ANNEXE PROTECTION DES DONNEES PERSONNELLES

1. OBJET

En application de l'article 14 des Conditions Générales de Vente Kosmos, la présente annexe a pour objet de stipuler les engagements de Kosmos dont les mesures techniques et organisationnelles déployées par ses soins, afin d'assurer la protection des données à caractère personnel du Client et la conformité des traitements objets du Contrat à la réglementation applicable (Règlement n°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 abrogeant la directive 95/46/CE (« RGPD ») et loi n°78-17 du 6 janvier 1978 modifiée (ci-après ensemble « Règlementation »). En aucun cas la responsabilité de Kosmos ne saurait être engagée du fait d'un refus de Kosmos de procéder à un Traitement non conforme à la Règlementation. La présente Annexe est convenue conformément à l'article 28 du RGPD.

2. DEFINITIONS

Sauf indication contraire, les définitions figurant dans le RGPD, en particulier les termes « *Responsable du traitement* », « *Sous-traitant* », « *Finalités* », « *Destinataires* », « *Personne concernée* », « *État membre* », « *Données à caractère personnel* », « *Violation de données à caractère personnel* », « *Traitement* », et « *Autorité de contrôle* », s'appliquent.

« *Données Personnelle* » dans le présent contexte désigne toute donnée à caractère personnel, telle que définie au RGPD, traitée par Kosmos pour le compte du Client en application ou dans le cadre du Contrat. Ces Données Personnelles incluent, selon précisions de la Sous-annexe 1 les Données Personnelles collectées, traitées ou hébergées par Kosmos en tant que Sous-traitant du Client dans le cadre de l'exécution des Services objets du Contrat.

En outre, Kosmos est susceptible de collecter et traiter des données à caractère personnel de préposés du Client en tant que Responsable de traitement dans le cadre de la formation et du suivi du Contrat.

3. QUALIFICATION DES PARTIES

La présente Annexe couvre l'ensemble des Services fournis par Kosmos, qu'il s'agisse (i) de Services SaaS, (ii) de Services informatiques récurrents (Support, TMA) ou ponctuels et plus généralement toute intervention de Kosmos sur les Données Personnelles du Client.

Dès lors que les Données Personnelles sont traitées ou hébergées sur les serveurs ou systèmes d'information de Kosmos, les mesures techniques et organisationnelles décrites en Sous-annexe 2 s'appliquent. Si les Données Personnelles sont traitées ou hébergées sur le système d'information du Client ou de tout tiers sous la responsabilité du Client, il appartient au seul Client d'assurer la protection desdites Données Personnelles, l'engagement de Kosmos se limitant à leur protection dans le cadre de leur manipulation par ses préposés dans le cadre des Services.

Au sens de la présente Annexe, Kosmos est le Sous-traitant du Client, qui est Responsable des traitements. La Sous-Annexe 1 présente le détail des (i) Finalités des Traitements confiés à Kosmos, (ii) catégories de Données Personnelles traitées par Kosmos, (iii) catégories de Personnes concernées par les Traitements et (iv) délais d'effacement (durée de conservation) des Données Personnelles par Kosmos.

Il appartient au Client de déterminer les destinataires tiers auxquels sont envoyées les Données Personnelles le cas échéant, et à indiquer les coordonnées de ces destinataires à Kosmos. Cette dernière n'est pas responsable de la protection des Données Personnelles par lesdits destinataires, ce que le Client reconnaît.

En cas de modification d'un Traitement, les Parties conviendront des éventuelles modifications à la Sous-Annexe 1 nécessaires pour répondre aux exigences de la Règlementation.

Sauf base légale distincte applicable à Kosmos en tant que Responsable de traitement, Kosmos n'intervient sur les Données Personnelles définies en Sous-annexe 1 qu'en application des Finalités définies en Sous-annexe 1, dans le cadre des Services qu'exécute Kosmos tels que définies au Contrat et des Traitements correspondants à ces Services uniquement.

4. MODALITES DE TRAITEMENT DES DONNEES PERSONNELLES PAR KOSMOS

Kosmos s'engage à ne traiter les Données Personnelles dans le cadre du Contrat que (i) conformément aux instructions documentées du Client, (ii) dans le respect et la limite des Finalités stipulées, (iii) dans le respect des mesures techniques et organisationnelles décrites à la présente Annexe, et (iv) pendant la ou les durée(s) de conservation stipulées.

