ADDENDUM RELATIF AU TRAITEMENT DES DONNÉES

Le présent Addendum relatif au traitement des données (« **ATD** ») fait partie du Contrat-cadre (« **Contrat** ») en vertu duquel l'entité du Prestataire fournit des Services pour les logiciels et les produits professionnels. Tous les termes commençant par une majuscule qui ne sont pas définis dans le présent ATD auront le sens qui leur est donné dans d'autres parties du Contrat.

1. Définitions et interprétation

« **Affilié autorisé** » désigne tout Affilié du Client qui (a) est soumis aux lois et réglementations sur la protection des données d'une Juridiction couverte, et (b) est autorisé à utiliser les Services en vertu du Contrat entre le Prestataire et le Client, mais n'a pas signé son propre Bon de commande avec le Prestataire et n'est pas un « Client » tel que défini en vertu du Contrat.

« **Juridiction couverte** » désigne un traitement transfrontalier de Données à caractère personnel qui est restreint par les Lois sur la protection des données parce que la divulgation est faite à une personne ou entité située dans une juridiction dont l'autorité gouvernementale compétente ou le Sous-traitant des données détermine qu'il n'assure pas le même niveau ou un niveau supérieur de protection des données par rapport à la juridiction d'où proviennent les Données à caractère personnel.

« **Responsable du traitement** » désigne la personne physique ou morale, l'autorité publique, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du Traitement des données à caractère personnel. Aux fins du présent ATD, le Responsable du traitement des données est le Client et, le cas échéant, ses Affiliés autorisés par le Client à soumettre des Données à caractère personnel au(x) Service(s) ou dont les Données à caractère personnel sont traitées dans le(s) Service(s).

« **Sous-traitant** » désigne la personne physique ou morale, l'autorité publique, l'agence ou tout autre organisme qui Traite les Données à caractère personnel pour le compte du Responsable du traitement. Aux fins du présent ATD, le Sous-traitant est l'entité du Prestataire qui est partie au Contrat.

« **Lois sur la protection des données** » désigne toutes les lois et réglementations applicables concernant le Traitement des données à caractère personnel, qui peuvent inclure, sans s'y limiter, chacune des lois suivantes, telle que modifiée, annulée ou remplacée : la Loi sur la protection des données à caractère personnel en Argentine (Argentina Personal Data Protection Act, ***ARGENTINE***). la Loi australienne sur la protection de la vie privée de 1988 et 13 Principes australiens de protection de la vie privée (Australia Privacy Act 1988 and 13 Australian Privacy Principles) ***AUSTRALIE***), la Loi californienne sur la protection de la vie privée des consommateurs (California Consumer Privacy Act), Cal. Civ. Code § 1798.100 et suivants (***CA, États-Unis***), la Loi canadienne sur la protection des renseignements personnels et les documents électroniques de 2000 (Canada Personal Information Protection and Electronic Documents Act 2000) et la Loi sur le secteur privé du Québec, Loi 25 (Quebec Private Sector Act, Law 25) (***CANADA***), les Lois sur la protection des informations personnelles de la République populaire de Chine (People's Republic of China Personal Information Protection Laws) (***CHINE***), les Lois et règlements du Dubai International Financial Centre sur la protection des données (Dubai International Financial Centre Data Protection Laws and Regulations) (***DUBAI***), le Règlement général sur la protection des données (UE) 2016/679 de l'Union européenne (***UNION EUROPÉENNE***), l'Ordonnance sur les données à caractère personnel (confidentialité) de Hong Kong (Hong Kong Personal Data (Privacy) Ordinance (Cap. 486, Laws of Hong Kong)) (***HONG KONG***), les Règles indiennes de 2011 en matière de technologie de l'information (India Information Technology Rules 2011) et la loi sur la protection des données personnelles numériques de 2023 (Digital Personal Data Protection Act, 2023) (***INDE***), la Loi japonaise sur la protection des informations personnelles (Kojin Joho no Hogo ni Kansuru Houritsu, Loi n° 57 de 2003) (***JAPON***), la Loi malaisienne sur la protection des données personnelles

de 2010 (Malaysia Personal Data Protection Act 2010) (***MALAISIE***), la Loi fédérale du Mexique sur la protection des données à caractère personnel (Mexico Federal Law on the Protection of Personal Data) (***MEXIQUE***) ; la Loi néo-zélandaise sur la protection de la vie privée de 2020 (New Zealand Privacy Act 2020) (***NOUVELLE-ZÉLANDE***), la Loi de 2012 sur la protection des données aux Philippines (Philippines Data Privacy Act 2012) (***PHILIPPINES***), la Loi saoudienne sur la protection des données à caractère personnel 2021 (Saudi Arabia Personal Data Protection Law 2021) (***ARABIE SAOUDITE***), la Loi de 2012 sur la protection des données personnelles de Singapour (Singapore Personal Data Protection Act 2012) (***SINGAPOUR***), la Protection des informations personnelles en Afrique du Sud de 2021 (South Africa Protection of Personal Information) (***AFRIQUE DU SUD***), la Loi turque n° 6698 relative à la protection des données à caractère personnel (Turkey Law No. 6698 on the Protection of Personal Data) (**TURQUIE**), la Loi de 2021 sur la protection des données à caractère personnel des Émirats arabes unis (United Arab Emirates Personal Data Protection Law 2021) (***ÉAU***) et la Loi britannique sur la protection des données de 2018 (United Kingdom Data Protection Act 2018) et le Règlement général sur la protection des données du Royaume-Uni (UK General Data Protection Regulation) (***ROYAUME-UNI***).

« **Personne concernée** » désigne une personne qui est la personne concernée par les Données à caractère personnel et à qui ou à propos de laquelle les Données à caractère personnel se rapportent ou qu'elles identifient, directement ou indirectement. « **Données à caractère personnel** » désigne toute information relative à une Personne concernée identifiée ou identifiable téléchargée par ou pour le Client dans les Services en tant que Données du client.

