Contrat de traitements de données à caractère personnel (DPA)

1. Préambule

Le présent contrat de traitements de Données à caractère personnel (ci-après le **« DPA »**) s'applique à tout contrat conclu entre Klaxoon et le Client (ci-après le **« Contrat »**) dans le cadre de la fourniture des services Klaxoon (ci-après **« les Services »).**

Le présent DPA pour objet de définir les rôles et obligations de Klaxoon et du Client (ci-après les **« Parties »)** au regard du 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 le **« RGPD**), lorsque ces dernières réalisent des traitements de Données à caractère personnel en tant que Responsable de traitement mais également lorsque Klaxoon collecte des Données à caractère personnel pour le compte du Client en tant que Sous-traitant.

2. Définitions

Les termes commençant par une majuscule et non définis au sein de la présente clause ont la même signification que ceux définis dans le Contrat et les termes**, « Responsable de traitement », « Sous-traitant », « Traitement », « Violation de Données à caractère personnel »** ont le même sens que ceux définis dans le RGPD.

« Clause Contractuelle type » désigne la version actuelle et toute version ultérieure des clauses type de la Commission européenne applicable au Sous-traitant en cas de transfert de Données à caractère personnel ;

« Données à caractère personnel » désigne toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement ;

« Lois Applicables » désigne toute loi, règlement, ordonnance en matière de protection de données à caractère personnel et notamment le RGPD ;

« Personnes Concernées » désigne les personnes physiques identifiées et identifiables concernées par les traitements mis en œuvre respectivement par Klaxoon et le Client ;

« Sous-traitant ultérieur » désigne les sociétés tierces engagées par le Sous-traitant pour réaliser les prestations directement liées au traitement de Données à caractère personnel pour lequel Klaxoon agit en qualité de Sous-traitant.

3. Traitement de Données à caractère personnel effectués par Klaxoon en tant que Sous-traitant.

3.1 Obligations générales du Sous-traitant

La présente clause a pour objet de définir les obligations de Klaxoon agissant en qualité de Sous-traitant lorsqu'il traite les Données à caractère personnel du Client agissant lui en qualité de Responsable de traitement en vertu du Contrat, et ce conformément à l'article 28 du RGPD.

Le Sous-traitant s'engage à traiter les Données à caractère personnel du Responsable de traitement selon les instructions documentées de ce dernier et pour les besoins de la fourniture des Services. Le détail des traitements réalisés par le Sous-traitant est décrit à l'Annexes 1 du présent DPA.

Les Parties reconnaissent que les instructions documentées désignent les stipulations du Contrat et du présent DPA. Le Responsable de traitement pourra formuler des instructions supplémentaires pendant la durée du Contrat à condition que lesdites instructions soient requises par les Lois Applicables ou convenues avec le Sous-

traitant. Le Sous-traitant ne sera donc pas tenu de suivre une instruction du qui serait non documentée et/ou non conforme aux Lois Applicables.

Dans le cadre de la réalisation du traitement qu'il réalise pour le compte du Responsable de traitement et conformément à l'Article 28 du RGPD, le Sous-traitant s'engage à :