Kosmos met en œuvre les mesures techniques et organisationnelles appropriées afin (i) d'empêcher le traitement non autorisé ou illicite des Données Personnelles, (ii) d'empêcher la perte, la destruction ou la détérioration d'origine accidentelle des Données Personnelles, (iii) d'assurer la sensibilisation et la formation de ses préposés à la protection des données à caractère personnel dans le cadre de leurs fonctions, et (iv) d'assurer que seuls ceux de ses collaborateurs et éventuels sous-traitants ayant à en connaître dans le cadre des Services accèdent aux Données Personnelles. Les mesures de sécurité techniques et organisationnelles mises en œuvre sont décrites à la Sous-annexe 2 (ci-après les « Mesures »).

En reconnaissant que les Mesures sont soumises à des progrès et évolutions techniques, les Parties conviennent que Kosmos est autorisée à apporter des améliorations aux Mesures, à condition que ces Mesures ne se situent pas en-deçà du niveau de sécurité prévu en Sous-annexe 2 et qu'elles soient conformes à l'état de l'art. Kosmos tiendra à la disposition du Client la description de tout changement significatif des Mesures auquel elle procéderait.

Dans la mesure où le Contrat porte sur la fourniture par Kosmos d'une Solution logicielle, Kosmos prend en compte dès sa conception ou dans le cadre de son évolution technique les principes de sécurité, de confidentialité, de minimisation et de protection des données à caractère personnel.

En cas de Service effectué par Kosmos sur le système d'information du Client, le Client est seul responsable des mesures techniques et organisationnelles ainsi que de sécurité entourant les Données Personnelles stockées sur son système d'information, Kosmos et le Client convenant d'une politique de gestion des accès des préposés de Kosmos en considération des exigences de la Règlementation.

5. GESTION DES DROITS DES PERSONNES CONCERNEES

Les Parties reconnaissent et conviennent qu'il incombe juridiquement au Client, en tant que Responsable de traitement, de traiter les demandes des Personnes concernées liées à leurs droits sur leurs Données Personnelles tels que définis par la Règlementation (droit à l'information, droits d'accès, de rectification, d'effacement, d'opposition, de limitation, de portabilité ou de révocation d'un éventuel consentement), concernant le Traitement des Données Personnelles effectué, et que Kosmos n'est pas tenue elle-même d'y donner suite directement, sauf obligation contraire imposée par des instructions documentées du Client.

Si le Client peut accéder directement aux Données Personnelles des Personnes concernées (notamment dans le cas de la fourniture d'une Solution), le Client prend lui-même en charge les demandes des Personnes concernées, selon des procédures qu'il détermine sous sa responsabilité. Le Client peut solliciter l'assistance de Kosmos dans l'identification des Données Personnelles et le traitement des demandes, par écrit.

Dans la mesure où la demande d'une Personne concernée parviendrait directement à Kosmos dans le cadre des Services, Kosmos l'adresse dans les meilleurs délais au Client afin que celui-ci statue sur la demande et apporte la réponse à la Personne concernée. Dans tous les cas, le Client est seul responsable de l'opportunité de la réponse à apporter à la Personne concernée, d'établir son identité, de solliciter des informations complémentaires, d'identifier d'éventuelles exceptions s'opposant à la demande, ou de refuser de donner la suite à la demande pour des motifs légitimes que le Client détermine et communique lui-même à la Personne concernée.

En cas de litige avec une Personne concernée ou en cas d'autres actions engagées par une Personne concernée eu égard au Traitement de Données Personnelles confié à Kosmos, le Client en informera Kosmos dans les meilleurs délais, et Kosmos apportera sa coopération et fournira au Client toutes informations utiles dans ce cadre.

6. GESTION DES VIOLATIONS DE DONNEES PERSONNELLES

Kosmos s'engage à mettre en œuvre un dispositif de détection des éventuelles Violations de Données Personnelles survenant sur son système d'information dans le cadre des Services. En cas de Violation de Données Personnelles constatée sur son périmètre d'intervention, Kosmos s'engage à (i) alerter le Responsable de traitement dans les meilleurs délais, (ii) mettre en place toute solution palliative limitant ou supprimant la Violation de Données Personnelles et (iii) investiguer les raisons de la Violation constatée.