« **Traitement, traiter** » désigne toute activité qui implique l'utilisation de Données à caractère personnel, ou selon les définitions des Lois sur la protection des données, qui peuvent différer. Cela comprend l'obtention, l'enregistrement ou la conservation des données, ou la réalisation de toute opération ou ensemble d'opérations sur les données, y compris l'organisation, la modification, l'extraction, l'utilisation, la divulgation, l'effacement ou la destruction de celles-ci. Le traitement comprend également le transfert de Données à caractère personnel à des tiers.

« **Violation de la sécurité** » désigne toute destruction, perte, altération, divulgation non autorisée ou accès accidentel ou illégal aux Données à caractère personnel.

« **Sous-traitant ultérieur** » désigne toute personne morale ou entité prenant part au Traitement des données à caractère personnel par le Sous-traitant.

2. Nature, portée et finalité du Traitement

2.1 Dans le cadre de l'exécution des Services, le Prestataire se conformera à la Politique de confidentialité du Prestataire, disponible à l'adresse https://gomomentus.com/privacy-policy et incorporée aux présentes par renvoi. La Politique de confidentialité du Prestataire est susceptible d'être modifiée à la discrétion du Prestataire. Cependant, les modifications apportées à la politique du Prestataire n'entraîneront pas de réduction substantielle du niveau de protection assuré pour les Données à caractère personnel fournies dans le cadre des Services en vertu du Contrat.

2.2 Le Client et le Prestataire reconnaissent qu'aux fins de toute Loi applicable sur la protection des données, le Client est le Responsable du traitement et que le Prestataire est le Sous-traitant.

2.3 Le Client conserve le contrôle des Données à caractère personnel et reste responsable de ses obligations de conformité en vertu des Lois sur la protection des données, y compris la fourniture de tous les avis requis et l'obtention de tous les consentements requis, et des instructions de traitement qu'il donne au Prestataire.

2.4 Le Prestataire ne traitera les Données à caractère personnel que conformément aux instructions du Client et dans la mesure nécessaire pour fournir les Services. Le Client reconnaît que toutes les Données à caractère personnel qu'il demande au Prestataire de traiter aux fins de fournir les Services doivent être limitées aux Données du client traitées dans le cadre du Service. Les détails du Traitement des données à caractère personnel effectué en vertu du présent ATD sont énoncés dans l'annexe A.

2.5 Les parties reconnaissent et conviennent qu'en signant le Contrat, le Client conclut le présent ATD en son nom et, le cas échéant, au nom de ses Affiliés autorisés, établissant ainsi un ATD distinct entre le Prestataire et chacune de ces Affiliés autorisés sous réserve des dispositions du Contrat. Chaque Affilié autorisé accepte d'être lié par les obligations prévues par le présent ATD. Afin d'éviter toute ambiguïté, un Affilié autorisé n'est pas et ne devient pas partie au Contrat et n'est partie qu'au présent ATD. Tout accès aux Services et toute utilisation des Services par des Affiliés autorisés doivent être conformes aux conditions générales du Contrat et toute violation des conditions générales du Contrat commise par un Affilié autorisé sera considérée comme une violation commise par le Client.

3. Mesures de traitement des données

3.1 Si le Prestataire estime que le respect des instructions du Client entraînerait une violation des Lois sur la protection des données ou n'est pas dans le cours normal des obligations du Prestataire dans le cadre de l'exploitation des Services, le Prestataire en informera rapidement le Client.

3.2 Les personnes autorisées par le Prestataire à traiter les Données à caractère personnel seront liées par des obligations de confidentialité appropriées. Le Prestataire a nommé un délégué à la protection des données. La personne désignée peut être contactée à l'adresse privacy@gomomentus.com.

3.3 Le Prestataire doit à tout moment mettre en œuvre des mesures techniques et organisationnelles appropriées conçues pour protéger les Données à caractère personnel contre le traitement, l'accès, la copie, la modification, le stockage, la reproduction, l'affichage ou la distribution non autorisés ou illégaux, et contre la perte, l'indisponibilité, la destruction ou les dommages accidentels. Pour certains Services, le Prestataire met également à disposition des fonctionnalités et des contrôles de sécurité que le Client peut choisir d'utiliser. Le Client est responsable de la mise en œuvre de toute mesure technique et organisationnelle facultative pour protéger les Données du client, comme décrit dans le Contrat ou la Documentation.

3.4 Le Prestataire aidera raisonnablement le Client à remplir ses obligations de conformité en vertu des Lois sur la protection des données, tout en tenant compte de la nature du traitement du Prestataire et des informations dont il dispose.

4. Notification de sécurité et de violation

4.1 Le Prestataire informera immédiatement le Client s'il prend connaissance de toute avancée technologique et de méthodes de travail, qui indiquent que les parties doivent ajuster leurs mesures de sécurité.

4.2 Le Prestataire doit prendre des précautions raisonnables pour préserver l'intégrité de toutes les Données à caractère personnel qu'il traite et pour prévenir toute corruption ou perte des Données à caractère personnel. Les Systèmes du prestataire sont programmés pour effectuer des sauvegardes quotidiennes de routine des données, comme indiqué dans la politique de sauvegarde du Prestataire en vigueur de temps à autre. Le Prestataire livrera au Client ses sauvegardes les plus récentes des Données du client. En cas de perte, destruction, dommage ou corruption des Données du client causés par les Systèmes ou les Services du prestataire, le Prestataire, à titre de seule obligation et responsabilité et comme seul recours du Client, déploiera des efforts commercialement raisonnables pour restaurer les Données du client à partir de la sauvegarde la plus récente desdites Données du client par le Prestataire.

4.3 Le Prestataire signalera au Client toute Violation de la sécurité sans retard injustifié après avoir constaté qu'une Violation de la sécurité s'est produite.

4.4 Le signalement initial sera adressé au(x) contact(s) de sécurité ou de confidentialité du Client désignés sur le portail d'assistance client du Prestataire (ou, si aucun contact n'est désigné, au contact technique principal désigné par le Client). Lorsque des informations pertinentes relatives à la Violation sont collectées ou deviennent autrement disponibles pour le Prestataire, il fournira lesdites informations sans retard injustifié au Client, afin d'aider le Client à se conformer à ses obligations de notification en vertu des Lois sur la protection des données. En particulier, et dans la mesure raisonnablement possible et applicable, le Prestataire fournira au Client les informations décrites à l'article 33 du RGPD.

