Sous-traitants ultérieurs, et, le cas échéant, du DPD ;
- Les catégories de traitements effectués pour le compte du Responsable de 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 RGPD, les documents attestant de l'existence de garanties appropriées ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
 - Le chiffrement des données à caractère personnel ;
 - Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
 - Des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
 - Une procédure visant à tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

XIV. Documentation et audit

Le Sous-traitant met à la disposition du Responsable de traitement, la documentation nécessaire pour démontrer le respect de toutes ses obligations.

XV. Obligations du Responsable de traitement vis-à-vis du Sous-traitant

Le Responsable de traitement s'engage à :

- Fournir au Sous-traitant les données visées au III de l'Avenant ;
- Documenter par écrit toute instruction concernant le traitement des données par le Sous-traitant ;
- Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le RGPD et toute législation applicable en France de la part du Sous-traitant ;
- Superviser le traitement et réaliser, le cas échéant, des audits et inspections auprès du Sous-traitant en collaboration avec celui-ci.

XVI. Loi applicable et juridiction compétente

La présente annexe est soumise à la loi applicable à la Convention de gestion et aux juridictions compétentes telles que visées dans la Convention.