ADDENDA SUR LE TRAITEMENT DES DONNÉES INTÉGRÉ À COMMAND ALKON

Mise à jour : 25/07/24

Cet addendum sur le traitement des données (« **DPA** ») fait partie du *contrat principal de licence et de services* (« **accord** ») entre : (i) le client (identifié dans le contrat de licence et de services principal) et ses filiales de l'EEE **(« Client ») ; et (ii)** Command Alkon Incorporated et ses filiales (« **Société** ») uniquement lorsque le règlement général sur la protection des données (« **RGPD** ») ou toute autre forme de confidentialité applicable législation.

Cet addendum remplace tout accord antérieur entre les parties concernant le sujet traité, à savoir la confidentialité et la sécurité des données conformément à la législation sur la protection de la vie privée.

Compte tenu des obligations mutuelles énoncées dans le présent document, les parties conviennent que les termes et conditions énoncés ci-dessous seront ajoutés en tant qu'addendum au contrat.

1. Définitions

Les « **données personnelles du client** » désignent les données personnelles traitées par l'entreprise pour le compte du client dans le cadre de la fourniture des produits et/ou services.

« **CCPA** » désigne la loi californienne sur la protection de la vie privée des consommateurs, telle que modifiée par la loi californienne sur les droits à la vie privée ou par d'autres législations/réglementations californiennes.

« **Personne concernée** » désigne la personne à laquelle se rapportent les données personnelles du client.

« Cadre de confidentialité des données » désigne le cadre juridique entre l'UE et les États-Unis pour les transferts transfrontaliers de données personnelles entre l'Union européenne et les États-Unis et inclut l'extension britannique à l'UE et aux États-Unis. DPF et Suisse-États-Unis PDF.

« **Lois sur la protection des données** » désigne toutes les lois et réglementations applicables relatives au traitement des données personnelles et à la confidentialité qui peuvent exister dans les juridictions concernées, y compris, le cas échéant, le règlement général sur la protection des données (UE) 2016/679 sur la protection des personnes physiques à l'égard du traitement des données personnelles et sur la libre circulation de ces données, et abrogeant la directive 95/46/CE (« RGPD ») (et toute modification ou remplacement de celle-ci), la loi fédérale suisse sur les données Protection (« FADP ») (et toute modification ou remplacement de celle-ci)), le RGPD européen tel que modifié et intégré au droit britannique en vertu de la loi britannique de 2018 sur le retrait et du droit secondaire applicable en vertu de cette loi (« RGPD britannique ») (et tout amendement ou remplacement de celui-ci), la loi canadienne sur la protection des informations personnelles et les documents électroniques (« PIPEDA ») (et tout amendement ou remplacement de celle-ci), la loi générale brésilienne

sur la protection des données (la « LRGPD ») (et tout amendement ou remplacement de celui-ci), le Privacy Act 1988 (Cth) de l'Australie, tel que modifié (« Loi australienne sur la protection de la vie privée ») (et tout amendement ou remplacement de celui-ci), le U.S. les lois de l'État sur la protection de la vie privée (y compris le CCPA et le CPRA de Californie) telles que publiées ou modifiées, ou toute autre législation applicable sur la protection de la vie privée exigeant un DPA. Lorsque le RGPD est spécifiquement mentionné, les mêmes exigences s'appliqueront à toute autre exigence équivalente de toute autre loi de protection des données applicable.

Les « **données personnelles** » désignent toutes les informations relatives 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'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de la personne concernée.

« **Processus** » ou « **Traitement** » désigne toute opération ou ensemble d'opérations effectuées sur les données personnelles du client, que ce soit par des moyens automatisés ou non, tels que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, la modification, la récupération, la consultation, l'utilisation, la divulgation, la suppression et/ou la destruction des données personnelles du client.

« **Faille de sécurité** » désigne une violation confirmée de la sécurité entraînant la destruction accidentelle ou illégale, la perte, l'altération, la divulgation ou l'accès non autorisé aux données personnelles du client transmises, stockées ou traitées d'une autre manière.

« **Clauses contractuelles types** » désigne les exigences contractuelles standard établies par la loi applicable en matière de protection des données (clauses contractuelles types de l'UE, clauses contractuelles types du Conseil latino-américain de protection des données du RIDP, clauses contractuelles types de l'ASEAN, etc.).

« Tiers » désigne un tiers autre que le client ou l'entreprise.