4.5 Le Client coopérera avec le Prestataire pour maintenir des coordonnées exactes sur le portail d'assistance à la clientèle et en fournissant toutes les informations raisonnablement demandées pour résoudre les Violations de sécurité, identifier sa ou ses causes profondes et empêcher qu'elles ne se reproduisent. Le Client, en tant que Responsable du traitement des données, est seul responsable de déterminer s'il doit informer les autorités de contrôle ou de réglementation compétentes et les Personnes concernées affectées en cas de Violation de la sécurité et de fournir un tel avis.

5. Demandes des personnes concernées et des autorités.

5.1 Pendant la Durée de validité, le Prestataire donnera au Client la possibilité d'accéder, de corriger, de rectifier, d'effacer ou de bloquer les Données à caractère personnel, ou de transférer ou de porter lesdites Données à caractère personnel, au sein du Service d'abonnement, tel que cela peut être requis en vertu des Lois sur la protection des données (collectivement, les « **Demandes des personnes concernées** »).

5.2 Le Client sera seul tenu de répondre aux Personnes concernées s'agissant de toute Demande émanant des Personnes concernées, à condition que le Prestataire coopère raisonnablement avec le Client en ce qui concerne les Demandes des personnes concernées dans la mesure où le Client n'est pas en mesure de répondre à ces Demandes des personnes concernées en utilisant la fonctionnalité des Services. Le Prestataire demandera à la Personne concernée de contacter le Client si elle reçoit une Demande de personne concernée directement.

5.3 Dans le cas d'un avis, d'un audit, d'une enquête ou d'une enquête menée par un organisme public, une autorité de protection des données ou les forces de l'ordre concernant le Traitement des données à caractère personnel, le Prestataire en informera rapidement le Client, sauf si le droit applicable l'interdit. Chaque partie coopérera avec l'autre partie en fournissant toutes les informations raisonnables demandées et disponibles.

6. Audits.

6.1 Le Prestataire autorisera et contribuera aux audits qui comprennent les inspections en accordant au Client l'accès à une documentation raisonnable et reconnue par le secteur attestant des politiques et procédures régissant la sécurité et la confidentialité des Données à caractère personnel (« **Audit** »). Les informations disponibles dans un Audit comprendront la documentation prouvant les politiques et procédures de confidentialité concernant les Données à caractère personnel traitées, ainsi que des copies de toutes les certifications et rapports d'attestation qui existent à ces moments (y compris les audits). Dans la mesure où le Client n'a pas pu raisonnablement satisfaire à ses exigences d'audit en suivant la procédure décrite dans la présente Clause, le Prestataire fournira au Client l'assistance supplémentaire qui peut raisonnablement être requise (conformément aux obligations d'assistance décrites dans les présentes) pour satisfaire substantiellement à ces exigences.

6.2 À la demande du Client en envoyant un e-mail à privacy@gomomentus.com, le Prestataire et le

Client peuvent planifier un moment qui conviendra aux deux parties pour s'entretenir de l'Audit. Dans le cas où l'Audit donnerait lieu à des constatations de non-conformité importante vis-à-vis de l'ATD, le Prestataire traitera rapidement ces constatations de non-conformité. Le Prestataire peut, à sa seule discrétion et conformément aux normes et pratiques du secteur et du Prestataire, faire des efforts commercialement raisonnables pour mettre en œuvre les améliorations suggérées par le Client notées dans l'Audit afin d'améliorer le programme de sécurité du Prestataire. L'Audit et les résultats qui en découlent sont des Informations confidentielles du prestataire.

7. Sous-traitants.

7.1 Le Client reconnaît et convient que (a) les Affiliés du prestataire peuvent être retenues en tant que Sous-traitants ultérieurs ; et (b) le Prestataire et les Affiliés du prestataire peuvent respectivement engager des Sous-traitants ultérieurs tiers dans le cadre de la fourniture des Services. Le Prestataire ou un Affilié du prestataire a conclu un accord écrit avec chaque Sous-traitant ultérieur contenant, en substance, des obligations de protection des données au moins aussi protectrices que celles du Contrat en ce qui concerne la protection des Données du client dans la mesure où elles s'appliquent à la nature des Services fournis par ce Sous-traitant ultérieur. La liste actuelle des Sous-traitants ultérieurs prenant part au Traitement des données à caractère personnel pour l'exécution de chaque Service applicable, y compris une description de leurs activités de traitement et de leurs pays de localisation, est indiquée à l'annexe B, qui peut être mise à jour de temps à autre ou conformément à la clause 7.2. Le Client consent par les présentes à ces Sous-traitants ultérieurs, à leurs emplacements et à leurs activités de traitement en ce qui concerne ses Données à caractère personnel.

7.2 Pour les Juridictions couvertes, avant que le Prestataire n'engage un nouveau Sous-traitant ultérieur pour les Services, le Prestataire : (a) informera le Client en envoyant un e-mail à l'interlocuteur désigné du Client sur les portails ou les comptes d'assistance du Prestataire (ou par tout autre mécanisme utilisé pour notifier sa clientèle) ; et (b) fera en sorte que ledit Sous-traitant ultérieur conclue un accord écrit avec le Prestataire (ou l'Affilié du prestataire concerné) exigeant que le Sous-traitant ultérieur respecte des conditions au moins aussi protectrices que celles prévues dans le présent ATD. En ce qui concerne la fourniture de l'avis décrit dans la phrase précédente, le Prestataire fournira un préavis écrit d'au moins 30 jours avant d'engager un Sous-traitant ultérieur en ce qui concerne les Services existants que le Client a achetés. Si un nouveau Sous-traitant ultérieur est engagé pour prendre en charge un nouveau Service ou une nouvelle fonctionnalité d'un Service d'abonnement existant, alors l'avis décrit dans la présente clause sera fournie au moment où cette fonctionnalité ou ce service d'abonnement sera mis à la disposition du public. Sur demande écrite du Client en envoyant un e-mail à l'adresse privacy@gomomentus.com, le Prestataire mettra à la disposition du Client un résumé des conditions de traitement des données avec le Sous-traitant ultérieur. Le Client peut demander par écrit en envoyant un e-mail à l'adresse privacy@gomomentus.com des informations supplémentaires raisonnables concernant la capacité du Sous-traitant ultérieur à effectuer les activités de Traitement pertinentes conformément au présent ATD.

