

Contrat RGPD

Table des matières

Article Préliminaire. Définitions	1
Article I. Objet	2
Article II. Description du ou des traitements effectués par le Sous-traitant	2
□ L'objet du traitement	3
□ La durée du traitement	3
□ La nature du traitement	3
□ La finalité du traitement	3
□ Les types de données traitées	3
□ Les catégories de personnes concernées	3
Article III. Obligations du Sous-traitant envers le Responsable de traitement	3
III-1. Limitation de l'action du Sous-traitant aux finalités déterminées	3
III-2. Traitement sur instruction documentée du Responsable de traitement	3
III-3. Confidentialité et formation	3
III-4. Mise en œuvre de mesures de sécurité	3
III-5. Notions de « Privacy by Design » et « Privacy by Default » (Protection de la vie privée dès la conception et par défaut)	4
III-6. Recours à un Sous-traitant de la part du Sous-traitant	4
III-7. Notification de violation de donnée	4
III-8. Accompagnement à la réalisation de l'analyse d'impact sur la vie privée	5
III-9. Information à la personne concernée	5
III-10. Coopération dans le traitement des demandes d'exercice de droits des personnes	5
III-11. Transfert de données hors de l'Union Européenne	5
III-12. Sort des données à la fin du contrat / clause de réversibilité	6
III-13. Identification du DPO	6
III-14. Registre des traitements effectués par le Sous-traitant	6
Article IV. Obligations et droits du Responsable de traitement :	6
Article V. Audit de contrôle	7
Article VI. Responsabilité	7

Article Préliminaire. Définitions

« **Données à caractère personnel** », toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique

identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

« **Traitement** », toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

« **Responsable du traitement** », la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;

« **Sous-traitant** », la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. Ce terme est différent de la notion de « sous-traitant » au sens du droit des marchés publics ;

« **Sous-traitant ultérieur** », la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du Sous-traitant ;

« **Violation de données à caractère personnel** », une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Article I. Objet

La présente annexe déroge à l'article 5.2 du Cahier des Clauses Administratives Générales.

Les présentes clauses ont 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 ci-après.

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, c'est-à-dire la **loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**, modifiée ainsi que le **règlement (UE) 2016/679 du Parlement européen et du Conseil 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** (ci-après, « RGPD », « *le règlement général sur la protection des données* »).

Article II. Description du ou des traitements effectués par le Sous-traitant

Le Responsable de traitement recourt à un Sous-traitant afin que celui-ci procède au(x) traitement(s) de données à caractère personnel pour son compte.

Une description du ou des traitements qui seront effectués par le Sous-traitant doit être réalisée dans l'annexe à l'acte d'engagement « Description des traitements sous-traités ». Cette description comportera :

- ☐ L'objet du traitement
- ☐ La durée du traitement
- ☐ La nature du traitement
- ☐ La finalité du traitement
- ☐ Les types de données traitées
- ☐ Les catégories de personnes concernées

Article III. Obligations du Sous-traitant envers le Responsable de traitement

III-1. Limitation de l'action du Sous-traitant aux finalités déterminées

Le Sous-traitant s'engage à ne traiter les données à caractère personnel que pour les seules finalités décrites dans l'annexe à l'acte d'engagement « Description des traitements sous-traités ». Il s'engage notamment à ne pas réutiliser pour son propre compte ou céder à un tiers, les données à caractère personnel recueillies dans le cadre du traitement en objet du présent contrat.

III-2. Traitement sur instruction documentée du Responsable de traitement

Le Sous-traitant s'engage à ne réaliser des traitements que sur les instructions documentées du Responsable de traitement. Ces instructions sont celles dictées par le présent contrat et l'annexe à l'acte d'engagement « Description des traitements sous-traités ». En cas de demande de modification ou de rajout d'un traitement, les instructions correspondantes devront faire l'objet d'un avenant au marché.

Le Sous-traitant informe le Responsable de traitement, dès que possible, lorsqu'il considère qu'une instruction constitue une violation du RGPD.

III-3. Confidentialité et formation

Le Sous-traitant veille à ce que le personnel autorisé à traiter les données à caractère personnel du Responsable de traitement :

- s'engage à respecter la confidentialité ou soit soumis à une obligation légale appropriée de confidentialité ;
- reçoit la formation nécessaire en matière de protection des données à caractère personnel.