En tant que de besoin et dans la mesure du possible, la notification adressée par Kosmos au Client inclura les informations demandées par l'article 33 du RGPD permettant de décrire (i) la nature de la Violation de Données à caractère personnel, (ii) les catégories de Données à caractère personnel et le ou les Traitement(s) en cause, (iii) le nombre et les catégories de Personnes concernées, (iii) l'origine et les conséquences prévisibles de la Violation pour les Personnes concernées et (iv) les mesures mises en œuvre pour mettre un terme à la Violation de Données à caractère personnel et tenter d'en limiter ou supprimer les conséquences. A défaut, Kosmos indiquera à quel terme les informations complémentaires seront fournies, notamment en cas d'investigation technique menée par Kosmos ou son Sous-traitant ultérieur.

Dans ce contexte, Kosmos n'est pas autorisé à notifier une Violation de Données à caractère personnel directement à l'Autorité de contrôle, aux Personnes concernées ou à d'autres tiers, à moins que Kosmos y soit tenue par le droit applicable. Hors ces cas, il appartient au seul Client, en tant que Responsable de traitement, de décider et de procéder aux notifications qui s'imposeraient, par tout moyen de son choix, auprès de l'Autorité de contrôle, et auprès des Personnes concernées en cas de risque pour leurs droits et libertés déterminé par le Responsable de traitement.

7. ASSISTANCE AU RESPONSABLE DE TRAITEMENT

Kosmos alerte le Client par écrit si elle constate une non-conformité manifeste entre les besoins exprimés par le Responsable de traitement dans le cadre du Contrat, et les exigences de la Règlementation. Cependant, en aucun cas Kosmos ne peut être tenue responsable (i) des non-conformités des Traitements du fait du Responsable de traitement ou (ii) de l'absence de détection d'une non-conformité qui ne serait pas grave et manifeste.

Kosmos apporte son assistance au Responsable de traitement (i) en répondant aux questions orales ou écrites du Responsable de traitement relatives aux Traitements, (ii) en cas de demande ou d'enquête d'une Autorité de contrôle et (iii) en cas d'analyse préalable d'impact menée sur le périmètre des Traitements en cause. A cette fin, Kosmos tient à la disposition du Client la documentation relative au respect de ses engagements dans le cadre de la présente Annexe.

En tant que de besoin, Kosmos rappelle au Client que le traitement de données à caractère personnel incluant des données « particulières » au sens de la Règlementation, des données à caractère personnel de personnes « vulnérables » telles que des mineurs, ou encore des traitements de données personnelles à grande échelle, ou de profilage comportemental, une analyse d'impact préalable peut être nécessaire, Kosmos s'engageant le cas échéant à apporter son concours à la ladite analyse s'agissant du périmètre des Traitements qui lui sont confiés par Contrat et des ressources mises en œuvre par ses soins à cet effet.

8. AUDIT

Une (1) fois par an moyennant un préavis écrit raisonnable, le Responsable de traitement aura la faculté de diligenter un audit portant sur la mise en œuvre par Kosmos des Mesures stipulées à la présente Annexe, sur le seul périmètre des Données Personnelles et Traitements liées au Contrat, à l'exclusion (i) de tout élément du système d'information de Kosmos non concerné par le Contrat, (ii) de toute donnée personnelle des autres clients de Kosmos, (iii) de tout élément constitutif du secret d'affaires ou du secret industriel de Kosmos, et (iv) dans le respect de la propriété intellectuelle, des procédures de sécurité, de la disponibilité des collaborateurs et de la production normale de Kosmos.

Kosmos devra valider au préalable l'identité de l'auditeur, et pourra le récuser s'il appartient à une entreprise concurrente de Kosmos. Le coût de l'audit est à la charge du Client. Si l'audit identifie une non-conformité aux engagements de Kosmos, celle-ci y remédie dans les meilleurs délais et en adresse confirmation écrite au Client. En toute hypothèse, le rapport d'audit est transmis par écrit à Kosmos, qui pourra faire valoir ses observations.

9. RECOURS A UN SOUS-TRAITANT ULTERIEUR

Kosmos peut faire intervenir un prestataire tiers aux fins d'exécution de tout ou partie des Services (ci-après le « Sous-traitant ultérieur »), à la condition que celui-ci (i) soit soumis à l'approbation préalable expresse du Client, et qu'il (ii) s'engage contractuellement auprès de Kosmos à assurer dans le cadre de son intervention la protection des Données Personnelles de manière substantiellement conforme aux exigences de la présente Annexe.