7.3 Le Client peut s'opposer au recours par le Prestataire à un nouveau Sous-traitant ultérieur en en informant rapidement le Prestataire par écrit dans les trente (30) jours suivant la réception de l'avis du Prestataire conformément au mécanisme énoncé à la clause 7.2. Si le Client s'oppose à un nouveau Sous-traitant ultérieur tel qu'autorisé dans la phrase précédente, le Prestataire déploiera des efforts raisonnables pour mettre à la disposition du Client une modification des Services ou recommander une modification raisonnable de la configuration ou de l'utilisation des Services par le Client afin d'éviter le Traitement des données à caractère personnel par le nouveau Sous-traitant ultérieur ayant fait l'objet de l'opposition sans surcharger déraisonnablement le Client. Si le Prestataire n'est pas en mesure de mettre à disposition cette modification dans un délai raisonnable après que les deux parties aient échangé de bonne foi, lequel délai qui ne dépassera pas quatre-vingt-dix (90) jours, le Client pourra, moyennant un préavis de trente (30) jours, résilier le ou les Bon(s) de commande concerné(s) s'agissant uniquement des Services qui ne peuvent pas être fournis par le Prestataire sans le recours au nouveau Sous-traitant ultérieur ayant fait l'objet de l'opposition. Le droit du Client de résilier les Services concernés en vertu de la présente clause ne dégagera pas le Client de toute

obligation de paiement en vertu du Contrat jusqu'à la date de résiliation. Si la résiliation conformément à la présente clause ne concerne qu'une partie des services en vertu d'un Bon de commande, le Client accepte de conclure un avenant ou une commande de remplacement pour tenir compte de ladite résiliation partielle.

7.4 Le recours à un Sous-traitant ultérieur n'aura pas pour effet la levée, la renonciation ou la diminution de toute obligation du Prestataire en vertu du présent ATD, et le Prestataire est responsable des actes et omissions de tout Sous-traitant ultérieur dans la même mesure que si les actes ou omissions étaient commis par le Prestataire.

8. Limitation de responsabilité et durée.

8.1 La responsabilité de chaque partie et de l'ensemble de ses Affiliés, prise ensemble, découlant du présent ATD ou y afférente, et de tous les ATD entre les Affiliés autorisés et le Prestataire, que ce soit en matière contractuelle, délictuelle ou en vertu de toute autre théorie de responsabilité, est soumise à la section « Limitation de responsabilité » du Contrat, et toute référence dans cette section à la responsabilité d'une partie désigne la responsabilité globale de cette partie et de tous ses Affiliés en vertu du Contrat et de tous les ATD pris ensemble. Pour éviter toute ambiguïté, la responsabilité totale du Prestataire et de ses Affiliés pour toutes les réclamations du Client et de tous ses Affiliés autorisés découlant du Contrat et de tous les ATD ou s'y rapportant s'appliquera dans l'ensemble pour toutes les réclamations en vertu du Contrat et de tous les ATD établis en vertu du Contrat, y compris par le Client et tous les Affiliés autorisés, et, en particulier, ne s'appliquera pas individuellement et solidairement au Client ou à tout Affilié autorisé qui est une partie contractuelle à un tel ATD.

8.2 Le présent ATD demeurera pleinement applicable tant que la Durée du contrat demeurera applicable ou que le Prestataire gardera toutes les Données à caractère personnel liées au Contrat en sa possession ou sous son contrôle. En cas de conflit entre les conditions du présent ATD et les conditions du Contrat en ce qui concerne l'objet des présentes, le présent ATD prévaudra. Le Sous-traitant principal est une société américaine et, par conséquent, la version standard de l'ATD est la version anglaise. En cas de mauvaise interprétation due à la traduction des documents en français ou en allemand, la version anglaise prévaut toujours.

9. Transferts internationaux de données.

9.1 Le transfert de Données à caractère personnel d'une Juridiction couverte vers un pays qui n'est pas situé dans une juridiction faisant l'objet d'une décision d'adéquation valide (telle que déterminée par les Lois sur la protection des données concernant les personnes au sujet desquelles les Données à caractère personnel sont traitées) (un « **Transfert de données** ») sera soumis aux clauses contractuelles types (CCT) ci-dessous, sous réserve des ajustements nécessaires pour se conformer aux Lois sur la protection des données. Pour tous les Services, les Données à caractère personnel seront stockées/hébergées dans la région du centre de données spécifiée dans le Bon de commande/Contrat pour lesdits Services ou, le cas échéant, la région géographique qui a été sélectionnée lors de l'activation de l'instance de production desdits Services. Nonobstant ces exigences de stockage/hébergement et sous réserve du présent ATD, le Prestataire peut traiter les Données à caractère personnel dans le monde entier si cela est nécessaire pour exécuter les Services, notamment à des fins d'assistance, de gestion des incidents ou de récupération des données.

9.2 Loi sur la protection des données de l'EEE.

(a) En cas de Transfert de données soumis aux Lois sur la protection des données de l'EEE, le Transfert de données sera soumis aux clauses contractuelles types pour le transfert de Données à caractère personnel vers des pays tiers conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil, telles qu'annexées à la décision d'exécution 2021/914 de la Commission et à toutes les mises à jour y afférentes (« **CCT** »), qui sont intégrées au présent ATD par ce renvoi.

(b) **Modules des CCT**. Le Module deux (Responsable du traitement à Sous-traitant) s'appliquera à un Transfert de données lorsque le Client est Responsable du traitement. Le Module trois (Sous-traitant à Sous-traitant) s'appliquera à un Transfert de données lorsque le Client est Sous-traitant.

