ADDENDA SUR LE TRAITEMENT DES DONNEES DE COMMAND ALKON INCORPORATED

Mise à jour : 12/06/2022

Le présent Addenda relatif au traitement des données (« **ATD** ») fait partie du *Contrat-cadre de licence et de services* (« **Contrat** ») passé entre : (i) le Client (identifié dans la ligne de signature ci-dessous) et ses sociétés affiliées dans l'EEE (« **Client** ») ; et (ii) Command Alkon Incorporated et ses sociétés affiliées (« **Société** ») uniquement lorsque requis par le Règlement général sur la protection des données (« RGPD ») ou toute autre législation applicable en matière de confidentialité.

Cet addendum remplace tout accord antérieur entre les parties concernant l'objet des présentes, c'est-à-dire la confidentialité et la sécurité des données applicables au RGPD.

Compte tenu des obligations mutuelles énoncées dans les présentes, les parties conviennent par la présente que les conditions générales énoncées ci-dessous seront ajoutées sous forme d'Addenda au Contrat.

1. Définitions

Le terme « **Données à caractère personnel du client** » désigne les données à caractère personnel ayant fait l'objet de Traitement par la Société pour le compte du Client dans le cadre de la fourniture des produits et/ou services.

« **Personne concernée** » désigne la personne à laquelle les Données à caractère personnel du Client se rapportent.

Le terme « **Lois sur la protection des données** » désigne le règlement général sur la protection des données (UE) 2016/679 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, et abrogeant la directive 95/46/CE (et tout amendement ou remplacement de celui-ci), la loi fédérale suisse sur la protection des données du 19 juin 1992 (et tout amendement ou remplacement de celle-ci), ou le RGPD de l'UE tel que modifié et incorporé dans la législation britannique en vertu de la loi britannique de 2018 sur (le retrait de) l'Union européenne et la législation secondaire applicable faite en vertu de cette loi (et toute modification ou remplacement de celle-ci), selon celle qui est applicable

Le terme « **Données à caractère personnel** » désigne toute information relative à une Personne concernée, y compris, mais sans s'y limiter, un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou un ou plusieurs facteurs spécifiques à l'état physique, physiologique, génétique, mental, l'identité économique, culturelle ou sociale de la Personne concernée.

« **Bouclier de protection** » désigne le cadre juridique du bouclier de protection des données personnelles convenu entre l'UE et les États-Unis et le cadre juridique du bouclier de protection des données personnelles convenu entre la Suisse et les États-Unis. Bien que les deux cadres soient actuellement inopérants, la Société continue de respecter leurs exigences,

et ce terme s'appliquera à toute version renouvelée et approuvée de l'accord de Bouclier de protection entre les États-Unis et l'Espace économique européen (« EEE »).

« **Traitement**» désigne tout opération ou ensemble d'opérations effectuées sur les Données à caractère personnel du Client, par des moyens automatisés ou non, telles que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, la modification, la récupération, la consultation, l'utilisation, la divulgation, l'élimination, la restriction, l'accès, la diffusion, la combinaison, l'adaptation, la copie, le transfert, l'effacement et/ou la destruction des Données à caractère personnel du Client.

« **Violation de sécurité** » désigne une violation confirmée de la sécurité entraînant une destruction, une perte, une altération accidentelles ou illégales, une divulgation ou un accès non autorisés aux Données à caractère personnel du Client transmises, stockées ou autrement traitées.

Le terme « **Tiers** » désigne une partie autre que le Client ou la Société.

Les termes « **Responsable du traitement** », « **Sous-traitant** » et « **Autorité de contrôle** » tels qu'utilisés dans le présent ATD auront la signification qui leur est attribuée dans le RGPD.

Tous les autres termes non définis, mais en majuscules, auront la signification indiquée dans le Contrat.

2. Traitement des Données à caractère personnel du Client

2.1 Objectif du Traitement. L'objectif du Traitement des données dans le cadre du présent ATD est la fourniture des produits et/ou services conformément au Contrat. L'annexe 1 décrit l'objet et les détails du Traitement des Données à caractère personnel du Client.