- assister raisonnablement le Responsable de traitement à satisfaire ses obligations légales au regard du Traitement que ce dernier réalise dans le cadre de l'utilisation des Services;
- informer le Responsable de traitement, dans la mesure où cela est permis par les Lois Applicables, de toute demande et/ou injonction émanant d'une autorité de contrôle concernant les Données à caractère personnel collectées pour les besoins du Contrat. Dans une telle situation, le Sous-traitant s'engage à rediriger la demande de l'autorité de contrôle directement auprès du Responsable de traitement afin de permettre à ce dernier de contester ladite demande dans le respect des Lois Applicables. Dans le cas où le Sous-traitant est tenu de traiter directement la demande de l'autorité de contrôle, ce dernier s'engage à ne communiquer que les Données à caractère personnel strictement nécessaires pour satisfaire à une telle demande ;
- ne pas conserver les Données à caractère personnel du Responsable de traitement pour une durée excédant celle décrite en Annexe 1 du présent DPA ;
- mettre en œuvre toutes les mesures techniques et organisationnelles telles que décrites en Annexe 2 du DPA et requises par l'Article 32 du RGPD afin de (i) garantir la sécurité et l'intégrité des Données à caractère personnel du Responsable de traitement et (ii) prévenir toute Violation de Données à caractère personnel ;
- désigner un délégué à la protection des Données à caractère personnel et communiquer l'identité de ce dernier sur demande du Responsable de traitement ;
- prendre en compte, dès la conception des Services, le principe de *Privacy by design* et *Privacy by default* tel que requis par les Lois Applicables ;
- aider raisonnablement le Responsable de traitement à satisfaire ses obligations légales au regard des droits des Personnes concernées et informer sans délai le Responsable de traitement lorsqu'une Personne concernée exerce une demande directement auprès de Klaxoon ;
- informer le personnel ayant accès aux Données à caractère personnel du Responsable de traitement des obligations décrites dans le présent DPA. Le Sous-traitant s'engage également à former son personnel afin de le sensibiliser aux exigences du RGPD ;
- assister raisonnablement le Responsable de traitement à réaliser une analyse d'impact conformément à l'article 35 du RGPD (si applicable).

3.2 Sous-traitant Ultérieur

Le Responsable de traitement est informé que le Sous-traitant peut sous-traiter une partie des prestations à un Sous-traitant Ultérieur et que le présent DPA constitue une autorisation écrite générale conformément à l'Article 28 du RGPD.

Pendant la durée du Contrat, le Sous-traitant pourra changer de Sous-traitant Ultérieur sous réserve d'en informer le Responsable de traitement au préalable au moyen d'un écrit.

Le Responsable de traitement disposera alors d'un délai de 8 jours à compter de la notification du Sous-traitant pour s'opposer au nouveau Sous-traitant Ultérieur. Le Responsable de traitement aura alors la possibilité de résilier le Contrat. Dans une telle situation, le Client est informé que la résiliation du Contrat ne pourra donner lieu à aucune compensation de quelque nature que ce soit au profit de ce dernier.

A défaut d'objection écrite du Responsable de traitement dans le délai précité, le nouveau Sous-traitant ultérieur sera considéré comme autorisé conformément à l'article 28 du RGPD.

Le Sous-traitant s'assure que chacun de ses Sous-traitants Ultérieurs présentent a minima les mêmes garanties que le Sous-traitant notamment en terme de confidentialité et de sécurité et veille à ce que ces derniers répondent aux exigences du RGPD.

Le Sous-traitant s'engage également à ce que tout Sous-traitant Ultérieur respecte pleinement les obligations décrites dans le présent DPA et engage sa responsabilité pour tout manquement causé par un Sous-traitant Ultérieur dans les conditions de l'Article « Responsabilité » du Contrat.

3.3 Transfert de Données Hors UE

Pour les besoins du Contrat, le Sous-traitant pourra être amené à transférer des Données à caractère personnel du Responsable de traitement. Le Sous-traitant s'engage à ce qu'une telle opération n'impacte pas la sécurité et l'intégrité des données du Responsable de traitement.

En cas de transfert de Données à caractère personnel en dehors de l'Union Européenne ou dans un pays ne bénéficiant pas d'une décision d'adéquation de la Commission européenne (ci-après un **« Pays Tiers »),** le Sous-traitant s'engage à en informer le Responsable de traitement par écrit au préalable et au plus tard dans les trente (30) jours avant le transfert.

Le Responsable de traitement aura la possibilité de s'opposer à ce transfert dans les huit (8) jours à compter de la notification du Sous-traitant et pourra ainsi résilier le Contrat sans que cela ne puisse lui donner droit à compensation. A défaut d'objection écrite du Responsable de traitement dans le délai précité, le transfert sera considéré comme autorisé.