(c) **Dispositions facultatives des CCT**. Lorsque les CCT identifient des dispositions facultatives :

(i) Clause 7 (Clause d'adhésion) – la disposition facultative sera réputée incorporée et appliquée ;

(ii) Clause 8.3 – Avant de divulguer une copie des CCT en vertu de la clause 8.3, la partie divulgatrice doit déployer des efforts raisonnables pour supprimer toutes les conditions commerciales, mais fournir un résumé fidèle si la personne concernée n'était pas en mesure de comprendre le contenu ou d'exercer ses droits suite à l'expurgation ;

(iii) Clause 9(a) (Recours à des sous-traitants ultérieurs) – L'option 2 s'applique (et les parties suivront le processus et les délais convenus dans l'ATD pour désigner des sous-traitants ultérieurs) ;

(iv) Clause 11(a) (Voies de recours) – la disposition facultative ne s'applique pas ;

(v) Clause 12 – toute réclamation introduite en vertu des CCT de l'UE sera soumise aux conditions énoncées dans le Contrat. En aucun cas une partie ne doit limiter sa responsabilité à l'égard des droits des Personnes concernées en vertu des CCT de l'UE ;

(vi) Clause 17 (Droit applicable) – l'option 1 s'applique, et lorsque le Contrat est régi par le droit d'un État membre de l'UE, le droit de cet État membre de l'UE s'applique ; sinon, le droit irlandais s'applique ; et

(vii) Clause 18(b) (Élection de for et juridiction) – lorsque le Contrat est soumis à la compétence des tribunaux d'un État membre de l'UE, les tribunaux de cet État membre de l'UE sont compétents ; sinon, les tribunaux de Dublin, en Irlande, sont compétents.

(d) **Annexes des CCT.**

(i) Annexe 1A : le ou les exportateur(s) de données sont le Client et ses Affiliés effectuant le Transfert de données (l'« **Exportateur de données** ») et les importateurs de données sont des entités du Prestataire destinataires du Transfert de données (l'« **Importateur de données** »). Le nom complet, l'adresse et les coordonnées de l'Exportateur de données et de l'Importateur de données sont indiqués dans le Contrat ou peuvent être demandés par l'une ou l'autre des parties.

(ii) Annexe 1B : Les détails pertinents sont ceux énoncés dans le Contrat, y compris l'annexe 1 « Détails du traitement » du présent ATD.

(iii) Annexe 1C : L'autorité de contrôle compétente est l'autorité de contrôle applicable au Client (ou, le cas échéant, applicable au représentant du Client).

(iv) Annexe 2 : les dispositions relatives à la sécurité contenues dans l'Addendum 1 ou d'autres dispositions relatives à la sécurité dans le Contrat s'appliquent.

(e) **Avis.** Tous les avis, demandes, droits de surveillance/d'audit, conduite des réclamations, responsabilité et effacement ou restitution des données relatives aux CCT seront fournis/gérés/interprétés, le cas échéant, conformément aux dispositions pertinentes du Contrat, dans la mesure où ces dispositions ne sont pas en conflit avec les CCT.

9.3 Loi suisse sur la protection des données.

(a) En cas de Transfert de données soumis aux Lois suisses sur la protection des données, les CCT s'appliqueront avec les modifications suivantes :

(i) les références au « RGPD » dans les CCT s'entendent comme des références aux Lois suisses sur la protection des données (« **LPD** ») ;

(ii) les références à un « État membre » et à un « État membre de l'UE » ne seront pas lues pour empêcher les personnes concernées en Suisse de faire valoir leurs droits dans leur lieu de résidence habituelle (Suisse) ; et

(iii) l'autorité de contrôle compétente à l'annexe 1.C en vertu de la clause 13 sera le Préposé fédéral à la protection des données et à la transparence (« **PFPDT** »). Toutefois, lorsque les Données à caractère personnel transférées sont soumises à la fois à la LPD et aux CCT, une surveillance parallèle doit s'appliquer : pour la LPD (révisée), le PFPDT est l'Autorité de contrôle compétente dans la mesure où le transfert est régi par la LPD (révisée) et pour les CCT, l'Autorité de contrôle compétente est (a) l'Autorité de contrôle du pays où l'Exportateur de données est établi si l'Exportateur de données est établi dans l'EEE, ou (b) l'Autorité de contrôle de l'Irlande si l'Exportateur de données n'est pas établi dans l'EEE.

9.4 Loi sur la protection des données du Royaume-Uni.

(a) En cas de Transfert de données soumis aux Lois sur la protection des données du Royaume-Uni, l'Addendum international de transfert de données aux CCT (« **IDTA britannique** »), tel que publié par le Commissaire à l'information (Information Commissioner) au Royaume-Uni, s'appliquera et est incorporé au présent ATD par renvoi. Les informations nécessaires pour remplir les Tableaux destinés à l'IDTA britannique sont énoncées dans le Contrat, y compris l'annexe 1 « Détails du traitement » du présent ATD.

(b) Dans le tableau 2 de l'IDTA britannique, les parties cochent la case suivante : « Les CCT de l'UE approuvés, y compris les informations de l'annexe et avec seulement les modules, clauses ou dispositions facultatives suivants des CCT de l'UE approuvés mis en vigueur aux fins du présent addendum », et le tableau d'accompagnement est réputé être complété selon les préférences des parties décrites dans cet ATD. Aux fins de l'IDTA britannique, le droit applicable est réputé être celui de l'Angleterre et du Pays de Galles.

(c) Dans le tableau 4, les parties conviennent que l'une ou l'autre des parties peut mettre fin à l'Addendum comme indiqué à la clause 19 de l'IDTA britannique.

9.5 Loi sur la protection des données de la République populaire de Chine.

(a) En cas de Transfert de données soumis aux Lois sur la protection des données de la République populaire de Chine, le Client en informera immédiatement le Prestataire et prendra toutes les mesures nécessaires pour minimiser la quantité de Données à caractère personnel partagées avec le Prestataire.

(b) Tout litige découlant des Lois sur la protection des données de la République populaire de Chine sera soumis à la sous-commission de Shanghai de la Commission internationale d'arbitrage économique et commercial de Chine (China International Economic and Trade Arbitration Commission, CIETAC) pour arbitrage, qui sera mené à Shanghai conformément aux règles d'arbitrage du CIETAC en vigueur au moment de l'arbitrage. Toutes les décisions prises par le tribunal arbitral seront définitives et contraignantes pour les parties.

