

CLAUSE DE PROTECTION DES DONNEES PERSONNELLES

1. CONFORMITE A LA PROTECTION DES DONNEES PERSONNELLES

Toute information transmise à l'occasion de la négociation ou de la mise en œuvre du Contrat ou qui contiendrait, à quelque titre que ce soit, des éléments reconnus par la loi ou la jurisprudence comme liés à la vie privée ou ayant un caractère personnel ou des données permettant d'identifier des individus et/ou des tiers ne pourra être utilisée qu'aux seules fins explicitement prévues lors de sa communication.

Les Parties seront conformes au plus tard le 25/05/2018 au 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.

Dans le cadre de leurs relations contractuelles, les Parties sont tenues de 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 « RGPD »).

Pour les besoins du présent article de cet Avenant/Contrat et des Annexes afférentes à cet article, les Parties sont renommées conformément aux définitions énoncées dans le RGPD comme suit :

- Le Client est dénommé le « Responsable de traitement »,
- Le Prestataire est dénommé le « Sous-traitant » au sens du RGPD.

Le Client reste dans tous les cas propriétaire des données traitées par le Prestataire au titre du Contrat Cadre.

Le Prestataire s'engage à respecter l'ensemble des directives et préconisations dictées par le Client au titre de ces aspects.

1.1 DESCRIPTION DU TRAITEMENT

La description du traitement faisant l'objet de la sous-traitance au sens du RGPD figure en Annexe 1.

1.2 OBLIGATIONS DU SOUS-TRAITANT VIS-A-VIS DU RESPONSABLE DE TRAITEMENT

1.2.1 Le Sous-traitant s'engage à :

- traiter les données uniquement pour la ou les seule(s) finalité(s) figurant en Annexe 1 ;
- traiter les données conformément aux instructions documentées du Responsable de traitement figurant en Annexe 1. Si, selon le Sous-traitant, une de ces instructions constitue une violation du RGPD, il en informe immédiatement le Responsable de traitement. 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 avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants 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 soient soumises à une obligation de confidentialité, et soient formées en matière de protection des données à caractère personnel.

1.2.2 Sous-traitance ultérieure

Le Sous-traitant peut confier la réalisation d'une partie du traitement à un tiers (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 minimum de 5 jours 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 convenu.

Les Sous-traitants Ultérieurs intervenant déjà dans l'exécution des Prestations demeurent autorisés à réaliser les traitements qui leurs sont confiés uniquement si des mesures techniques et organisationnelles ont été prises.

Le Responsable de traitement s'assure 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 RGPD. Si le Sous-traitant Ultérieur ne remplit pas ses obligations en matière de protection des données, le Sous-traitant demeure pleinement responsable devant le Responsable de traitement de l'exécution par le Sous-traitant Ultérieur de ses obligations.

Le Sous-traitant ne peut librement confier tout ou partie de la réalisation du traitement à toute société de son groupe qu'il contrôle ou qui le contrôle au sens de l'article L 233-3 du Code de commerce. L'autorisation du Responsable de traitement doit être obtenue au préalable.

1.2.3 Droit d'information des personnes concernées

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

1.2.4 Exercice des droits des personnes concernées

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, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées exercent auprès du Sous-traitant des demandes d'exercice de leurs droits, le Sous-traitant doit adresser ces demandes dès réception par courrier électronique au Responsable de traitement.

1.2.5 Notification des violations de données à caractère personnel

Le Sous-traitant notifie au Responsable de traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir eu connaissance et par tous moyens écrits y compris les correspondances électroniques. Il convient que le Sous-traitant transmette au responsable de traitement la nature de la violation des données à caractère personnel ; le nombre approximatif de personnes concernées ; le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact ; la description des conséquences probables de la violation des données à caractère personnel ; la description des mesures prises ou que le Responsable de traitement propose de prendre pour remédier à la violation des données à caractère personnel, y compris, le cas échéant, les mesures pour atténuer les éventuelles conséquences négatives afin de permettre au Responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

1.2.6 Mesures de sécurité

Le Sous-traitant s'engage à mettre en œuvre les mesures de sécurité arrêtées d'un commun accord avec le Responsable de traitement et définies en Annexe 2.

1.2.7 Sort des données

Au terme des Prestations de service relatives au traitement de ces données ou à l'issue du Contrat, les Parties définiront d'un commun accord le sort des données personnelles : destruction, restitution ou conservation en fonction de la réglementation applicable, des possibilités techniques, des options de prestations retenues et des coûts financiers associés. La restitution des données à caractère personnel doit se faire selon le format imposé par le Responsable de traitement défini au moment de ladite restitution. Le Sous-traitant s'engage à détruire les données dans un délai de 15 (quinze) jours après accord du Responsable du traitement ayant vérifié l'effectivité de la restitution complète des données.

1.2.8 Registre des catégories d'activités de traitement

Le Sous-traitant déclare 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 pour le compte duquel il agit, des éventuels Sous-traitants Ultérieurs et, le cas échéant, du délégué à la protection des données (DPO) du Responsable de traitement lequel est défini en Annexe 1;
- Les catégories de traitements effectués pour le compte du Responsable du traitement ;
- Les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale implique que le Sous-traitant fournisse au Responsable de traitement les documents attestant de l'existence de garanties appropriées.

1.2.9 Documentation / audit

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 permettre la réalisation d'audits, y compris des inspections, aux frais du Responsable de traitement. Toutefois, en cas de manquement à ses obligations prévues au §1.2.1, les coûts incomberont au Sous-traitant. L'audit sera mené par le Responsable du traitement ou un auditeur qu'il aura mandaté, non-concurrent du Sous-traitant, soumis à une obligation de confidentialité.

