

ANNEXE 1 :

ACCORD DE TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

Concernant les traitements de Données Personnelles réalisés dans le cadre de l'exécution de la Convention, le Client est responsable de traitement et le Prestataire est sous-traitant. Les Parties conviennent de définir la notion d'instruction comme étant acquise lorsque le Prestataire agit dans le cadre de l'exécution des présentes. Les termes utilisés dans cette annexe qui sont définis par le RGPD s'entendent comme dans le RGPD.

ARTICLE 1 - OBLIGATIONS DU RESPONSABLE DE TRAITEMENT

Il appartient au Client de s'assurer que les mesures de sécurité et de confidentialité offertes par le Prestataire, sont en adéquation avec le niveau de précaution que le Client doit prendre au regard de son obligation de sécurité des données à caractère personnel dont il est responsable, et que les garanties présentées par le Prestataire à cet effet sont suffisantes. La base légale des traitements de données personnelles liés à l'exécution de la Convention est l'intérêt légitime du Client et relève de sa responsabilité. Les données personnelles traitées dans le cadre de la Convention seront collectées par le Client puis communiquées au Prestataire sur la base des éléments demandés par ce dernier. Le Client garantit avoir informé les personnes concernées par le traitement, et respecter le principe de minimisation des données.

ARTICLE 2 - OBLIGATIONS DU SOUS-TRAITANT

Le Prestataire s'engage à prendre toutes les mesures appropriées au respect par lui-même et par son personnel de ces obligations et notamment à :

- ne pas traiter, consulter les données en dehors du cadre des instructions documentées et des autorisations reçues du Client, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers à l'Union Européenne - à l'exception des pays appartenant au groupe LEYTON - ou à une organisation internationale, à moins que le Prestataire ne soit tenu d'y procéder en vertu d'une disposition impérative résultant du droit communautaire ou du droit de l'Etat membre auquel elle est soumise. Dans ce cas, le Prestataire informe le Client de cette obligation juridique avant le traitement des données, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public;
- veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36 du RGPD.

Le Prestataire s'engage à tenir à jour un registre des activités de traitement effectuées pour le compte du Client.

Si une personne concernée contacte directement le Prestataire afin que d'exercer des droits que le RGPD lui confère, le Prestataire transmettra cette demande au Client dans les meilleurs délais. Le Prestataire s'engage à mettre en œuvre à la demande du Client des moyens et mesures appropriés et raisonnables afin d'aider le Client, à s'acquitter de son obligation de donner suite aux demandes des personnes concernées.¹

ARTICLE 3 – SECURITE

Le Prestataire s'engage, au regard de la nature des données et des risques présentés par le traitement, et compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, portée, contexte et finalités du traitement ainsi que des risques pour les droits et libertés des personnes physiques, à prendre toutes mesures requises pour préserver la sécurité des données des fichiers et notamment empêcher toute déformation, altération, endommagement, destruction de manière fortuite ou illicite, perte, divulgation et/ou tout accès par des tiers non autorisés préalablement. En conséquence, le Prestataire met en œuvre les mesures techniques et organisationnelles appropriées afin de préserver un niveau adapté de sécurité des données et notamment, empêcher qu'elles ne soient déformées, endommagées, et empêcher tout accès qui ne serait pas préalablement autorisé par le Client. Sur simple demande, le Prestataire communiquera sa politique de sécurité au Client.

ARTICLE 4 - VIOLATION DE DONNEES

En cas de violation de données à caractère personnel, le Prestataire s'engage à notifier la violation au Client dans les meilleurs délais après en avoir pris connaissance et au maximum sous 48 heures. Cette notification sera envoyée par courrier électronique et précisera, dans la mesure du possible, la nature et les conséquences de la violation des données ainsi que les mesures déjà prises ou celles qui sont proposées pour y remédier. Le Prestataire s'engage à collaborer avec le Client afin qu'il soit en mesure de répondre à ses obligations en matière de notification à la personne concernée.