9.6 Loi sur la protection des données en Argentine.

(a) En cas de Transfert de données soumis aux Lois sur la protection des données en Argentine, le Prestataire et le Client conviennent par les présentes des clauses supplémentaires énoncées dans les Annexes au Règlement n° 60- E/2016, disponibles à l'adresse http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm.

(b) Les juridictions considérées comme assurant un niveau adéquat de protection des données en vertu des Lois sur la protection des données en Argentine comprennent les membres de l'Espace économique européen (EEE), la Suisse, Guernesey, Jersey, l'île de Man, les îles Féroé, le Canada (uniquement pour le secteur privé), la Principauté d'Andorre, la Nouvelle-Zélande, la République d'Uruguay, l'État d'Israël (uniquement pour les données soumises à un traitement automatisé) et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord.

9.7 Nonobstant le fait que les CCT ou l'IDTA britannique soient incorporées aux présentes par renvoi sans que les pages de signature des CCT soient effectivement signées par l'exportateur de données ou l'importateur de données, les parties conviennent que leur signature respective du Contrat est réputée constituer leur signature des CCT ou de l'IDTA britannique au nom de l'exportateur de données/l'importateur de données (le cas échéant).

9.8 Si un mécanisme de transfert alternatif, comme les règles d'entreprise contraignantes, est adopté par le Prestataire, ou le Cadre de protection des données transatlantique (un « **Mécanisme alternatif** ») devient disponible pendant la durée du Contrat, et si le Prestataire notifie au Client que tout ou partie des Transferts de données peuvent être effectués conformément aux Lois sur la protection des données dans le cadre du Mécanisme alternatif, les parties s'appuieront sur le Mécanisme alternatif au lieu des dispositions ci-dessus pour les Transferts de données auxquels le Mécanisme alternatif s'applique.

9.9 Le Prestataire peut modifier le présent ATD si le changement reflète un changement de nom ou de forme d'une entité juridique ; ou est nécessaire pour se conformer aux Lois sur la protection des données (y compris les directives émises par une autorité de protection des données dans une Juridiction couverte), ou une ordonnance réglementaire ou judiciaire contraignante.

ANNEXE A

Finalités et détails du traitement des données à caractère personnel

1. Objet. L'objet du traitement des données en vertu du présent ATD est les Données à caractère personnel incluses dans les Données du client.

2. Durée. Entre le Prestataire et le Client, la durée du traitement des données en vertu du présent ATD est la Durée en vertu du Contrat.

3. Finalité et nature. La finalité et la nature du traitement des données en vertu du présent ATD sont la fourniture des Services par le Prestataire en vertu du Contrat et des Bons de commande concernés.

4. Type de données à caractère personnel. Les Données à caractère personnel incluses dans les Données du client qui sont téléchargées par le Client ou les Utilisateurs autorisés vers les Services.

5. Catégories de personnes concernées. Les personnes concernées peuvent inclure les employés, fournisseurs, agents, partenaires ou utilisateurs finaux du Client, comme autorisé dans les Bons de commande.

Mesures de sécurité des données

1. PROGRAMME DE SÉCURITÉ

Lors de la fourniture du ou des Service(s), le Prestataire veillera à ce qu'il existe un programme écrit de sécurité de l'information composé de politiques, procédures et contrôles alignés sur les normes du secteur, régissant le traitement, le stockage, la transmission et la sécurité des Données du client. Le Programme de sécurité comprendra des processus et procédures conformes aux normes du secteur, conçus pour protéger les Données du client contre la destruction accidentelle ou illégale, la perte, l'altération, la divulgation ou l'accès non autorisés. Le Prestataire met à jour le Programme de sécurité pour tenir compte de l'évolution des nouvelles technologies de sécurité, des changements apportés aux pratiques standard du secteur et des menaces de sécurité changeantes, à condition qu'aucune mise à jour ne réduise sensiblement le niveau global d'engagements ou de protections fournis au Client comme décrit dans les présentes.

1.1 ORGANISATION DE SÉCURITÉ. Il y aura un Responsable de la sécurité des systèmes d'information, ou un cadre équivalent, qui sera désigné comme responsable de la coordination, de la gestion et de la surveillance de la fonction, des politiques et des procédures de sécurité de l'information.

1.2 POLITIQUES. Les politiques de sécurité de l'information seront : (i) documentées ; (ii) examinées et approuvées par la direction, y compris après des changements importants ; et (iii) publiées et communiquées au personnel et aux sous-traitants, y compris les conséquences appropriées en cas de non-respect.

1.3 GESTION DES RISQUES. Des évaluations des risques liés à la sécurité de l'information seront effectuées dans le cadre d'un programme de gouvernance des risques qui est établi dans le but de tester et d'évaluer régulièrement l'efficacité du programme de sécurité. Ces évaluations seront conçues pour reconnaître et évaluer l'impact des risques et mettre en œuvre des stratégies de réduction ou d'atténuation des risques identifiés pour tenir compte de l'évolution des nouvelles technologies de sécurité, des changements apportés aux pratiques standard du secteur et des menaces de sécurité changeantes.

2. AUDITS

2.1 AUDIT. Le Prestataire autorisera et contribuera aux audits qui comprennent les inspections en accordant au Client l'accès à une documentation raisonnable et reconnue par le secteur attestant des politiques et des procédures régissant la sécurité et la confidentialité des Données du client et du Programme de sécurité via un portail de documentation en libre accès et sans frais supplémentaires. Les informations disponibles sur le portail comprendront la documentation justificative du Programme de sécurité, y compris les politiques et procédures de confidentialité concernant les Données à caractère personnel traitées. Dans la mesure où le Client n'a pas pu raisonnablement satisfaire à ses exigences d'audit en suivant la procédure décrite dans la présente Clause, le Prestataire fournira au Client l'assistance supplémentaire qui peut raisonnablement être requise (conformément aux obligations d'assistance décrites dans les présentes) pour satisfaire substantiellement à ces exigences.

