

ANNEXE RGPD

DEFINITION DES REGLES DE LA SOUS-TRAITANCE DES DONNEES A CARACTERE PERSONNEL

SOMMAIRE

ARTICLE 1 – Objet	Page 2
ARTICLE 2 – Cadre légal	Page 2
ARTICLE 3 – Définitions au sens du RGPD	Page 2
ARTICLE 4 – Traitement des données	Page 3
ARTICLE 5 – Obligations du sous-traitant	Page 4
ARTICLE 6 – Modalités de mise en place d’une sous-traitance	Page 6
ARTICLE 7 – Obligations du responsable de traitement envers le sous-traitant	Page 6
ARTICLE 8 – Droits des personnes concernées par le traitement	Page 6
ARTICLE 9 – Notification des violations de données personnelles	Page 7

ARTICLE 1 – Objet

Cette annexe vise à définir les règles applicables à la sous-traitance des données à caractère personnel dans le cadre des marchés publics et les conditions dans lesquelles le sous-traitant, titulaire du marché, s'engage à effectuer pour le compte du responsable de traitement, les opérations de traitement de données à caractère personnel définies ci-après.

La Chambre de Commerce et d'Industrie de La Réunion est responsable du traitement des données personnelles et le titulaire du marché est sous-traitant.

Le sous-traitant doit présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées, assurant le respect des exigences du RGPD, en particulier des droits des personnes concernées.

ARTICLE 2 – Cadre légal

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter les dispositions du Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données, RGPD), et de toute loi ou réglementation française y afférent.

ARTICLE 3 – Définitions au sens du Règlement général sur la protection des données (RGPD)

- **Responsable du traitement :** l'acheteur est considéré comme le " responsable du traitement " en tant qu'autorité publique déterminant les finalités et les moyens du traitement des données.
- **Sous-traitant :** le titulaire est généralement considéré comme le " sous-traitant " en tant que personne traitant des données à caractère personnel pour le compte de l'acheteur.
- **Sous-traitant ultérieur :** le sous-traitant du marché est considéré comme le " sous-traitant ultérieur " en tant que personne à qui le titulaire peut faire appel pour mener des activités de traitement spécifiques.
- **Données à caractère personnel :** toute information se rapportant à une personne physique identifiée ou identifiable exploitée directement ou indirectement par la CCI Réunion dans le cadre de son activité.
- **Typologie des données personnelles :** désignation des catégories de données personnelles traitées par le Prestataire en exécution du contrat.
- **Traitement :** toute opération ou ensemble d'opérations portant sur des données à caractère personnel, automatisée ou manuel, telle que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, la suppression ou la destruction.

- **Finalité** : objectif en vue duquel les données seront collectées, enregistrées, exploitées, transmises, conservées par l'organisme.

ARTICLE 4 – Description du traitement

La présente annexe fait partie du contrat conclu par la CCI Réunion ci-dessous :

- Nature du contrat : (accord-cadre à bon de commande ou autre
- Date :à compléter par le soumissionnaire
- Nom du prestataire :à compléter par le soumissionnaire
- Objet : Commissaire aux comptes CCI Réunion – **2026 -2031**

La CCI Réunion autorise le prestataire à effectuer les traitements suivants :

Traitement	Contrôle conformité des comptes de la CCI Réunion
Finalités	Certification des comptes de la CCI Réunion
Durée du traitement	6 exercices comptables
Données personnelles visées	Nom, prénoms
Personnes concernées	

En vue de sécuriser les (les) traitement(s) de données personnelles dans le cadre de l'exécution de ce contrat, le Prestataire met en œuvre les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque suivantes :

.....A compléter par le soumissionnaire

Mesures garantissant un niveau de sécurité adapté au risque (mettre une croix dans la case Oui ou la case Non)	Oui	Non
Mesures techniques		
Chiffrement des données personnelles		
Pseudonymisation		
Dispositifs permettant de garantir la confidentialité, intégrité, disponibilité et résilience des systèmes		
Moyens permettant le rétablissement des données en cas d'incident		
Procédure de test, d'analyse et d'évaluation de l'efficacité des mesures techniques et organisationnelles mises en place		
Mesures organisationnelles		
Charte informatique		
Politique de sécurité des systèmes d'information (PSSI)		
Formation et sensibilisation des personnels		
Gestion des mots de passe		
Contrôle des accès		
Audit réguliers		
Documentation des actions entreprises pour la protection des données		

Supervision et alerte pour détecter rapidement toute atteinte aux données et en informer le responsable du traitement		
Archivage et suppression des données		
Spécifiques téléphonie		
Protection des communications, gestion des sous-traitants, privacy by design/default		

Ces mesures visent à protéger les données personnelles traitées contre les risques de destruction, de perte, d'altération, de divulgation non autorisée ou d'accès non autorisé, accidentel ou illicite.

ARTICLE 5 – Obligations du sous-traitant

5.1. Respect des instructions de la CCI Réunion

Le sous-traitant s'engage à traiter les données à caractère personnel pour la (les) finalité(s) objet de la sous-traitance et uniquement sur instruction documentée du responsable du traitement.

Le sous-traitant déclare que les données sont hébergées exclusivement sur le territoire de l'Union européenne.

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'Etat membre auquel il est soumis, il doit informer la CCI Réunion de cette obligation juridique avant le traitement.