Les termes « **responsable du traitement** », « **sous-traitant** » et « **autorité de surveillance** » tels qu'ils sont utilisés dans le présent DPA auront le sens qui leur est attribué dans la loi sur la protection des données applicable.

Tous les autres termes non définis mais en majuscules auront le sens indiqué dans le contrat ou dans la loi sur la protection des données applicable.

2. Traitement des données personnelles des clients

2.1 Finalité du traitement. Le but du traitement des données dans le cadre de ce DPA est de fournir les produits et/ou services conformément au contrat. L'annexe 1 décrit l'objet et les détails du traitement des données personnelles des clients.

2.2 Responsabilités du processeur et du responsable du traitement. Les parties reconnaissent et conviennent que : (a) La société traite les données personnelles des clients en vertu des lois sur la protection des données ; (b) le client est responsable du traitement des données personnelles du client en vertu des lois sur la protection des données ; (c) le client est chargé d'obtenir toutes les autorisations et approbations

nécessaires pour saisir, utiliser, fournir, stocker et traiter les données personnelles du client afin de permettre à l'entreprise de fournir les produits et/ou services ; et (d) chaque partie respectera les obligations applicables à conformément aux lois sur la protection des données en ce qui concerne le traitement des Données personnelles du client.

2.3 Lois américaines sur la protection des données. Aux fins des lois américaines sur la protection des données (y compris le CCPA), « responsable du traitement » inclut « entreprise » ; « processeur » inclut « fournisseur de services » ; « personne concernée » inclut « consommateur » ; et « données personnelles » inclut les « informations personnelles ». L'entreprise est un fournisseur de services et le client est une entreprise.

2.4 Instructions pour les clients. Le client demande à l'entreprise de traiter ses données personnelles : (a) conformément au contrat et à tout supplément applicable ; (b) dans la mesure où cela est nécessaire pour fournir les produits et/ou services au client ; (c) conformément à la loi ou à la réglementation en vigueur ; et (d) pour se conformer aux autres instructions écrites raisonnables fournies par le client lorsque ces instructions sont conformes aux termes du contrat. Le client veillera à ce que ses instructions relatives au traitement de ses données personnelles soient 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 de ses données personnelles et de la manière dont le client les a obtenues.

2.5 Conformité de l'entreprise aux instructions du client. La société ne traitera les données personnelles du client que conformément aux instructions du client et traitera les données personnelles du client comme des informations confidentielles. Si la société pense ou apprend que l'une des instructions du client est contraire aux lois sur la protection des données, elle en informera le client dans un délai raisonnable. La société peut traiter les données personnelles du client autrement que selon les instructions écrites du client si cela est requis par la loi applicable à laquelle l'entreprise est soumise. Dans ce cas, la société informera le client de cette exigence avant de traiter les données personnelles du client, sauf si la loi applicable l'interdit.

2.6 Traitement CCPA. Dans la mesure où le traitement des données personnelles par l'entreprise est soumis au CCPA, l'entreprise certifie qu'elle ne doit pas : (a) conserver, utiliser ou divulguer les données personnelles du client autrement que comme prévu dans le contrat, pour fournir les produits et/ou services, pour créer ou améliorer la qualité des produits et/ou services, pour détecter les incidents de sécurité, pour se protéger contre les activités frauduleuses ou illégales, pour faire appel à des sous-traitants conformément à ce DPA, ou comme autorisé autrement par le CCPA ; ou (b) vendre ou partager les données personnelles des clients.

3. Sous-traitants

3.1 Désignation de sous-traitants. Le client fournit par la présente une autorisation écrite générale permettant à la société de faire appel à des sous-traitants tiers pour fournir des services limités ou accessoires liés à la fourniture de produits et/ou de services. Le site Web de la société répertorie les sous-processeurs actuellement engagés par la société pour effectuer des activités de traitement spécifiques liées aux données

personnelles des clients (https://commandalkon.com/sub-processor-list/) et la société mettra à jour la liste des sous-processeurs avant de faire appel à un nouveau sous-traitant pour effectuer un traitement spécifique. Le client peut s'inscrire pour recevoir des mises à jour électroniques chaque fois que la liste des sous-traitants de la société est modifiée en envoyant une telle demande à privacy@commandalkon.com. Le client peut s'opposer à tout sous-traitant en communiquant son objection à la société dans les trente (30) jours suivant la mise à jour, et les parties travailleront de bonne foi pour résoudre l'objection. Le client accepte par la présente que les activités de sous-traitement soient sous-traitées par les sous-traitants actuels répertoriés sur le site Web de la société.