2.2 RÉSULTAT. À la demande du Client, le Prestataire et le Client peuvent planifier un moment qui conviendra aux deux parties pour s'entretenir de l'Audit. Dans le cas où l'Audit donnerait lieu à des constatations de non-conformité importante vis-à-vis de l'Addendum relatif au traitement des données ou de ces Mesures de sécurité des données (MSD), le Prestataire traitera rapidement ces constatations de non-conformité. Le Prestataire peut, à sa seule discrétion et conformément aux normes et pratiques du secteur et du Prestataire, faire des efforts commercialement raisonnables pour mettre en œuvre les améliorations suggérées par le Client notées dans l'Audit afin d'améliorer le Programme de sécurité du Prestataire. L'Audit et les résultats qui en découlent sont des Informations confidentielles du prestataire.

3. MESURES DE SÉCURITÉ PHYSIQUES, TECHNIQUES ET ORGANISATIONNELLES

3.1 MESURES DE SÉCURITÉ PHYSIQUE.

3.1.1. INSTALLATIONS DU CENTRE DE DONNÉES. Les installations du centre de données prévoiront : (1) des restrictions d'accès physique et la surveillance qui comprendront une combinaison de l'un des éléments suivants : sécurité multizones, pièges, mesures de dissuasion appropriées, gardes sur place, contrôles biométriques, vidéosurveillance et cages sécurisées ; et (2) des systèmes de détection et d'extinction des incendies à la fois localisés et répartis sur l'ensemble des étages du centre de données.

3.1.2. MÉDIAS. Pour la suppression de données, une norme sectorielle telle que NIST 800-88 ou sensiblement équivalente sera utilisée pour la suppression de documents sensibles, y compris les Données du client, avant l'élimination finale de ces médias.

3.2 MESURES DE SÉCURITÉ TECHNIQUES.

3.2.1. ADMINISTRATION DES ACCÈS. L'accès par le personnel aux Données du client sera effectué d'une façon qui : (i) est protégée par des mécanismes d'authentification et d'autorisation ; (ii) exige qu'un compte utilisateur unique soit attribué au personnel ; (iii) restreint le partage de comptes d'utilisateurs individuels ; (iv) nécessite une authentification forte avec des mots de passe complexes ; (v) s'assure que les comptes sont verrouillés ; (vi) nécessite un accès via un VPN ; (vii) exige que les privilèges d'accès soient basés sur des exigences professionnelles limitées à celles nécessaires aux membres du personnel concernés pour s'acquitter de leurs fonctions ; (viii) fait en sorte que l'accès est révoqué à la fin de l'emploi ou des relations de conseil ; et (ix) exige que les droits d'accès soient examinés par la direction tous les trimestres.

3.2.2. ENREGISTREMENT ET SURVEILLANCE. Les activités du journal de l'infrastructure de production seront recueillies de manière centralisée, sécurisées pour éviter toute altération et surveillées pour détecter les anomalies par une équipe de sécurité formée.

3.2.3. SYSTÈME DE PARE-FEU. La technologie de pare-feu sera installée et gérée pour protéger les systèmes et inspecter les connexions d'entrée. Les règles de pare-feu géré seront examinées conformément aux procédures opérationnelles alors en vigueur, qui seront revues au moins une fois par trimestre.

3.2.4. GESTION DES VULNÉRABILITÉS. Des analyses de vulnérabilité seront effectuées dans l'environnement pour déterminer les vulnérabilités potentielles conformément aux procédures opérationnelles de sécurité alors en vigueur, qui seront au moins trimestrielles. Lorsque des vulnérabilités logicielles sont révélées et traitées par un correctif du fournisseur, le correctif sera obtenu auprès du fournisseur concerné et appliqué dans un délai approprié en tenant compte des risques conformément à la procédure opérationnelle standard de gestion des vulnérabilités et des correctifs de sécurité alors en vigueur et uniquement après que ce correctif a été testé et jugé sûr pour l'installation dans les systèmes de production.

3.2.5. ANTIVIRUS. Les logiciels antivirus, anti-logiciels malveillants et anti-logiciels espions seront mis à jour à intervalles réguliers et enregistrés de manière centralisée.

3.2.6. CONTRÔLE DES MODIFICATIONS. Les modifications apportées à l'environnement seront examinées afin de minimiser les risques. Ces modifications seront mises en œuvre conformément à la procédure opérationnelle standard en vigueur.

3.2.7. GESTION DES CONFIGURATIONS. Les configurations standard renforcées pour les composants du système au sein de l'environnement seront maintenues à l'aide de guides de renforcement standard du secteur, tels que les guides du Center for Internet Security.

3.2.8. CHIFFREMENT DES DONNÉES EN TRANSIT. Le chiffrement standard du secteur sera utilisé pour chiffrer les Données du client en transit sur les réseaux publics.

3.2.9. CHIFFREMENT DES DONNÉES AU REPOS. Le chiffrement des Données du client au repos sera déterminé par le Client et, en cas de chiffrement, celui-ci sera tel que déterminé par le Client conformément aux offres applicables.

3.2.10. CODE ILLICITE ET DÉVELOPPEMENT LOGICIEL SÉCURISÉ. Le Prestataire suivra les pratiques de développement de logiciels sécurisés et d'examen du code décrites dans la présente clause afin de prévenir les dommages causés par les logiciels malveillants, tels que les virus, les vers, les bombes de date, les bombes à retardement ou les dispositifs d'arrêt. Le logiciel sera développé à l'aide de politiques et de procédures de développement d'applications sécurisées alignées sur les pratiques standard du secteur telles que le Top Ten de l'OWASP ou une norme substantiellement équivalente. Le personnel responsable de la conception et du développement sécurisés des applications recevra une formation appropriée concernant les pratiques de développement sécurisé des applications.

3.2.11. EXAMEN DU CODE SÉCURISÉ. Une combinaison de tests statiques et dynamiques du code sera effectuée avant la publication de ce code à l'intention des Clients. Les vulnérabilités seront traitées conformément au programme de gestion des vulnérabilités

logicielles alors en vigueur. Pour remédier aux vulnérabilités où le code a été mis à la disposition des Clients, des correctifs logiciels seront régulièrement mis à la disposition des Clients.

3.3 MESURES DE SÉCURITÉ ORGANISATIONNELLES.

3.3.1. SÉCURITÉ DU PERSONNEL. Une vérification des antécédents sera effectuée sur tous les employés et sous-traitants qui ont accès aux Données du client conformément à la procédure opérationnelle standard applicable et sous réserve du Droit applicable.