2.2 Responsabilités du Sous-traitant et du Responsable du traitement. Les parties reconnaissent et conviennent ce qui suit : (a) la Société est un Sous-traitant des Données à caractère personnel du Client en vertu des Lois sur la protection des données ; (b) le Client est un Responsable du traitement des Données à caractère personnel du Client en vertu des Lois sur la protection des données ; et (c) chaque partie se conformera aux obligations qui lui sont applicables en vertu des Lois sur la protection des données en ce qui concerne le Traitement des Données à caractère personnel du Client.

2.3 Instructions du Client. Le Client demande à la Société de procéder au Traitement des Données à caractère personnel du Client : (a) conformément au Contrat et à tout Supplément applicable ; (b) autrement nécessaire pour fournir les produits et/ou services au Client ; (c) si nécessaire pour se conformer à la loi ou à la réglementation applicable ; et (d) pour se conformer à d'autres instructions écrites raisonnables fournies par le Client lorsque ces instructions sont conformes aux termes du Contrat. Le Client s'assurera que ses instructions pour le Traitement des Données à caractère personnel du Client sont conformes aux Lois sur la protection des données. Entre les parties, le Client est seul responsable de l'exactitude, de la qualité et de la légalité des

Données à caractère personnel du Client et des moyens par lesquels le Client a obtenu les Données à caractère personnel du Client.

2.4 Conformité de la Société aux instructions du Client. La Société ne traitera les Données à caractère personnel du Client que conformément aux instructions du Client et traitera les Données à caractère personnel du Client comme des informations confidentielles. Si la Société estime ou prend conscience que l'une des instructions du Client est en conflit avec les Lois sur la protection des données, la Société en informera le Client dans un délai raisonnable. La Société peut procéder au Traitement des Données à caractère personnel du Client autrement que selon les instructions écrites du Client si cela est requis en vertu de la loi applicable à laquelle la Société est soumise. Dans cette situation, la Société informera le Client de cette exigence avant que la Société ne procède au Traitement des Données à caractère personnel du Client, sauf si la loi applicable l'interdit.

3. Sous-traitants ultérieurs

3.1 Nomination de Sous-traitants ultérieurs. Le Client fournit par la présente une autorisation écrite générale permettant à la Société d'engager des Sous-traitants ultérieurs tiers pour fournir des services limités ou auxiliaires en rapport avec la fourniture de produits et/ou de services. Le site Web de la Société répertorie les Sous-traitants ultérieurs actuellement engagés par la Société pour effectuer des activités de Traitement spécifiques liées aux Données à caractère personnel du Client et la Société mettra à jour la liste des Sous-traitants ultérieurs avant d'engager un nouveau Sous-traitant ultérieur pour effectuer un Traitement spécifique. Le Client peut s'inscrire aux mises à jour électroniques chaque fois que la liste des sous-traitants ultérieurs de la Société est modifiée en envoyant une telle demande à privacy@commandalkon.com. Le Client peut s'opposer à tout Sous-traitant ultérieur en communiquant cette objection à la Société dans les trente (30) jours suivant une mise à jour, et les parties travailleront de bonne foi pour résoudre l'objection. Le Client accepte par la présente les activités de sous-traitement par les Sous-traitants ultérieurs actuels répertoriés sur le site Web de la Société.

3.2 Sécurité du Sous-traitant ultérieur. Lorsque la Société sous-traite ses obligations, elle ne le fera que par le biais d'un accord écrit avec le Sous-traitant ultérieur qui impose des obligations contractuelles au moins équivalentes aux obligations imposées à la Société en vertu du présent Addenda.

3.3 Responsabilité. Si le Sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données en vertu d'un tel accord écrit, la Société restera entièrement responsable envers le Client de l'exécution des obligations du Sous-traitant ultérieur en vertu dudit accord.

4. Évaluations des impacts sur la sécurité et la vie privée

4.1 Sécurité de la Société. La Société mettra en œuvre les mesures techniques et organisationnelles appropriées pour protéger les Données à caractère personnel du Client (« Programme de sécurité de l'information ») en tenant compte de l'état de l'art, des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du Traitement, ainsi que du risque de probabilité et de gravité variable pour

les droits et libertés des personnes physiques. Les mesures techniques et organisationnelles actuelles de la Société sont énumérées à l'Annexe II des Clauses contractuelles types (ci-jointes) et la Société se régit selon les normes de sécurité suivantes : NIST 800-171; AWS CIS.