III-4. Mise en œuvre de mesures de sécurité

Le Sous-traitant s'engage à mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Le Sous-traitant s'engage à prendre toutes précautions utiles afin de préserver la sécurité des données et notamment de les protéger contre toute destruction accidentelle ou illicite, perte accidentelle, altération,

diffusion ou accès non autorisés, ainsi que contre toute autre forme de traitement illicite ou communication à des personnes non autorisées.

III-5. Notions de « Privacy by Design » et « Privacy by Default » (Protection de la vie privée dès la conception et par défaut)

Le Sous-traitant s'engage à respecter les principes affirmés par le Règlement général sur la protection des données. Cela couvre notamment les notions de « Privacy by design » et de « Privacy by default ».

III-6. Recours à un Sous-traitant de la part du Sous-traitant

Pour l'exécution du contrat, l'Eurométropole autorise le Sous-traitant à recourir à un (ou des) autre(s) Sous-traitant(s) (ci-après, « *Sous-traitant ultérieur* ») listé(s) dans le DC4 annexé aux pièces du marché ou la notification ultérieure en cours de marché. Lorsque le Sous-traitant a recours à un Sous-traitant ultérieur, le premier doit obligatoirement compléter le DC4.

Avant tout recours du Sous-traitant de l'Eurométropole à un Sous-traitant ultérieur qui n'est pas inscrit dans la liste ci-dessus, le Sous-traitant s'engage à informer l'Eurométropole de l'identité du nouveau Sous-traitant. Sans réponse de l'Eurométropole dans un délai de 40 jours calendaires suivant la demande, celle-ci est réputée acceptée.

La demande doit être adressée cumulativement :

- ☐ Au Délégué à la Protection des Données à l'adresse dpo@strasbourg.eu ☐ Au contact habituel du Sous-traitant à l'Eurométropole.

Le Sous-traitant garantit au Responsable de traitement que le Sous-traitant ultérieur auquel il recourt possède des garanties suffisantes quant à la mise en place de mesures techniques et organisationnelles permettant de répondre aux exigences du RGPD.

Le Sous-traitant est responsable envers l'Eurométropole du non-respect des exigences en matière de protection des données à caractère personnel par le Sous-traitant qu'il sollicite.

Les obligations imposées au Sous-traitant dans le présent contrat doivent également être imposées au Sous-traitant ultérieur par contrat.

III-7. Notification de violation de donnée

Le Sous-traitant s'engage à notifier à l'Eurométropole toute violation de données à caractère personnel qu'il constate, ceci dans un délai de 24 heures après en avoir pris connaissance.

Cette notification doit être faite par courrier électronique cumulativement :

- Au Délégué à la Protection des Données à l'adresse dpo@strasbourg.eu ☐ Au contact habituel du Sous-traitant à l'Eurométropole.

La notification sera accompagnée de toute documentation utile afin de permettre à l'Eurométropole de notifier cette violation à la CNIL. Cette documentation devra notamment comporter les éléments suivants :

- la description de 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 ;

- la description des mesures prises ou que le Sous-traitant 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.

III-8. Accompagnement à la réalisation de l'analyse d'impact sur la vie privée

Le Sous-traitant s'engage à conseiller et accompagner l'Eurométropole pour la réalisation d'analyses d'impact relatives à la protection des données. Il mettra notamment à disposition les documentations et renseignements nécessaires à la réalisation de l'étude.

III-9. Information à la personne concernée

L'Eurométropole est responsable de l'information des personnes concernées par le traitement.

Le cas échéant, le Sous-traitant s'engage à fournir les moyens techniques permettant à l'Eurométropole de remplir cette obligation (possibilité d'insertion de mentions sur un formulaire web par exemple).

III-10. Coopération dans le traitement des demandes d'exercice de droits des personnes

L'Eurométropole est chargée de répondre aux demandes d'exercice de leurs droits par les personnes concernées par le traitement.

Le Sous-traitant s'engage à collaborer avec l'Eurométropole pour fournir une réponse à ces demandes si nécessaire (dans le cas d'une demande d'exercice du droit à la portabilité par exemple).

Cependant, toute demande d'exercice d'un droit (accès, rectification, suppression, portabilité) par une personne concernée par un traitement de données à caractère personnel, faite auprès du Sous-traitant, doit être renvoyée à l'Eurométropole dans un délai de 24 heures (jour ouvré) à l'adresse dpo@strasbourg.eu.