ARTICLE 5 - SOUS-TRAITANCE

La liste des sous-traitants ultérieurs, au sens de la réglementation Informatique et libertés est la suivante :

- Toute société appartenant au Groupe LEYTON, dont certaines sont situées dans des pays en dehors de l'Union Européenne.

Le Prestataire peut révoquer, remplacer ou nommer des sous-traitants ultérieurs sous réserve des dispositions suivantes :

¹ DPO : Xavier de Marcillac, dpo@leyton.com

- imposer au sous-traitant ultérieur les mêmes obligations en matière de protection des données que celles fixées dans la présente annexe ;
- informer le Client par courrier électronique à l'avance (sauf hypothèse d'un remplacement d'urgence) de toutes les modifications affectant la liste des sous-traitants ultérieurs. Le Client est tenu d'informer le Prestataire de tout motif valable d'opposition par écrit dans les quinze (15) jours qui suivent la réception du courrier électronique. Si le Client ne manifeste pas son opposition dans les quinze (15) jours qui suivent la réception de la notification, le(s) nouveau(x) sous-traitant(s) ultérieur(s) sera/seront réputé(s) accepté(s) par le Client. En cas d'opposition valable du Client, le Prestataire peut, à son choix, (i) renoncer à l'idée de recourir au sous-traitant ultérieur ou (ii) prendre les mesures correctives sollicitées par le Client, ou (iii) confirmer au Client qu'il recourra au sous-traitant ultérieur malgré l'opposition du Client. Dans cette dernière hypothèse, le Client dispose de la faculté de résilier la Convention pour convenance dans un délai d'un mois à compter de la date de réception de la confirmation du recours au sous-traitant.

Lorsque ses sous-traitants ne remplissent pas leurs obligations en matière de protection des données, le Prestataire demeure pleinement responsable devant le Client de l'exécution par les sous-traitants ultérieurs de leurs obligations.

ARTICLE 6 - TRANSFERT TRANSFRONTALIER DE DONNÉES

En cas de transfert de données à caractère personnel vers un pays tiers, n'appartenant pas à l'Union Européenne et ne faisant pas partie du groupe LEYTON, le Groupe LEYTON devra obtenir l'accord préalable écrit du Client. A l'exception de transferts au sein du Groupe Leyton² ainsi que vers des pays reconnus par la Commission Européenne comme assurant un niveau de protection adéquat, le Prestataire s'engage à ce que le transfert de ces données soit réalisé dans un cadre sécurisé et encadré par des clauses contractuelles ou par des règles d'entreprise contraignantes approuvé conformément à l'article 46 du Règlement Général de Protection des Données.

ARTICLE 7 – AUDIT

Le Prestataire s'engage à collaborer de manière raisonnable et à mettre à disposition du Client toutes les informations nécessaires pour démontrer le respect de leurs obligations contractuelles en matière de traitement de données à caractère personnel et permettre la réalisation d'audit sur la protection des données, par le Client ou par une autorité de contrôle habilitée. Il ne pourra être réalisé plus de 2 jours d'audit par période de 12 mois, tout audit devant être notifié au dpo³ par mail, en respectant un préavis minimum de 30 jours. Le Client se porte fort de la signature d'un engagement de confidentialité par les

² Les transferts au sein du Groupe LEYTON sont encadrés par des BCR, disponibles à l'adresse : https://www.leyton.com/BCR-P_FR

³ DPO : Xavier de Marcillac, dpo@leyton.com

auditeurs, qui ne pourront pas être un concurrent direct du Prestataire ou l'un de ses anciens salariés. L'audit ne devra pas interférer avec la capacité du Prestataire à fournir ses services en conformité avec la Convention. Si les conclusions de certains audits contiennent des recommandations tendant à la modification ou à l'amélioration des procédures et services audités, la mise en œuvre de ces recommandations entre les parties sera discutée de manière contradictoire et fera, le cas échéant, l'objet d'un avenant à la Convention.