4.2 Sécurité du Client. Le Client reconnaît que les produits et/ou services incluent certaines caractéristiques et fonctionnalités que le Client peut choisir d'utiliser et qui ont un impact sur la sécurité des Données à caractère personnel du Client traitées par l'utilisation des produits et/ou services par le Client. Le Client est responsable de l'examen des informations que la Société met à disposition concernant la sécurité de ses données et de déterminer de manière indépendante si les produits et/ou services répondent aux exigences et aux obligations légales du Client, y compris ses obligations en vertu des Lois sur la protection des données applicables. Le Client est en outre responsable de la configuration correcte des produits et/ou services et de l'utilisation des caractéristiques et fonctionnalités mises à disposition par la Société pour maintenir une sécurité appropriée à la lumière de la nature des Données à caractère personnel du Client traitées à la suite de l'utilisation par le Client des produits et/ou services. Le Client est responsable de son utilisation des produits et/ou services et de son stockage de toute copie des Données à caractère personnel du Client en dehors des systèmes de la Société ou des Sous-traitants ultérieurs de la Société, y compris, mais sans s'y limiter, la sécurisation des informations d'identification, des systèmes et des appareils d'authentification du compte, et la conservation des copies de ses Données à caractère personnel Client, le cas échéant.

4.3 Personnel de la Société. La Société s'assurera que chaque membre de son personnel engagé dans le Traitement des Données à caractère personnel du Client est informé de la nature confidentielle des Données à caractère personnel du Client et est soumis à des obligations de confidentialité, ces obligations restant en vigueur après la résiliation de l'engagement dudit membre du personnel avec la Société.

4.4 Test de sécurité. La Société testera et évaluera l'efficacité du Programme de sécurité de l'information pour assurer le Traitement sécurisé des Données à caractère personnel du Client. La Société se conformera à son Programme de sécurité de l'information et déclare et garantit que son Programme de sécurité de l'information est et sera conforme à la loi applicable.

4.5 Évaluations d'impact. La Société prendra des mesures raisonnables pour coopérer et aider le Client à mener des évaluations d'impact et des consultations connexes avec toute Autorité de contrôle, si le Client est tenu de procéder à de telles évaluations d'impact en vertu des Lois sur la protection des données.

5. Droits des personnes concernées

5.1 Assistance aux obligations du Client. Dans la mesure où le Client, lors de son utilisation ou de la réception des produits et/ou services, n'a pas la capacité de corriger, modifier, restreindre, bloquer ou supprimer les Données à caractère personnel du Client comme l'exigent les Lois sur la protection des données, la Société doit se conformer rapidement aux demandes raisonnables par le Client pour faciliter de telles actions dans la mesure où la Société est légalement autorisée et en mesure de

le faire. Si la loi l'autorise, le Client sera responsable de tout coût découlant de la fourniture d'une telle assistance par la Société.

5.2 Obligation de notification. La Société doit, dans la mesure autorisée par la loi, informer rapidement le Client si elle reçoit une demande d'une Personne concernée pour l'accès, la correction, la modification, la suppression ou l'objection au Traitement des Données à caractère personnel du Client relatives à cette personne. La Société ne répondra à aucune demande de la Personne concernée relative aux Données à caractère personnel du Client sans le consentement écrit préalable du Client, sauf pour confirmer que la demande concerne le Client. En outre, la Société doit, dans la mesure autorisée par la loi, informer rapidement le Client si elle reçoit une demande de divulgation ou une correspondance, un avis ou toute autre communication relative aux Données à caractère personnel du Client de la part des forces de l'ordre, d'une autorité compétente ou d'une autorité de protection des données pertinente. La Société fournira au Client une coopération et une assistance raisonnables appropriées pour traiter une telle demande, dans la mesure autorisée par la loi et dans la mesure où le Client n'a pas accès à ces Données à caractère personnel du Client par le biais de son utilisation ou de la réception des Produits et/ou Services. Si la loi l'autorise, le Client sera responsable de tout coût découlant de la fourniture d'une telle assistance par la Société.