En tout état de cause et avant tout transfert hors Union Européenne ou vers un Pays Tiers, le Sous-traitant s'engage à (i) mettre en œuvre les garanties appropriées telles que requises par l'Article 46 du RGPD ; et (ii) signer les Clauses Contractuelles Types avec tout Sous-traitant Ultérieur concerné par le transfert.

3.4 Sécurité des Données à caractère personnel

Les Données à caractère personnel collectées par le Sous-traitant pour les besoins du Contrat sont hébergées sur des serveurs situés dans l'Union Européenne et reconnu par un certificat validé par un tiers de confiance.

La sécurité des Données du Responsable de traitement est une préoccupation majeure pour le Sous-traitant. A ce titre, le Sous-traitant bénéficie d'une infrastructure technique et d'outils matériels et logiciels de monitoring permettant d'assurer la sécurité et l'intégrité des Données du Client dans des conditions conformes aux règles de l'art.

A ce titre, le Sous-traitant s'engage à implémenter toutes les mesures techniques et organisationnelles requises par les Lois Applicables et telles que décrites à l'Annexe 2 du DPA en vue de prévenir toute Violation de Données à caractère personnel.

Le Responsable de traitement est informé que le Sous-traitant pourra mettre à jour, à sa discrétion ou pour se conformer aux Lois Applicables, les mesures techniques et organisationnelles sous réserve que lesdites mesures présentent un niveau de sécurité a minima aussi élevé que les mesures décrites au présent DPA.

3.5 Violation des Données à caractère personnel

En cas de Violation de Données à caractère personnel avérée et portée à la connaissance du Sous-traitant, ce dernier s'engage à en informer le Responsable de traitement sans délai et au plus tard dans les soixante-douze (72) heures après en avoir eu connaissance.

La notification du Sous-traitant devra indiquer la nature de la violation, ses conséquences probables et les mesures correctives sélectionnées par le Sous-traitant pour résoudre la Violation de Données à caractère

personnel. Le Sous-traitant devra également notifier au Responsable de traitement et dans la mesure du possible, les catégories et le nombre approximatif de Personnes concernées par la violation, les catégories et le nombre approximatif d'enregistrements de Données à caractère personnel concernés.

Dans l'hypothèse où le Sous-traitant ne disposerait pas d'un tel niveau d'information concernant la violation au moment de la notification, ce dernier s'engage à communiquer au Responsable de traitement les informations complémentaires requises dès qu'il en aura eu connaissance. En toute état de cause, le Responsable de traitement sera tenu d'informer l'autorité de contrôle compétente ainsi que toutes les Personnes concernées de l'existence de la violation dès la première notification du Sous-traitant.

Le Sous-traitant mettra en œuvre toutes les mesures correctives nécessaires à la résolution de la Violation de Données à caractère personnel et informera le Responsable de traitement de l'évolution de la situation. Si les mesures correctives implémentées par le Sous-traitant restent ineffectives et que ce dernier ne parvient pas à résoudre la violation, le Client pourra résilier le Contrat pour manquement du Sous-traitant dans les conditions décrites aux articles « Résiliation » et Responsabilité » du Contrat.

3.6 Audit

Le Sous-traitant accorde un droit d'audit au Responsable de traitement dans le seul but de vérifier la conformité du Sous-traitant au présent DPA et aux Lois Applicables. Le Responsable de traitement devra respecter un préavis de quinze (15) jours ouvrables et pourra faire appel à un auditeur externe à condition que ce dernier (i) ne soit pas considéré comme un concurrent direct du Sous-traitant ; ii) soit soumis à minima aux mêmes engagements de confidentialité que le Responsable de traitement.

L'audit sera réalisé à la demande et aux frais du Client et sera limité à un (1) audit par année contractuelle. Le périmètre de cet audit devra être convenu mutuellement entre les Parties préalablement à sa mise en œuvre.