3.2 Sécurité des sous-processeurs. Lorsque la société sous-traite ses obligations, elle ne le fera que par le biais d'un accord écrit avec le sous-traitant qui impose des obligations contractuelles au moins équivalentes à celles imposées à la société en vertu du présent addendum. Les parties conviennent que les copies des accords avec les sous-traitants autorisés qui doivent être fournies conformément aux clauses contractuelles types applicables ne seront fournies que sur demande écrite du client.

3.3 Responsabilité. Lorsque le sous-traitant ne respecte 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 en vertu de cet accord.

4. Responsabilités en matière de sécurité

4.1 Sécurité de l'entreprise. La société mettra en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données personnelles des clients (« **Programme de sécurité de l'information** ») en tenant compte de l'état de la technique, des coûts de mise en œuvre, de la nature, de l'étendue, du contexte et des objectifs du traitement, ainsi que du risque plus ou moins probable pour les droits et libertés des personnes physiques. L'entreprise se gouverne selon les normes de sécurité suivantes : NIST 800-171 ; AWS CIS.

4.2 Sécurité des clients. Le client reconnaît que les produits et/ou services incluent certaines caractéristiques et fonctionnalités qu'il peut choisir d'utiliser et qui ont un impact sur la sécurité des données personnelles du client traitées dans le cadre de son utilisation des produits et/ou services. Le client est chargé d'examiner les informations mises à disposition par l'entreprise 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 de la législation applicable en matière de protection des données. Le client est également responsable de la configuration correcte des produits et/ou services et de l'utilisation des fonctionnalités mises à disposition par la société afin de garantir une sécurité appropriée compte tenu de la nature des données personnelles du client traitées dans le cadre de l'utilisation des produits et/ou services par le client. Le client est responsable de son utilisation des produits et/ou services et du stockage de toute copie de ses données personnelles en dehors des systèmes de l'entreprise ou des sous-traitants de l'entreprise, y compris, mais sans s'y limiter, de la sécurisation des informations d'identification, des systèmes et des appareils d'authentification du

compte, et de la conservation de copies de ses données personnelles du client, le cas échéant.

4.3 Personnel de l'entreprise. La société doit veiller à ce que son personnel chargé du traitement des données personnelles des clients soit informé de la nature confidentielle des données personnelles des clients, ait reçu une formation appropriée sur ses responsabilités et soit soumis à des obligations de confidentialité, ces obligations survivant à la fin de l'engagement de cette personne au sein de la société.

4.4 Tests de sécurité. La société testera, évaluera et évaluera l'efficacité du programme de sécurité de l'information pour garantir le traitement sécurisé des données personnelles des clients. La société se conformera à son programme de sécurité des informations 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 à mener des consultations connexes avec toute autorité de surveillance si le client est tenu de réaliser de telles évaluations d'impact en vertu des lois sur la protection des données.

5. Droits des personnes concernées

5.1 Assistance au respect des obligations du client. Dans la mesure où le client, lorsqu'il utilise ou reçoit les produits et/ou services, n'est pas en mesure de corriger, modifier, restreindre, bloquer ou supprimer ses données personnelles comme l'exigent les lois sur la protection des données, la société doit rapidement répondre aux demandes raisonnables du client visant à faciliter de telles actions dans la mesure où la société est légalement autorisée et capable de le faire. Si la loi l'autorise, le client est responsable de tous les frais liés à la fourniture d'une telle assistance par la société.

5.2 Obligations de notification. Dans la mesure permise par la loi, la société informera rapidement le client si elle reçoit une demande d'accès, de correction, de modification, de suppression ou d'objection au traitement des données personnelles du client concernant cette personne. La société ne répondra à aucune demande de ce type concernant les données personnelles du client sans le consentement écrit préalable du client, sauf pour confirmer que la demande concerne le client. En outre, dans la mesure permise par la loi, la société informera rapidement le client si elle reçoit une demande de divulgation ou de correspondance, un avis ou toute autre communication concernant les données personnelles du client de la part des forces de l'ordre, d'une autorité compétente ou d'une autorité de protection des données compétente. La société doit apporter au client une coopération et une assistance appropriées et raisonnables pour traiter toute demande de ce type, dans la mesure permise par la loi et dans la mesure où le client n'a pas accès à ces données personnelles du client par le biais de son utilisation ou de la réception des produits et/ou services. Si la loi l'autorise, le client est responsable de tous les frais liés à la fourniture d'une telle assistance par la société.