6. Violation des Données à caractère personnel

6.1 Obligation de notification. Dans le cas où la Société prendrait connaissance d'une Violation de sécurité vérifiée, la Société informera le Client de la Violation de sécurité sans retard injustifié et dans tous les cas au plus tard soixante-douze (72) heures après sa découverte. Les obligations découlant de la présente section 6 ne s'appliquent pas aux incidents causés par le Client ou le personnel du Client ou les utilisateurs finaux ni aux tentatives ou activités infructueuses qui ne compromettent pas la sécurité des Données à caractère personnel du Client, y compris les tentatives de connexion infructueuses, les pings, les analyses de port, les attaques par déni de service et autres attaques réseau contre les pare-feu ou les systèmes en réseau.

6.2 Mode de notification. La notification de toute Violation de sécurité, le cas échéant, sera envoyée au point de contact RGPD du Client par e-mail ou par téléphone. Il est de la seule responsabilité du Client de s'assurer qu'il conserve à tout moment des informations de contact exactes sur les systèmes d'assistance de la Société. Le Client est seul responsable du respect des exigences de notification de violation applicables au Client et de l'exécution de toute obligation de notification de tiers liée à toute Violation de la sécurité des données personnelles.

6.3 Contenu de la notification. Lorsqu'une notification est requise, celle-ci doit au minimum :

6.3.1 décrire la nature de la Violation de sécurité, les catégories et nombres de Personnes concernées affectées, ainsi que les catégories et nombres d'enregistrements de Données à caractère personnel concernés ;

6.3.2 communiquer le nom et les coordonnées du contact pertinent de la Société auprès duquel de plus amples informations peuvent être obtenues ;

6.3.3 décrire les conséquences probables de la Violation de sécurité ; et

6.3.4 décrire les mesures prises ou proposées pour remédier à la Violation de sécurité.

7. Suppression ou retour des Données à caractère personnel du Client

7.1 Suppression ou retour. Sous réserve de la section 7.3, la Société s'engage à, rapidement et en tout état de cause dans les trente (30) jours suivant la date de cessation de tout service impliquant le Traitement des Données à caractère personnel du Client (« **Date de cessation** »), supprimer en toute sécurité les Données à caractère personnel du Client ou, à la demande écrite en temps opportun du Client, renvoyer une copie complète de toutes les Données à caractère personnel du Client au Client par transfert de fichier sécurisé dans le format raisonnablement demandé par le Client.

7.2 Définition du terme « supprimer »/ « suppression ». Pour plus de clarté, le terme « **Supprimer** » ou « **Suppression** » signifie éliminer ou effacer des Données à caractère personnel de sorte qu'elles ne puissent pas être récupérées ou reconstruites.

7.3 Enregistrements. La Société peut conserver les Données à caractère personnel du Client dans la mesure requise par les Lois applicables ou conformément au calendrier de conservation des documents de la Société, à condition que la Société garantisse la confidentialité de toutes ces Données à caractère personnel du Client.

8. Droits d'audit

8.1 Droits d'audit. Pas plus d'une fois par an, le Client peut engager un tiers convenu d'un commun accord pour auditer la Société uniquement dans le but de répondre à ses exigences d'audit conformément à l'article 28, section 3 (h) du RGPD. Pour demander un audit, le Client doit soumettre un plan d'audit détaillé au moins quatre (4) semaines avant la date d'audit proposée décrivant la portée, la durée et la date de début proposées de l'audit. Les demandes d'audit doivent être envoyées à privacy@commandalkon.com. L'auditeur doit signer un accord de confidentialité écrit acceptable pour la Société avant de procéder à l'audit. L'audit doit être effectué pendant les heures normales de bureau, sous réserve des politiques de la Société, et ne doit pas interférer de manière déraisonnable avec les activités commerciales de la Société. Tous les audits sont à la charge exclusive du Client. La Société coopérera avec tout Client ou toute demande d'audit de l'autorité de réglementation ou de l'Autorité de contrôle compétente pour vérifier le respect par la Société de ses obligations en vertu du présent ATD en mettant à disposition, sous réserve des obligations de non-divulgation, des rapports d'audit de tiers, le cas échéant, des descriptions des contrôles de sécurité et d'autres les informations raisonnablement demandées par le Client concernant les pratiques et politiques de sécurité de la Société.