Le droit d'audit accordé au Responsable de traitement au titre de la présente clause se fera par transmission de documents *(le Contrat, le présent DPA, les rapports d'audit et de certification rendus disponibles*) et sera réalisé à distance. Ce n'est que dans le cas où la transmission de documents se révèlerait insuffisante pour démontrer la conformité au DPA et après discussions des Parties, que le Client pourra réaliser l'audit dans les locaux du Sous-traitant à l'exception des zones bénéficiant du statut de Zone à Régime Restrictif en application du Décret n° 2011-1425 du 2 novembre 2011 *relatif à la protection du potentiel scientifique et technique de la Nation*, ce que le Client reconnaît et accepte sans réserve.

Au terme de l'Audit, l'auditeur devra restituer toutes les copies des informations confidentielles mises à sa disposition par le Sous-traitant. Les conclusions de l'audit devront être communiquées au Responsable de traitement qui pourra émettre ses observations et réserves sous trente (30) jours. En l'absence de rapport transmis par le Responsable de traitement, l'Audit sera considéré conforme en tout point.

Dans l'hypothèse où l'audit révèle un manquement du Sous-traitant à ses obligations légales et/ou contractuelles, le Sous-traitant mettra alors en œuvre, à ses frais, les mesures correctives nécessaires à la résolution de ce manquement. Si le Sous-traitant ne parvient pas à résoudre le manquement révélé par l'audit, le Client sera en mesure de résilier le Contrat conformément aux dispositions des articles « Résiliation » du Contrat.

3.7 Les obligations du Responsable de traitement

Le Client est responsable de toutes les Données à caractère personnel qu'il collecte dans le cadre de l'utilisation des Services (contenu utilisateur). A ce titre, le Client s'engage à respecter les Lois Applicables et les obligations de conformité imposées par le RGPD.

Le Client est informé qu'il est et demeure responsable de toute données qu'il crée, modifie, supprime (de façon accidentelle ou non) dans le cadre de l'utilisation des Services.

Dans le cadre des opérations de traitement réalisées par le Client, ce dernier est désigné comme point de contact auprès des Personnes concernées pour l'exercice de leurs droits et sera gestionnaire des demandes reçues par ces dernières.

4 Obligations de Klaxoon en tant que Responsable de traitement

Dans le cadre du Contrat, Klaxoon est également amenée à traiter des Données à caractère personnel du Client en tant que Responsable de traitement pour les finalités décrites à l'Annexe 1 du DPA. Dans le cadre de ces traitements, Klaxoon s'engage à respecter les stipulations du Contrat, du présent DPA ainsi que la Politique de Confidentialité accessible sur le lien suivant : https://static.klaxoon.com/website/pdf/politique-de-confidentialite.pdf

Par souci de clarté, lorsque les Parties agissent toutes deux en tant que Responsable de traitement, chacune d'entre elles détermine individuellement et indépendamment, les moyens de la collecte de Données Personnelles et les finalités des opérations de traitement qu'elle met en œuvre dans le cadre de l'exécution Contrat. Ainsi, le Contrat et le présent DPA n'établissent aucune solidarité entre les Parties.

En sa qualité de Responsable de traitement, Klaxoon s'engage à :