6. Violation de données personnelles

6.1 Obligations de notification. Si la société prend connaissance d'une violation de sécurité avérée impliquant les données personnelles du client, elle en informera le client dans les meilleurs délais et en tout état de cause au plus tard soixante-douze (72) heures après la confirmation. Les obligations énoncées dans cette section 6 ne s'appliquent pas aux incidents causés par le client ou le personnel du client ou aux utilisateurs finaux, ni aux tentatives infructueuses ou aux activités qui ne compromettent pas la sécurité des données personnelles du client, y compris les tentatives de connexion infructueuses, les pings, les scans de port, les attaques par déni de service et les autres attaques réseau contre des pare-feux ou des systèmes en réseau.

6.2 Mode de notification. La notification des violations de sécurité, le cas échéant, sera envoyée au point de contact 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 applicables au client et de toute obligation de notification à un tiers liée à une violation de la sécurité des données personnelles.

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

6.3.1 décrire la nature de la faille de sécurité, les catégories et le nombre de personnes concernées, ainsi que les catégories et le nombre d'enregistrements de données personnelles concernés ;

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

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

6.3.4 décrire les mesures prises ou proposées pour remédier à cette faille de sécurité.

7. Suppression ou renvoi des données personnelles des clients

7.1 Supprimer ou retourner. Sous réserve de la section 7.3, la société accepte de supprimer 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 personnelles du client (la « **date de cessation** »), de supprimer de manière sécurisée les données personnelles du client ou, sur demande écrite du client en temps opportun, de renvoyer une copie complète de toutes les données personnelles du client par transfert de fichiers sécurisé dans le format raisonnablement demandé par le client.

7.2 Si le client et l'entreprise ont conclu des clauses contractuelles types exigeant la certification de suppression par écrit (comme les clauses 8.5 et 16 des CCS de l'UE), les parties conviennent que la certification écrite ne sera fournie que sur demande écrite du client.

7.3 Définition de la suppression. Pour plus de précisions, « **Supprimer** » signifie supprimer ou effacer les données personnelles du client afin qu'elles ne puissent pas être récupérées ou reconstruites.

7.4 Records. La société peut conserver les données personnelles des clients 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 personnelles des clients.

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 l'étendue, 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, conformément aux politiques de l'entreprise, et ne doit pas interférer de manière déraisonnable avec les activités commerciales de la société. Tous les audits sont aux frais et frais du client. La société coopérera à tout client ou à toute demande d'audit émanant d'une autorité réglementaire ou de surveillance compétente afin de vérifier le respect par la société de ses obligations en vertu du présent DPA en mettant à disposition, sous réserve d'obligations de confidentialité, des rapports d'audit tiers, le cas échéant, et/ou des descriptions des contrôles de sécurité et autres informations raisonnablement demandées par le client concernant les pratiques et politiques de sécurité de l'entreprise.

8.2 Assistance en matière de conformité. Compte tenu de la nature du traitement et des informations mises à la disposition de l'entreprise, la société fournira une coopération et une assistance appropriées et raisonnables au client en ce qui concerne 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 traiter les données personnelles du client aux États-Unis d'Amérique et dans tout autre pays dans lequel la société ou l'un de ses sous-traitants possède des installations ou traite des données personnelles d'une autre manière. Tout transfert de ce type sera régi d'abord par la certification du cadre de confidentialité des données de la société ou, sinon, par les clauses contractuelles types interaffiliées de la société. La société ne transférera ni ne fera transférer les données personnelles du client d'une juridiction à une autre, sauf conformément à la loi applicable, et n'obligera pas le client à enfreindre une quelconque loi sur la protection des données.

9.2 Clauses contractuelles types. Dans la mesure et uniquement dans la mesure où l'entreprise traite les données personnelles des clients depuis l'Espace économique européen et que des clauses contractuelles types sont requises, le module 2 des clauses contractuelles types s'applique et est intégré aux présentes. Aux fins des clauses

contractuelles types, le client est « l'exportateur de données » et l'entreprise est « l'importateur de données ».

9.3 Addendum britannique aux clauses contractuelles types de l'UE. Dans la mesure et uniquement dans la mesure où l'entreprise traite les données personnelles des clients depuis le Royaume-Uni et où des clauses contractuelles types sont requises, les parties conviennent que l'addendum britannique s'appliquera aux données personnelles transférées via les produits et/ou services depuis le Royaume-Uni, directement ou par transfert ultérieur, vers un pays ou un destinataire en dehors du Royaume-Uni qui n'est pas reconnu par l'autorité réglementaire ou l'organisme gouvernemental britannique compétent pour le Royaume-Uni comme fournissant un niveau adéquat de protection pour les données personnelles.