8.2 Assistance à la conformité. Compte tenu de la nature du Traitement et des informations dont dispose la Société, la Société fournira une coopération et une assistance raisonnables et adéquates au Client concernant les obligations de conformité du Client décrites aux articles 32 à 36 du RGPD.

9. Transferts de données

9.1 Autorisation générale. Le Client accepte que la Société puisse, sous réserve de la section 9.2, stocker et procède au Traitement des Données à caractère personnel du Client aux États-Unis d'Amérique et dans tout autre pays dans lequel la Société ou l'un de ses Sous-traitants ultérieurs dispose d'installations ou procède autrement au Traitement des Données à caractère personnel. De tels transferts seront régis par les clauses contractuelles types inter-affiliées de la Société ou par la certification du Bouclier de protection de la Société (si celui-ci est rétabli). La Société ne transférera pas, ou ne fera pas transférer, les Données à caractère personnel du Client d'une juridiction à une autre, sauf en conformité avec la loi applicable et n'entraînera pas le Client à enfreindre une Loi sur la protection des données.

9.2 Clauses contractuelles types. Dans la mesure, et uniquement dans la mesure où, la Société procède au Traitement des Données à caractère personnel du Client de l'Espace économique européen, de la Suisse ou du Royaume-Uni et que des clauses contractuelles types sont requises, les Clauses contractuelles types applicables (EEE ou Royaume-Uni) s'appliquent et sont incorporées aux présentes. Aux fins des Clauses contractuelles types, le Client est « Exportateur de données » et la Société est « Importateur de données ». La Société a mis en place les Clauses contractuelles types de 2021 entre les filiales de la Société et a maintenu l'auto-certification du Bouclier de protection (au cas où il serait rétabli) aux fins des transferts de données vers les États-Unis d'Amérique.

9.3 Clauses contractuelles types du Royaume-Uni. Les parties conviennent que les Clauses contractuelles types du Royaume-Uni s'appliqueront aux Données à caractère personnel qui sont transférées via les produits et/ou services depuis le Royaume-Uni, soit directement, soit par transfert ultérieur, vers tout pays ou destinataire en dehors du Royaume-Uni qui n'est pas reconnu par l'autorité de régulation compétente du Royaume-Uni ou l'organisme gouvernemental du Royaume-Uni comme assurant un niveau adéquat de protection des Données à caractère personnel. Pour les transferts de données depuis le Royaume-Uni qui sont soumis aux Clauses contractuelles types du Royaume-Uni, les Clauses contractuelles types du Royaume-Uni seront réputées avoir été conclues (et incorporées au présent Addenda par cette référence).

9.4 Mesures supplémentaires. En complément des Clauses contractuelles types, si la Société apprend qu'une autorité gouvernementale (y compris les forces de l'ordre) souhaite obtenir l'accès ou une copie de tout ou partie des Données à caractère personnel du Client traitées par la Société, que ce soit sur une base volontaire ou obligatoire, à des fins liées au renseignement entourant la sécurité nationale, alors, à moins que la loi ne l'interdise ou en vertu d'une contrainte légale obligatoire qui en dispose autrement, la Société : 1) notifiera immédiatement le Client auquel les Données à caractère personnel s'appliquent ; 2) informera l'autorité gouvernementale compétente qu'elle n'a pas été autorisée à divulguer les Données à caractère personnel du Client et, sauf interdiction légale, devra en notifier immédiatement le Client auquel les Données à caractère personnel du Client s'appliquent ; 3) informera l'autorité gouvernementale qu'elle doit adresser toutes les demandes ou requêtes directement au Client auquel les Données à caractère personnel du Client s'appliquent ; et 4) ne donnera pas accès aux Données à caractère personnel du Client tant que le Client auquel les Données à caractère personnel du Client s'appliquent n'aura pas donné son

autorisation par écrit ou tant qu'elle n'aura pas l'obligation légale de le faire. En cas d'obligation légale, la Société déploiera des efforts raisonnables et légaux pour contester cette interdiction ou obligation. Si la Société est obligée de produire les Données à caractère personnel du Client, la Société ne divulguera les Données à caractère personnel du Client que dans la mesure où la loi l'exige, conformément à la procédure légale applicable.