A la date de signature du Contrat, le Client est informé et approuve expressément le recours au(x) Sous-traitant(s) ultérieur(s) suivant(s) stipulés à la Sous-annexe 1, pour l'exécution des Traitements visés. Tout recours ultérieur à un autre Sous-traitant ultérieur impliquera le respect de la procédure suivante.

Kosmos informera au préalable, par voie écrite, le Client du projet de désignation d'un nouveau Sous-traitant ultérieur, précisant la dénomination, l'adresse et les coordonnées du Sous-traitant ultérieur ainsi que les aspects des Traitements dont ledit Sous-traitant ultérieur sera en charge et notamment s'il implique un flux transfrontalier des Données Personnelles. Si, dans un délai de huit (8) jours calendaires à compter de la réception de cette notification, le Client exprime par écrit des objections légitimes et motivées à la désignation du Sous-traitant ultérieur en cause, Kosmos échangera avec le Client afin de répondre aux objections soulevées par celui-ci et, s'il n'est pas possible de s'entendre sur de telles mesures, Kosmos ne nommera pas le Sous-traitant ultérieur proposé. A défaut, le Sous-traitant ultérieur présenté sera accepté par le Client.

En cas de manquement par le Sous-traitant ultérieur à ses obligations contractuelles, Kosmos demeure responsable devant le Client dans les conditions stipulées au Contrat.

10. Gestion des flux transfrontaliers de Donnees Personnelles

Par défaut, Kosmos s'engage à n'effectuer les Traitements des Données Personnelles que sur le territoire de l'Espace Economique Européen (« EEE »). Cependant, dans le cas où les Services (dont l'éventuel recours à une Sous-traitant ultérieur) impliquent un transfert des Données Personnelles en dehors de l'EEE, Kosmos (i) en tient le Client informé et (ii) s'assure au préalable que ledit transfert est effectué dans le cadre de garanties conformes aux exigences de la Règlementation, telles que clauses contractuelles types édictées par la Commission européenne ou l'Autorité de contrôle, règles contraignantes d'entreprise, décision d'adéquation de l'Autorité de contrôle ou tout autre dispositif autorisé par la Règlementation, dont Kosmos tiendra l'exposé à la disposition du Client à première demande.

A la date de signature du Contrat, le Client est informé et approuve expressément les transferts stipulés à la Sous-annexe 1, pour l'exécution des Traitements visés.

11. Donnees Personnelles des collaborateurs des Parties

Dans le cadre de la conclusion et de la gestion opérationnelle et comptable du Contrat, chacune des Parties peut également accéder aux Données Personnelles de certaines catégories de personnes (signataire du Contrat pour le Client, contacts opérationnels, contacts juridiques, contacts comptables, etc.). Chaque Partie s'engage, en tant que Responsable de traitement, à protéger et n'utiliser les Données Personnelles de ces contacts de l'autre Partie qu'aux fins de gestion du Contrat, et à leur appliquer les mesures techniques organisationnelles appropriées pendant toute la durée du Contrat. Les Données Personnelles de ces contacts seront supprimées par chaque Partie à la fin du Contrat, sous réserve d'une conservation prolongée en cas d'obligation légale d'archivage ou de conservation de la preuve.

12. Communication avec l'Autorite de controle

Dans la mesure où le droit applicable le permet, Kosmos informera dans les meilleurs délais le Client en cas d'enquête, mise en demeure ou autre procédure susceptible de porter sur des Traitements qu'elle effectue des Données Personnelles du Client par une Autorité de contrôle ou toute autre autorité publique. Le cas échéant les Parties s'apportent assistance mutuellement pour assurer une communication cohérente avec l'Autorité concernant toute enquête de celle-ci. En cas de litige, d'injonction ou d'amende imposée ou envisagée par l'Autorité de contrôle ou une autre autorité compétente concernant les Traitements des Données Personnelle contre l'une ou l'autre des Parties ou les deux, les Parties doivent s'informer sans délai dans le but de se défendre efficacement contre ces actions ou les régler à l'amiable en temps opportun.

13. Sort des Donnees Personnelles en fin de Contrat

Kosmos conserve les Données Personnelles du Client (i) pendant la ou les durées définies par le Client à la Sous-annexe 1, et (ii) en tant que de besoin, pendant toute la durée du Contrat augmenté des durées légales de preuve et prescription.