9.4 Swiss FADP. Dans la mesure et uniquement dans la mesure où l'entreprise traite les données personnelles des clients depuis la Suisse, les exigences supplémentaires suivantes s'appliquent dans la mesure où les transferts de données sont exclusivement soumis au FADP ou à la fois au FADP et au RGPD de l'UE : (a) le terme « État membre » ne doit pas être interprété de manière à exclure les personnes concernées en Suisse de la possibilité de faire valoir leurs droits dans leur lieu de résidence habituel (Suisse) en conformément à la clause 18 (c) des clauses contractuelles types ; (b) dans la mesure où les transferts de données sous-jacents aux clauses contractuelles types sont exclusivement soumis au FADP, les références au RGPD de l'UE doivent être considérées comme des références au FADP ; et (c) dans la mesure où les transferts de données sous-jacents aux clauses contractuelles types sont soumis à la fois au FADP et au RGPD de l'UE, les références au RGPD de l'UE doivent être considérées comme des références au FADP dans la mesure où les transferts de données sont soumis au FADP.

9.5 Mesures supplémentaires. Outre les clauses contractuelles types, si la société apprend qu'une autorité gouvernementale (y compris les forces de l'ordre) souhaite accéder à certaines ou à toutes les données personnelles du client traitées par l'entreprise, que ce soit sur une base volontaire ou obligatoire, à des fins liées au renseignement de sécurité nationale, alors sauf interdiction légale ou obligation légale contraire, la société : 1) informera immédiatement le client auquel s'appliquent les données personnelles ; 2) informera le autorité gouvernementale compétente qui n'a pas été autorisée à divulguer les données personnelles du client et, sauf interdiction légale, devra immédiatement informer le client auquel s'appliquent les données personnelles du client ; 3) informer les autorités gouvernementales qu'elles doivent adresser toutes les demandes ou demandes directement au client auquel s'appliquent les données personnelles du client ; et 4) ne pas donner accès aux données personnelles du client avant d'avoir obtenu l'autorisation écrite du client concerné ou d'y être légalement obligée. Si la loi l'y oblige, la société déploiera des efforts raisonnables et légaux pour contester cette interdiction ou cette contrainte. Si la société est obligée de produire les données personnelles du client, elle ne divulguera les données personnelles du client que dans la mesure où la loi l'y oblige conformément à la procédure légale applicable.

9.6 Loi sur la surveillance du renseignement extérieur. La société n'avait encore reçu aucune directive en vertu de la section 702 de la loi américaine sur la surveillance du renseignement extérieur, codifiée au 50 U.S.C. §1881a (« Section 702 de la FISA »).

Aucun tribunal n'a considéré que la société était le type d'entité éligible au traitement délivré en vertu de la section 702 de la FISA. L'entreprise n'est pas le type de fournisseur éligible à la collecte en amont (collecte « en vrac ») conformément à la section 702 de la FISA, telle que décrite dans la décision *Schrems II.*

9.7 Priorité de transfert. Si les services sont couverts par plusieurs mécanismes de transfert, le transfert des données personnelles du client sera soumis à un mécanisme de transfert unique conformément à l'ordre de priorité suivant : (i) certification du cadre de confidentialité des données de l'entreprise ; (ii) clauses contractuelles types applicables (lorsque la loi sur la protection des données l'exige).

10. Durée et résiliation

Durée du DPA. Ce DPA entrera en vigueur à la date à laquelle le contrat sera entièrement exécuté et, indépendamment de l'expiration de la durée de tout abonnement acheté, restera en vigueur jusqu'à la suppression de toutes les données personnelles du client, comme décrit dans ce DPA.

11. Non-conformité ; voies de recours ; parties

11.1 Limitation de responsabilité. La responsabilité de l'entreprise en cas de violation de ses obligations en vertu du présent DPA est soumise aux dispositions de limitation de responsabilité du contrat.

11.2 Parties à ce DPA. Aucune disposition du DPA ne confère d'avantages ou de droits à une personne ou entité autre que les parties à ce DPA.