9.5 Priorité de transfert. Dans le cas où les services sont couverts par plus d'un mécanisme de transfert, le transfert des Données à caractère personnel du Client sera soumis à un mécanisme de transfert unique conformément à l'ordre de priorité suivant : (i) Clauses contractuelles types de l'UE (lorsque cela est requis par la Loi sur la protection des données applicable) ; (ii) Auto-certification du Bouclier de protection (si celui-ci est rétabli).

10. Durée et résiliation

Durée de l'ATD. Le présent ATD entrera en vigueur à la date à laquelle il est dûment signé et, nonobstant l'expiration de la durée de tout abonnement acheté, restera en vigueur jusqu'à la suppression de toutes les Données à caractère personnel du Client, comme décrit dans le présent ATD, et expirera automatiquement.

11. Non-conformité ; Règlement des litiges ; Parties

11.1 Limitation de responsabilité. La responsabilité de la Société en cas de manquement à ses obligations découlant du présent ATD est soumise à la clause de limitation de responsabilité du Contrat.

11.2 Parties du présent ATD. Rien dans le présent ATD ne confère d'avantages ou de droits à toute personne ou entité autre que les parties au présent ATD.

12. Conditions générales

Droit applicable et juridiction compétente

12.1 Le présent ATD sera révisé un an après sa date d'émission, puis trois ans après, ou plus tôt si nécessaire.

12.2 Sauf si les Clauses contractuelles types l'exigent :

12.2.1 les parties au présent Addenda se soumettent par la présente au choix de la juridiction stipulée dans le Contrat en ce qui concerne tout litige ou réclamation découlant de quelque manière que ce soit en vertu du présent Addenda, y compris les litiges concernant son existence, sa validité ou sa résiliation ; et

12.2.2 le présent Addenda et toutes les obligations non contractuelles ou autres découlant de celui-ci ou en relation avec celui-ci sont régis par les lois du pays ou du territoire stipulé à cet effet dans le Contrat.

Ordre de préséance

12.3 En cas de conflit ou d'incohérence entre le présent Addenda et les Clauses contractuelles types lorsque les Clauses contractuelles types sont requises, celles-ci prévaudront.

12.4 Sous réserve de la section 12.2, en ce qui concerne l'objet du présent Addenda, en cas d'incohérences entre les dispositions du présent Addenda et tout autre accord entre les parties, y compris le Contrat et y compris (sauf convention contraire explicite par écrit, signée au nom des parties) les accords conclus ou censés être conclus après la date du présent Addenda, les dispositions du présent Addenda prévaudront.

Modifications des Lois sur la protection des données

12.5 Le Client peut :

12.5.1 moyennant un avis écrit d'au moins trente (30) jours calendaires à la Société, proposer de temps à autre des modifications aux Clauses contractuelles types qui sont nécessaires à la suite de toute modification ou décision d'une autorité compétente en vertu de cette Loi sur la protection des données ; et

12.5.2 proposer toute autre modification du présent Addenda que le Client considère raisonnablement nécessaire pour répondre aux exigences de toute Loi sur la protection des données.

12.6 Si le Client donne l'avis en vertu de la section 12.5, les parties doivent discuter rapidement des modifications proposées et négocier de bonne foi en vue de convenir et de mettre en œuvre ces modifications ou d'autres variantes conçues pour répondre aux exigences identifiées dans l'avis du Client dès que cela est raisonnablement possible.

Divisibilité

12.7 Si une disposition du présent Addenda devient non valide ou inapplicable, le reste dudit Addenda restera valide et en vigueur. La disposition non valide ou inapplicable sera soit : (i) modifiée si nécessaire pour assurer sa validité et son caractère exécutoire, tout en préservant le plus fidèlement possible les intentions des parties ou, si cela n'est pas possible ; (ii) interprétée comme si la partie non valide ou inapplicable n'a avait jamais été contenue dans les présentes.