- informer toute autorité de contrôle compétente des traitements de Données à caractère personnel réalisés par Klaxoon pour les besoins du Contrat ;
- obtenir le consentement de toutes les Personnes concernées et informer ces dernières des droits dont elles disposent au regard de les Lois Applicables ;
- maintenir un registre à jour de tous les traitements réalisés par Klaxoon sous sa responsabilité ;
- mettre en œuvre les mesures techniques et organisationnelles pour préserver la confidentialité et l'intégrité des Données à caractère personnel et de prévenir toute violation de ces données ;
- informer le Client sans délai et au plus tard dans les soixante-douze (72) heures en cas de Violation de Données à caractère personnel et mettre en œuvre toutes les mesures correctives nécessaires pour résoudre ladite violation ;
- vérifier que tous ses Sous-traitants agissant pour son compte et pour les besoins du Contrat présentent les garanties appropriées et respectent les exigences des Lois Applicables ;
- donner suite aux demandes des Personnes concernées et en particulier de toute demande d'accès, de rectification, d'effacement, restitution ou d'objection des Données à caractère personnel. A ce titre, les Personnes concernées pourront modifier, supprimer, récupérer leurs Données à caractère personnel directement via les Services ou à défaut s'adresser par courrier électronique à KLAXOON legal@klaxoon.com.

KLAXOON Représentée par Hervé SIMONIN Position : CEO Le…… Signature :	…… Représentée par : Position : Le…….. Signature :

Annexe 1 - Détails des Traitements

Dans le cadre du Contrat et de la réalisation de ses prestations, Klaxoon réalise les traitements listés dans la présente Annexe.

I). Traitements réalisés par Klaxoon en tant que Sous-traitant

- Objet du traitement : Hébergement des données collectées par les utilisateurs dans le cadre de l'utilisation des Services ;
- Nature du traitement : collecte, stockage, suppression, archivage ;
- Finalité du traitement : stockage sécurisé des données des utilisateurs ;
- Catégorie de Données à caractère personnel collectées : Toute Donnée à caractère personnel collectée par les utilisateurs dans le cadre de l'utilisation des Services ;
- Personnes concernées par le traitement : les utilisateurs de la solution Klaxoon;
  Durée du traitement : les données sont conservées jusqu'à ce que l'utilisateur supprime lui-même ses données ou jusqu'à la suppression du compte utilisateur.

II). Traitements réalisés par Klaxoon en tant que Responsable de traitement

A) Traitement n°1

- Objet du traitement : création et administration des comptes utilisateurs ;
- Nature du traitement : Collecte, utilisation, stockage, suppression ;
- Finalité du traitement : créer et administrer les comptes utilisateurs ;
- Catégorie de données collectées : noms, prénoms, adresses email, photo (facultatif, au choix de l'utilisateur) ;
- Personnes concernées par le traitement : les utilisateurs de la solution Klaxoon ;
- Durée du traitement : les données personnelles sont conservées jusqu'à la suppression du compte utilisateur.

B) Traitement n°2

- Objet du traitement : gestion de la relation contractuelle ;
- Nature du traitement : utilisation, collecte, stockage, suppression ;
- Finalité du traitement : Gérer la relation contractuelle entre Klaxoon et le Client (*ex : envoi de devis, factures, renouvellement contrats, gestion des paiements*) ;
- Catégorie de données collectées : noms, prénoms, adresses email, numéros de téléphone ;
- Personnes concernées par le traitement : les personnes en charge de la relation contractuelle et commerciale chez le Client ;
- Durée du traitement : les données sont conservées pour la durée du Contrat et pour satisfaire toute obligation légale, comptable et fiscale (notamment à des fins probatoires ou de communication à des autorités compétentes).

C) Traitement n°3

- Objet du traitement : gestion de la relation client ;
- Nature du traitement : Collecte, utilisation, stockage, suppression ;
- Finalité du traitement : Répondre aux demandes des utilisateurs ; informer les utilisateurs sur l'usage du Service, recevoir et traiter les demandes d'assistance technique des utilisateurs ; Gérer les demandes de droit d'accès aux données personnelles, de rectification et d'opposition ;
- Catégorie de données collectées : Noms, prénoms, adresses email, numéros de téléphone, données d'utilisations des services

- Personnes concernées par le traitement : les utilisateurs de la solution Klaxoon ;
- Durée du traitement : les données personnelles sont conservées jusqu'à la suppression du compte utilisateur.