Sans préjudice de ce qui précède, et à concurrence des exigences liées à l'exécution des Services, Kosmos procède à la suppression des Données Personnelles lorsque la ou les durée(s) définie(s) par le Client parvien(nen)t à échéance ou (ii) sur demande expresse du Client, ou (iii) sur demande documentée d'une Personne concernée, relayée et validée par écrit par le Client et en toute hypothèse, (iii) au terme du Contrat (sous réserve des durées complémentaires liées à la preuve ou aux prescriptions), après restitution au Client des Données Personnelles en cause.

Sous les réserves stipulées ci-dessus, en cas (i) de résiliation du Contrat, ou (ii) à tout moment sur demande écrite du Client, Kosmos doit supprimer et obtenir la suppression par son ou ses Sous-traitant(s) ultérieur(s) de toutes copies des Données Personnelles du Client, ou sur demande écrite et précise, de certaines de ces Données.

14. PERIMETRE DE RESPONSABILITE

En tant que Responsable de traitement, il appartient au Client d'assurer l'information des Personnes concernées par ses Traitements (qu'ils soient réalisés directement par ses utilisateurs via la Solution ou qu'ils correspondent aux Services confiées à Kosmos, au sujet (i) des Données Personnelles collectées, (ii) des Traitements mis en œuvre, (iii) des Finalités poursuivies, (iv) des bases légales fondant les Traitements, (v) des éventuels tiers Destinataires des Données Personnelles, ainsi que (vi) de l'ensemble des autres informations dues aux personnes selon les articles 13 ou 14 du RGPD, en ce compris le rappel des droits dont elles disposent sur leurs Données Personnelles et les coordonnées auxquelles les faire valoir. Le Responsable de traitement détermine les modalités de diffusion et l'effectivité de cette information sous sa seule responsabilité. Le cas échéant, il communique les messages d'information à Kosmos aux fins de publication sur l'éventuelle Solution fournie.

En toute hypothèse il appartient au Client, en tant que Responsable de traitement, de veiller à la conformité à la Règlementation des Traitements de Données Personnelles qu'il confie à Kosmos, ainsi plus généralement que des traitements sur son propre système d'information, auprès de ses propres collaborateurs et autres sous-traitants, et de déployer les mesures techniques et organisationnelles appropriées au sein de son organisation. Kosmos dégage toute responsabilité liée à la conformité du Responsable de traitement pour ce qui excède le seul périmètre des Services objets du Contrat.

A cet égard, il appartient au Client en tant que Responsable de traitement de (i) collecter sous sa responsabilité les Données Personnelles dont il s'assure qu'elles sont strictement nécessaires et proportionnées aux Finalités poursuivies, (ii) s'assurer qu'elles ont été collectées conformément à une base légale éprouvée (et le cas échéant, qu'elles ont fait l'objet des consentements nécessaires dont le Client conserve la preuve), (iii) assurer l'information préalable complète due aux Personnes concernées, (iv) documenter l'ensemble des instructions qu'il adresse à Kosmos relatives aux Données Personnelles, (v) veiller pendant toute la durée du Contrat au respect des obligations prévues par la règlementation de la part de Kosmos et (vi) superviser l'exécution des Traitements effectués pour son compte.

Il est rappelé que Kosmos n'est susceptible d'engager sa responsabilité que pour un dommage directement lié à un manquement de Kosmos à ses engagements en tant que Sous-traitant, ou si elle a agi en dehors ou contrairement aux instructions conformes à la Règlementation émanant du Client.

En cas d'amende, de condamnation ou de préjudice subi par Kosmos (i) du fait d'un manquement du Responsable de traitement à ses obligations au regard de la Règlementation, ou (ii) du fait d'une instruction adressée à Kosmos, notamment si l'instruction conduit à une non-conformité des Traitements confiés à Kosmos à la Règlementation, le Responsable de traitement s'engage à indemniser Kosmos de toute amende, condamnation ou préjudice subi.

15. REGISTRES DE TRAITEMENTS ET DESIGNATION DPO

Chaque Partie s'engage à répertorier les Traitements objets des Services au sein d'un registre des traitements. Kosmos indiquera au sein de son registre les Traitements qu'elle effectue au nom et pour le compte du Client conformément aux exigences de l'article 30, 2° Du RGPD. Le Client est responsable de son propre registre des Traitements conformément aux exigences de l'article 30 1° du RGPD.

La désignation des DPO des Parties figure en Sous-annexe 1.

*