Le Responsable de traitement s'engage à notifier par écrit avec un préavis minimum de quinze (15) jours au Sous-traitant tout audit, en lui communiquant notamment l'objet de la mission, sa durée envisagée, et le nom du ou des expert(s) détaché(s).

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 d'un jour/homme par an dans le cas d'un audit portant sur le registre des traitements. Toutefois, concernant un audit de la sécurité logistique du système d'hébergement, le périmètre et la durée seront définis d'un commun accord (au cas par cas). 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 le rapport d'audit dans le cadre du comité de pilotage, et identifieront, le cas échéant, les actions à engager par l'une ou l'autre des Parties pour mettre en œuvre les décisions prises lors de ce comité.

1.2.10 Aide du Sous-traitant

Par ailleurs, 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 notamment dans la réalisation d'analyses d'impact relatives à la protection des données, ainsi que pour la préparation de la consultation préalable de l'autorité de contrôle.

2. 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 personnelles traitées, et notamment à :

- Respecter le principe de limitation des données personnelles nécessaires au regard des finalités de traitement. Le Responsable de traitement s'engage à minimiser autant que possible la collecte des données à caractère personnel, et en tout état de cause à confier ensuite au Sous-traitant que les données personnelles strictement nécessaires à l'exécution des Prestations. Aussi, quand la prestation permet de travailler sur des données non réelles, le Client s'engage à ne confier au Prestataire que des données personnelles non réelles.
- S'assurer que les traitements et leurs finalités sont conformes au RGPD,
- Fournir au Sous-traitant la description du traitement et les instructions associées, qui figurent toutes deux en Annexe 1 ; toute modification de l'Annexe 1 devra faire l'objet d'un avenant au Contrat,
- Veiller, au préalable et pendant toute la durée du traitement, au respect par le Sous-traitant des obligations prévues par le RGPD, dont notamment les dispositions de l'article 25 dudit règlement,
- Superviser le traitement, y compris réaliser les audits et les inspections auprès du Sous-traitant, selon les conditions et modalités visées ci-dessus (article 4.2.9 « Documentation / audit »).

3. DONNEES PERSONNELLES « COLLECTEES » PAR LE PRESTATAIRE EN QUALITE DE RESPONSABLE DU TRAITEMENT

Le Prestataire est amené dans le cadre de l'exécution du Contrat à traiter des données personnelles relatives aux employés ou dirigeants du Client (notamment les contacts techniques et commerciaux), ce qui peut inclure en particulier mais de façon non limitative les informations de type, nom, adresse ou numéros de téléphone professionnels, adresse mail. Ces informations seront collectées auprès du Client. Le traitement de ces données est indispensable à la relation entre les Parties et à l'activité du Prestataire, à des fins de communication entre les équipes.

Le Prestataire, en qualité de responsable de traitement de ces données personnelles, s'engage à ne traiter ces données que dans la mesure où cela est strictement nécessaire à la réalisation des Prestations décrites au Contrat, et s'engage à ce titre à respecter les dispositions légales applicables en la matière, et notamment mettre en œuvre toutes les mesures techniques et d'organisation appropriées pour assurer la protection des données contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés ainsi que contre toute autre forme de traitement illicite.

Annexe 1 : La description du Traitement des Données à caractère personnel

1. Finalité du traitement

La/les finalité(s) du traitement des données à caractère personnel sont les suivantes :

2. Nature des opérations réalisées sur les Données à caractère personnel

Les opérations réalisées sur les données à caractère personnel sont les suivantes :

(Stockage etc.)

3. Type de Données à caractère personnel traitées

Les données à caractère personnel traitées dans le cadre du Contrat sont les suivantes :

(Nom, prénom, @IP ou autre)

4. Catégorie des personnes concernées

Les catégories de personnes concernées dont les Données à caractère personnel sont traitées dans le cadre du Contrat sont :

5. Durée du traitement et de conservation des Données à caractère personnel

Le prestataire ne conservera pas les Données à caractère personnel du Client plus longtemps que la durée convenue avec le Client, dans le respect des Lois et Règlements applicables aux Données à caractère personnel.

Si aucune durée de conservation n'a été définie, alors la durée de conservation des Données à caractère personnel est limitée à la durée du Contrat, en tenant compte des Lois et Règlements applicables aux Données à caractère personnel.

6. Sous-traitance

Liste exhaustive

Toute modification dans la liste des sous-traitants devra être acceptée par le Client et formalisée par voie d'avenant.

7. Transfert international des Données à caractère personnel

Le Prestataire ainsi que le ou le(s) sous-traitants qu'il emploie dans le cadre du Contrat ou le ou les sous-traitant(s) ultérieurs ne doivent pas transférer à des fins de traitement, d'hébergement ou d'octroi d'un accès à distance, sans l'accord écrit et préalable du Client, en dehors des pays de l'Union Européenne et des pays reconnus par la Commission Européenne comme des pays assurant une protection adéquate à la date du transfert en question.

Par ailleurs, le Prestataire ou le ou le(s) sous-traitants qu'il emploie dans le cadre du Contrat ou le ou les sous-traitant(s) ultérieurs doivent s'assurer que le nouveau centre de traitement des Données Personnelles dispose d'une infrastructure technique d'un niveau de sécurité et de conditions d'exploitation au moins équivalents à ceux fournis par le centre de traitement initial et, en tout état de cause, en conformité avec le présent Contrat.

Annexe 2 : MESURES DE SECURITE TECHNIQUES ET ORGANISATIONNELLES