Le sous-traitant doit informer immédiatement le responsable du traitement si une instruction constitue, selon lui, une violation de la réglementation applicable.

5.2. Garantie de confidentialité

Le sous-traitant doit garantir la confidentialité des données traitées dans le cadre du présent contrat.

Le sous-traitant doit garantir la confidentialité des données en veillant à ce que les personnes autorisées à les traiter soient soumises à une obligation légale ou contractuelle de confidentialité.

Le sous-traitant s'interdit :

- La consultation et le traitement des données autres que celles concernées par les présentes, et ce, même si l'accès des données est techniquement possible.
- De divulguer, sous quelque forme que ce soit, tout ou partie des données exploitées.
- De prendre copie ou de stocker tout ou partie des informations ou données contenues sur les supports ou documents qui lui ont été confiées ou recueillies par elle au cours de l'exécution des présentes, en dehors des cas couverts par les présentes.

5.3. Mesures techniques et organisationnelles

Le sous-traitant doit prendre toutes les mesures techniques et organisationnelles appropriées pour assurer la sécurité des données personnelles.

5.4. Formation du personnel

Le sous-traitant s'engage à ce que toutes les personnes autorisées à traiter les données à caractère personnel aient bien reçu l'information et la formation nécessaires en matière de protection des données à caractère personnel.

5.5. Respect des droits des personnes

Le sous-traitant doit assister le responsable du traitement dans l'exercice des droits des personnes concernées, notamment en matière d'accès, de rectification, d'effacement, de limitation et de portabilité des données.

5.6. Information du Délégué à la protection des données (DPO)

Le sous-traitant communique à la CCI Réunion les nom / prénom et les coordonnées de son Délégué à la protection des données (DPO) s'il en a désigné un conformément à l'article 37 du Règlement européen sur la protection des données : **A compléter par le soumissionnaire**

Nom / prénom :

Adresse postale :

Courriel :

5.7. Création d'un Registre de traitement des données personnelles

Le sous-traitant déclare tenir par écrit un Registre de toutes les activités de traitement effectuées pour le compte de la CCI Réunion comportant les mentions obligatoires :

- a) Le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
- b) Les finalités du traitement ;
- c) Une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
- d) Les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
- e) 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, les documents attestant de l'existence de garanties appropriées ;
- f) Dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;
- g) Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

5.8. Suppression ou restitution des données personnelles

Le sous-traitant supprime ou restitue toutes les données personnelles au terme de la prestation, sauf obligation légale de conservation.

5.9. Audit et contrôle

Le sous-traitant permet au responsable du traitement de réaliser des audits et inspections pour vérifier la conformité au RGPD.

5.10. Résiliation

En cas de manquement par le sous-traitant à ses obligations légales et contractuelles relatives à la protection des données personnelles, le marché peut être résilié pour faute en application de l'article 21 CCP.

ARTICLE 6 – Modalités de mise en place d'une sous-traitance

6.1. Le sous-traitant principal ne peut recruter un sous-traitant ultérieur sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement.

6.2. Le sous-traitant principal doit imposer au sous-traitant ultérieur les mêmes obligations en matière de protection des données que celles qui lui incombent en vertu du présent contrat.

6.3. Le sous-traitant principal doit fournir au responsable du traitement toutes les informations nécessaires concernant le sous-traitant ultérieur, y compris son identité, sa localisation et les traitements qui lui seront confiés.

ARTICLE 7 – Obligations du responsable de traitement envers le sous-traitant

Le responsable du traitement s'engage à :

- Déterminer les finalités et les moyens du traitement des données personnelles.
- S'assurer que le sous-traitant présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées.
- Émettre des instructions documentées claires au sous-traitant.
- Vérifier, pendant toute la durée du contrat, que le sous-traitant respecte ses obligations en matière de protection des données.
- Réaliser des audits ou inspections pour s'assurer de la conformité du sous-traitant.

ARTICLE 8 – Droits des personnes concernées par le traitement

8.1. Droit à l'information des personnes

Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement doit l'informer du traitement opéré.

8.2. Droit d'accès

La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel.

8.3. Droit de rectification

La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes.

8.4. Droit de d'effacement

La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique :

- a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
- b) les données à caractère personnel ont fait l'objet d'un traitement illicite ;
- c) les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis.

8.5. Droit de limitation du traitement

La personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement lorsque l'un des éléments suivants s'applique :

- a) l'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel;
- b) le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation;
- c) le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice;
- d) la personne concernée s'est opposée au traitement en vertu de l'article 21, paragraphe 1, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leur droits, le sous-traitant doit adresser ses demandes dès réception par courriel à l'adresse suivante : dpo@reunion.cci.fr

ARTICLE 9 – Notification des violations de données personnelles

En cas de violation de données à caractère personnel, le sous-traitant notifie au responsable du traitement la violation de données à caractère personnel dans un délai

de 48 après en avoir pris connaissance par lettre recommandée avec accusé réception ou par courriel envoyé à l'adresse suivante : dpo@reunion.cci.fr.

Après accord du responsable du traitement, le sous-traitant notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

La notification doit, à tout le moins :

- a)** décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- b)** communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- c)** décrire les conséquences probables de la violation de données à caractère personnel ;
- d)** décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

Après accord du responsable du traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, la violation de données à caractère personnel, à la personne concernée. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.