ANNEXE I AUX CLAUSES CONTRACTUELLES TYPES

A. LISTE DES PARTIES

Exportateur(s) de données[1] **:** *[Identité et coordonnées du ou des exportateurs de données et, le cas échéant, de son/leur délégué à la protection des données et/ou représentant dans l'Union européenne]*

Nom :

Adresse :

Nom, fonction et coordonnées de la personne à contacter :

Activités pertinentes pour les données transférées en vertu de ces Clauses :

Signature et date :

Rôle : Responsable du traitement

Importateur(s) de données : *[Identité et coordonnées du ou des importateurs de données, y compris toute personne de contact responsable de la protection des données]*

Nom : Command Alkon Incorporated

Adresse : 1800 Industrial Park Drive, Suite 400, Birmingham, Alabama 35243 États-Unis

Nom, fonction et coordonnées de la personne à contacter : David R. Burkholder, Directeur juridique associé et responsable de la protection de la vie privée, dburkholder@commandalkon.com, 1-205-263-5524 poste 2837

Activités pertinentes pour les données transférées en vertu de ces Clauses :

Responsable de la protection de la vie privée à des fins de conformité

Signature et date :

Rôle : Sous-traitant

B. DESCRIPTION DU TRANSFERT

[1] Si cette section n'est pas remplie, l'Exportateur de données sera l'entité identifiée dans le Contrat-cadre de licence et de services associé et les documents associés.

Catégories de Personnes concernées dont les Données à caractère personnel sont transférées

Employés du Client ; clients du Client ; employés des sociétés affiliées du Client.

Catégories de Données à caractère personnel transférées

Coordonnées ; informations sur les interactions avec le site Web, les produits et les services ; adresses ; date de naissance ; lieu de naissance ; adresses e-mail ; noms ; genre ; titre ; numéros de téléphone ; numéro de permis de conduire ; signature ; matricule d'employé ; informations de géolocalisation ; taux de rémunération ; nom d'utilisateur ; mot de passe ; informations sur les performances ; qualifications et restrictions.

Données sensibles transférées (le cas échéant) et restrictions ou garanties appliquées qui tiennent pleinement compte de la nature des données et des risques encourus, telles que, par exemple, une limitation stricte de la finalité, des restrictions d'accès (y compris l'accès uniquement au personnel ayant suivi une formation spécialisée), la conservation d'un enregistrement de l'accès aux données, les restrictions pour les transferts ultérieurs ou les mesures de sécurité supplémentaires

Aucune donnée sensible au sens du RGPD n'est transférée.

La fréquence du transfert (par exemple, si les données sont transférées de manière ponctuelle ou continue).

Transfert continu de données au fur et à mesure que le produit/la plateforme est utilisé par les utilisateurs finaux.

Nature du Traitement

Selon la nécessité pour la fourniture du produit/service en vertu du Contrat et selon les instructions de l'Exportateur.

Finalité(s) du transfert de données et Traitement ultérieur

Selon la nécessité pour la fourniture du produit/service ou à l'appui du produit/service.

La durée pendant laquelle les Données à caractère personnel seront conservées ou, si cela n'est pas possible, les critères utilisés pour déterminer cette durée

Pendant la période requise pour fournir le produit/service et en conjonction avec la politique et le calendrier de conservation des données de la Société ou tel que requis par la loi ou la réglementation applicable.

Pour les transferts aux Sous-traitants (ultérieurs), précisez également l'objet, la nature et la durée du Traitement

Pour l'assistance requise pour fournir le produit/service (c'est-à-dire les services de stockage dans le cloud) et pour la période requise pour fournir le produit/service.

C. AUTORITÉ DE CONTRÔLE COMPÉTENTE

Identifiez la ou les autorité(s) de contrôle compétente(s) conformément à la Clause 13

Autorité de protection des données des Pays-Bas.