12. Conditions générales

Loi applicable et juridiction

12.1 Ce DPA sera revu un an après sa date de publication, puis trois ans plus tard, ou plus tôt s'il y a lieu.

12.2 Sauf si les clauses contractuelles types l'exigent :

12.2.1 les parties à cet addendum se soumettent au choix de la juridiction stipulé dans le contrat en ce qui concerne tout litige ou réclamation découlant de cet addendum, y compris les litiges concernant son existence, sa validité ou sa résiliation ; et

12.2.2 cet addendum et toutes les obligations non contractuelles ou autres qui en découlent ou y sont liées 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 addendum et les clauses contractuelles types dans lesquelles les clauses contractuelles types sont requises, les clauses contractuelles types prévaudront.

12.4 Sous réserve de la section 12.2, en ce qui concerne l'objet du présent addendum, en cas d'incompatibilité entre les dispositions de cet addendum et tout autre accord entre les parties, y compris le contrat et y compris (sauf accord contraire explicite écrit, signé au nom des parties) les accords conclus ou censés avoir été conclus après la date de cet addendum, les dispositions du présent addendum prévaudront.

Modifications apportées aux lois sur la protection des données

12.5 Le client peut :

12.5.1 par un préavis écrit d'au moins trente (30) jours calendaires adressé à la société de temps à autre, proposer toute modification des clauses contractuelles types qui serait requise à la suite d'une modification ou d'une décision d'une autorité compétente en vertu de cette loi sur la protection des données ; et

12.5.2 proposer toute autre variante de cet addendum que le client juge raisonnablement nécessaire pour répondre aux exigences de toute loi sur la protection des données.

12.6 Si le client donne un préavis conformément à la section 12.5, les parties discuteront rapidement des variantes proposées et négocieront de bonne foi en vue de convenir et de mettre en œuvre ces variantes ou d'autres variantes conçues pour répondre aux exigences identifiées dans la notification du client dès que cela sera raisonnablement possible.

Indemnité

12.7 Si l'une des dispositions de cet addendum est invalide ou inapplicable, le reste de cet addendum restera valide et en vigueur. La disposition invalide ou inapplicable doit être soit : (i) modifiée si nécessaire pour garantir sa validité et son applicabilité, tout en préservant au maximum les intentions des parties, soit, si cela n'est pas possible ; (ii) interprétée de manière à ce que la partie invalide ou inapplicable n'y ait jamais été contenue.

Annexe I — Détails du traitement des données

Exportateur de données (responsable du traitement) : client tel qu'identifié dans le contrat.

Importateur de données (processeur) : société telle qu'identifiée dans le contrat.

Objet : L'objet du traitement des données dans le cadre de ce DPA concerne les données personnelles du client.

Durée du traitement : La durée du contrat plus la période jusqu'à ce que la société supprime toutes les données personnelles du client conformément au présent DPA.

Objectif : Le but du traitement des données est de fournir les produits et/ou services au client.

Nature du traitement : La nature du traitement des données est destinée à la fourniture des produits et/ou services tels que décrits dans le contrat.

Catégories de personnes concernées : employés des clients et employés des filiales, clients et partenaires commerciaux du client.

Types de données personnelles : Le client peut télécharger, soumettre ou fournir certaines données personnelles relatives aux produits et/ou services, dont l'étendue est généralement déterminée et contrôlée par le client à sa seule discrétion et peut inclure des informations de contact ; des informations sur les interactions avec le site Web, les produits et les services ; des adresses ; des adresses ; des informations de géolocalisation ; des adresses e-mail ; des noms ; le sexe ; le titre ; les numéros de téléphone ; le numéro de permis de conduire ; la signature ; le numéro d'employé ; les informations de géolocalisation ; le taux de rémunération ; nom d'utilisateur ; mot de passe ; performance informations ; qualifications et restrictions ; informations sur l'appareil.

Données sensibles transférées : aucune.

Fréquence du transfert : continue selon les besoins pour la fourniture des produits et/ou services.

Transferts aux sous-traitants : comme indiqué dans la liste des sous-processeurs de la société disponible sur https://commandalkon.com/sub-processor-list/ .

Autorité de surveillance compétente : conformément aux lois applicables en matière de protection des données ou, par ordre d'entrée en vigueur, 1) conformément aux termes du contrat ou 2) Autorité de protection des données des Pays-Bas.

Conservation : conformément au contrat et au présent DPA.

Mesures **techniques et organisationnelles : Les mesures** de sécurité techniques et organisationnelles mises en œuvre par l'importateur de données sont décrites dans la section 4.1 du DPA. Des informations supplémentaires sont disponibles sur demande.