D) Traitement n°4

- Objet du traitement : Prospection commerciale et marketing ; (*envoi de Newsletters, appels téléphoniques*);
- Nature du traitement : Collecte, utilisation, stockage, suppression ;
- Finalité du traitement : informer les utilisateurs de l'évolution des Services et notamment de toute nouvelle version des Services, nouvelle fonctionnalité, nouvelle mise à jour disponible, lancement d'un nouveau produit et/ou organisation d'évènement en lien avec le lancement d'un nouveau produit.
- Catégorie de données collectées : Noms, prénoms, adresses email, numéro de téléphone ;
- Personnes concernées par le traitement : les utilisateurs de la solution Klaxoon ;
- Durée du traitement : les données personnelles sont conservées jusqu'à la suppression du compte utilisateur. Les Informations Personnelles utilisées dans le cadre de ce traitement sont conservées conformément aux préconisations de la CNIL dans la délibération n°2016-264 du 21 juillet 2016, à savoir trois (3) ans à compter de leur collecte ou du dernier contact émanant de l'utilisateur. L'utilisateur conserve la possibilité de s'opposer à tout moment à ce traitement en le notifiant à Klaxoon ou, concernant les newsletters, en se désinscrivant des listes d'envoi directement via le mail reçu.

Annexe 2 – Standards techniques et de sécurité du Service

Exigences techniques pour l'utilisation des Services.

Klaxoon Cloud est une application collaborative SaaS disponible avec une connexion Internet, sur tous types de périphériques. Rien à télécharger ni à installer.

Avec le navigateur de votre choix : Google Chrome ; Mozilla Firefox ; Windows Edge ; Safari.

Totalement fonctionnel avec les 3 dernières versions de ces navigateurs (mode mobile et Desktop).

Configuration obligatoire du navigateur : Activation Javascript, les cookies fonctionnels requis par l'application doivent être activés.

Avec l'appareil de votre choix : Tablette ; Smartphone ; Desktop

Certaines activités synchrones utilisent des requêtes web-sockets côté client, pour cela vous l'URL suivante doit être autorisée : wss://*.klaxoon.com/*.

Équipement : Pour utiliser l'Equipement en mode wifi, il est nécessaire de permettre la connexion à un point d'accès wifi privé depuis les terminaux (PC, smartphones, tablettes).

Les mesures techniques et organisationnelles mises en œuvre par Klaxoon dans le but de garantir la confidentialité et l'intégrité des Données :

Les mesures techniques :

- *Privacy by Default* : Mise en œuvre des meilleures pratiques actuelles (top 10 OWASP, CWE, NIST) dans les développements logiciels contribuant à l'approche *Security by Design* et au principe de Défense en Profondeur
- Protection de l'accès physique aux locaux Klaxoon et aux datacenters
- Authentification de l'utilisateur avec hachage du mot de passe. L'authentification de l'utilisateur peut également être délégué au Client (sur devis).
- Gestion des accès à la plateforme et au SI interne (différents rôles implémentés avec différents accès)
- Séparation des réseaux interne, R&D, Production
- Traçabilité de toutes les connexions
- Chiffrement des données client en transit et au repos
- Possibilité d'anonymiser l'accès à KLAXOON : l'utilisateur peut choisir le mode 'pseudonyme' en invitant des participants.

Les mesures organisationnelles :

- Tous les salariés KLAXOON et les sous-traitants sont soumis à l'obligation de confidentialité contractuelle à l'égard de toutes les informations auxquelles ils ont accès dans l'exercice de leur mission
- Une charte informatique est signée par tous les employés KLAXOON
- KLAXOON applique une politique globale de sécurité des systèmes d'information
- Notre DPO maintient un registre des activités de gestion des Données à caractère personnel et s'assure de l'application des mesures techniques et organisationnelles.

Des informations complémentaires en matière de sécurité sont disponibles sur le Site à l'adresse suivante : https://klaxoon.com/solutions-trust-center