ANNEXE II AUX CLAUSES CONTRACTUELLES TYPES

MESURES TECHNIQUES ET ORGANISATIONNELLES, Y COMPRIS LES MESURES TECHNIQUES ET ORGANISATIONNELLES VISANT À ASSURER LA SÉCURITÉ DES DONNÉES

Description des mesures techniques et organisationnelles mises en œuvre par le ou les Importateurs de données (y compris les éventuelles certifications pertinentes) pour assurer un niveau de sécurité approprié, compte tenu de la nature, de la portée, du contexte et de la finalité du Traitement, ainsi que des risques pour les droits et libertés des personnes physiques.

Mesures de pseudonymisation et de cryptage des Données à caractère personnel **Le cryptage en transit et au repos est mis en œuvre**

Mesures pour assurer la confidentialité, l'intégrité, la disponibilité et la résilience continues des systèmes et services de Traitement **Command Alkon s'auto-régit selon le cadre de sécurité NIST 800-171, ainsi que les AWS CIS Benchmarks v1.2 et AWS Foundational Best Practices v1.0**

Mesures pour garantir la capacité de restaurer la disponibilité et l'accès aux Données à caractère personnel en temps opportun en cas d'incident physique ou technique **Command Alkon effectue des sauvegardes programmées régulières et une architecture structurée à haute disponibilité est utilisée**

Processus de test et d'évaluation réguliers de l'efficacité des mesures techniques et organisationnelles afin d'assurer la sécurité du Traitement **Tests de vulnérabilité réguliers automatisés ; tests d'intrusion annuels ; audits annuels de confidentialité et de sécurité**

Mesures d'identification et d'autorisation des utilisateurs **Authentification multifacteur ; programme de mot de passe sophistiqué ; limitations d'autorisations ; journalisation**

Mesures de protection des données lors de la transmission **Cryptage en transit**

Mesures de protection des données pendant le stockage **Cryptage au repos ; contrôles d'accès logiques ; redondance via sauvegarde et basculement**

Mesures pour assurer la sécurité physique des lieux où les Données à caractère personnel sont traitées **Cartes/codes clés ; enregistrement des visiteurs ; vidéo de sécurité ; agents de sécurité ; formation en sécurité/confidentialité**

Mesures pour garantir la journalisation des événements **Journalisation en place et surveillée ; la journalisation est transmise à un service tiers géré ; alertes d'événement activées**

Mesures pour garantir la configuration du système, y compris la configuration par défaut **Tous les états et modifications de la configuration sont suivis ; programme de gestion du changement mis en place**

Mesures pour la gouvernance et la gestion internes de l'informatique et de la sécurité informatique **Politiques et procédures de sécurité et de confidentialité ; directeur de la sécurité de l'information ; équipe SecOps dédiée ; responsable de la confidentialité ; formation sécurité/confidentialité**

Mesures de certification/assurance des processus et des produits **NIST 800-171; CIS AWS Benchmark v1.2; AWS Foundational Best Practices v1.0**

Mesures pour garantir la minimisation des données **Les données traitées ne concernent que les champs saisis par les utilisateurs finaux/le Client/le Responsable du traitement**

Mesures pour garantir la qualité des données **Les données traitées sont saisies et conservées par les utilisateurs finaux/le Client/le Responsable du traitement**

Mesures pour garantir une conservation limitée des données **La conservation des données est contrôlée par des obligations contractuelles ainsi que par la politique et le calendrier de conservation des données**

Mesures pour garantir l'imputabilité **L'imputabilité est assurée par une journalisation surveillée ; la journalisation est transmise à un service tiers géré ; alertes d'événement activées**

Mesures pour permettre la portabilité des données et assurer leur effacement **La portabilité des données est gérée au cas par cas et l'effacement est assuré par des obligations contractuelles et des processus de notification et de confirmation**

Pour les transferts vers les Sous-traitants (ultérieurs), décrivez également les mesures techniques et organisationnelles spécifiques que le Sous-traitant (ultérieur) doit prendre pour pouvoir fournir une assistance au Responsable du traitement et, pour les transferts d'un Sous-traitant à un Sous-traitant ultérieurs, à l'Exportateur de données

Les Sous-traitants ultérieurs qui traitent les Données à caractère personnel sont soumis à des restrictions contractuelles et à des Addenda de traitement des données exigeant le respect des Clauses contractuelles types, le cas échéant.