III-11. Transfert de données hors de l'Union Européenne

Le Sous-traitant s'engage, par défaut, à stocker les données à caractère personnel qu'il traite exclusivement sur le territoire européen.

Pour l'exécution du contrat, l'Eurométropole autorise le Sous-traitant à transférer les données à caractère personnel, listée(s) à [l'annexe à l'acte d'engagement « Description des traitements sous-traités »](#) hors de l'Union Européenne, s'il existe des garanties permettant d'assurer une protection des données à caractère personnel équivalente à celle de l'Union Européenne.

Avant tout transfert de données hors de l'Union Européenne, qui n'est pas inscrit dans la liste de [l'annexe à l'acte d'engagement « Description des traitements sous-traités »](#), le Sous-traitant s'engage à informer l'Eurométropole du type de données susceptibles d'être transférées, du pays de destination du transfert ainsi que des dispositifs permettant de garantir le maintien permanent du niveau de protection requis par le RGPD. Sans réponse de l'Eurométropole dans un délai de 40 jours calendaires suivant la demande, celle-ci est réputée acceptée.

La demande doit être adressée cumulativement :

- Au Délégué à la Protection des Données à l'adresse dpo@strasbourg.eu
- Au contact habituel du Sous-traitant à l'Eurométropole

III-12. Sort des données à la fin du contrat / clause de réversibilité

En fonction de la demande de l'Eurométropole, le Sous-traitant doit :

- Soit détruire les données de l'Eurométropole que le Sous-traitant a en sa possession.
- Soit restituer ces données. Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du Sous-traitant.
- Soit les transférer à un nouveau prestataire de l'Eurométropole.

Le Sous-traitant garantit un transfert des données à caractère personnel dans des conditions sécurisées afin de garantir leur intégrité et leur confidentialité.

Une fois détruites, le Sous-traitant doit justifier par écrit de la destruction.

Le Sous-traitant dispose de 15 jours calendaires à compter de la date de la demande de l'Eurométropole et en tout état de cause à compter de la fin du contrat liant l'Eurométropole et le Sous-traitant, pour réaliser les actions ci-dessus.

Le Sous-traitant veillera si possible à supprimer les données à caractère personnel contenues dans les sauvegardes sous le même délai. En cas d'impossibilité technique, le Sous-traitant veillera à en informer l'Eurométropole.

III-13. Identification du DPO

Le Sous-traitant communique à l'Eurométropole le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un, conformément à l'article 37 du RGPD.

III-14. Registre des traitements effectués par le Sous-traitant

Le Sous-traitant déclare tenir, par écrit, un registre de toutes les catégories d'activités de traitement effectuées pour le compte de l'Eurométropole comprenant :

- le nom et les coordonnées du Responsable de traitement, 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 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.

Article IV. Obligations et droits du Responsable de traitement :

L'Eurométropole s'engage à :

- s'assurer de la licéité, la limitation et la minimisation des traitements qu'elle opère ;
- 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 règlement européen sur la protection des données de la part du Sous-traitant ;

- superviser le traitement, y compris réaliser les audits et les inspections auprès du Sous-traitant.

Article V. Audit de contrôle

L'Eurométropole, après en avoir avisé le Sous-traitant par écrit avec un préavis minimum de 15 jours calendaires pourra faire procéder, à ses frais, à un audit permettant de s'assurer du respect par le Soustraitant du présent contrat.

Le Sous-traitant s'engage à collaborer de bonne foi avec l'expert désigné par le Responsable de traitement et à lui procurer toutes les informations et documentations nécessaires pour la réalisation de cet audit.

Un exemplaire du rapport d'audit rédigé par l'auditeur sera remis à chaque partie et sera examiné conjointement par les Parties qui s'engagent à se rencontrer à cet effet et à prendre les mesures nécessaires à la correction des manquements aux obligations du contrat.

Article VI. Responsabilité

Le Sous-traitant garantit le Responsable de traitement de l'ensemble des recours contentieux, notamment les appels en garantie, résultant d'une faute exclusivement imputable au Sous-traitant.

Réciproquement, le Responsable de traitement garantit le Sous-traitant de l'ensemble des recours contentieux, notamment les appels en garantie, résultant d'une faute exclusivement imputable au Responsable de traitement.

Le Responsable de traitement et le Sous-traitant supportent, à proportion de leurs fautes respectives, l'engagement de leur responsabilité par un tiers à l'occasion de l'exécution du présent contrat.