3.3.2. SENSIBILISATION ET FORMATION À LA SÉCURITÉ. Une formation de sensibilisation à la sécurité et à la confidentialité sera dispensée aux employés et sous-traitants qui ont accès aux Données du client. Cette formation sera dispensée au moment de l'embauche et au moins une fois par an tout au long de la relation d'emploi.

3.3.3. GESTION DES RISQUES FOURNISSEURS. Tout fournisseur qui accède, stocke, traite ou transmet des Données du client sera évalué pour s'assurer qu'il dispose de contrôles de sécurité et de confidentialité appropriés.

3.3.4. INVENTAIRE DES LOGICIELS ET DES ACTIFS. Un inventaire des composants logiciels, y compris, mais sans s'y limiter, les logiciels open source utilisés dans l'environnement, sera tenu.

3.3.5. SÉCURITÉ DES POSTES DE TRAVAIL. Des mécanismes de sécurité sur les postes de travail du personnel, y compris des pare-feu, un antivirus et un cryptage complet du disque avec un cryptage AES 256 bits minimum seront mis en œuvre et maintenus. Le personnel ne pourra pas désactiver les mécanismes de sécurité.

4. CONTINUITÉ DU SERVICE

4.1 EMPLACEMENT DES DONNÉES. Le Prestataire hébergera les instances souscrites dans des centres de données situés dans la région géographique par défaut indiquée sur l'ATD ou autrement indiquée dans l'accord contractuel, qui ont obtenu des attestations SOC2 Type 2, des certifications ISO 27001, ou des attestations/certifications équivalentes ou ultérieures.

4.2 SAUVEGARDE DES DONNÉES. Des sauvegardes de toutes les Données du client seront effectuées conformément au mode opératoire en vigueur publié sur le portail.

4.3 REPRISE APRÈS SINISTRE. Un Plan de continuité des activités/Récupération après sinistre (CA/RAS) pour traiter la reprise après sinistre sera maintenu, conformément aux normes du secteur pour l'environnement et : (i) inclura les processus de protection du personnel et des actifs (ii) testera le CA/RAS au moins une fois par an ; (iii) mettra à disposition des résultats de test récapitulatifs qui incluront le point de reprise réel et les temps de reprise ; et (iv) documentera tous les plans d'action dans les résultats sommaires des tests pour remédier rapidement à toute déficience et préoccupations, ou aux problèmes qui ont empêché ou peuvent empêcher la récupération de l'environnement conformément au CA/RAS et les résoudre.

5. SURVEILLANCE ET GESTION DES INCIDENTS

5.1 SURVEILLANCE ET GESTION DES INCIDENTS. Les événements du système sont surveillés et analysés en temps opportun conformément aux procédures opérationnelles standard actuelles du Prestataire. Les équipes d'intervention en cas d'incident seront prévenues et sollicitées si nécessaire pour traiter un incident de sécurité.

5.2 NOTIFICATION DE VIOLATION.

5.2.1. NOTIFICATION. Le Prestataire signalera au Client toute destruction, perte, altération, divulgation non autorisée, ou accès non autorisé aux Données du client sans retard injustifié après avoir déterminé qu'une Violation s'est produite.

5.2.2. SIGNALEMENT. Le signalement initial sera fait au contact de sécurité, de confidentialité ou technique principal désigné par le Client. Au fur et à mesure que les informations pertinentes relatives à la Violation sont collectées ou deviennent autrement disponibles pour le Prestataire, il fournira ces informations sans retard injustifié au Client, afin d'aider le Client à se conformer à ses obligations de notification en vertu des Lois sur la protection des données. Dans la mesure raisonnablement possible et applicable, le Prestataire fournira au Client les informations décrites à l'article 33 du RGPD.

5.2.3. OBLIGATIONS DU RESPONSABLE DU TRAITEMENT. Le Client coopérera avec le Prestataire pour maintenir des coordonnées exactes sur le portail d'assistance à la clientèle et en fournissant toutes les informations raisonnablement demandées pour résoudre les incidents de sécurité, y compris les Violations, identifiera sa ou ses cause(s) profondes et empêchera qu'elles ne se reproduisent. Le Client est seul responsable de déterminer s'il doit informer les autorités de contrôle ou de réglementation compétentes et les Personnes concernées affectées en cas de Violation et de fournir un tel avis.

6. TESTS DE PÉNÉTRATION

6.1 PAR UN TIERS. Le Prestataire engagera des fournisseurs tiers qualifiés pour effectuer une pénétration sur l'application et la plateforme du Prestataire afin d'identifier les vulnérabilités. Les rapports exécutifs des tests de pénétration sont mis à la disposition des Clients sur le portail.

6.2 PAR LE CLIENT. Le Client peut demander à effectuer, à ses propres frais, un test de pénétration Web sur les environnements d'hébergement dans lesquels les Données du client sont stockées, à condition que le Client : (i) informe le Prestataire et soumette une demande de planification d'un tel test à l'aide du Portail d'assistance. Dans le cas où les tests de pénétration autorisés du Client identifient des vulnérabilités que le Prestataire est en mesure de reproduire, le Prestataire déploiera, conformément aux pratiques standard du secteur, des efforts raisonnables pour apporter rapidement les modifications nécessaires afin d'améliorer la sécurité du Service.

7. RESPONSABILITÉ PARTAGÉE EN MATIÈRE DE SÉCURITÉ

7.1 CAPACITÉS DU PRODUIT. Le Prestataire fournit une variété de paramètres de sécurité qui permettent au Client de configurer la sécurité des Services pour son propre usage, notamment : (i) authentifier les utilisateurs avant d'accéder à l'instance du Client ; (ii) crypter les mots de passe ; (iii) permettre aux utilisateurs de gérer les mots de passe ; et (iv) accéder aux journaux d'application des instances. Le Client gérera l'accès et l'utilisation des Services par chaque utilisateur en attribuant à chaque utilisateur un identifiant et un type d'utilisateur qui contrôlent le niveau d'accès aux Services applicables. Le Client assume l'entière responsabilité de l'examen du Programme de sécurité et de la prise d'une décision indépendante quant à savoir s'il répond aux exigences du Client, en tenant compte du type et de la sensibilité des Données du client que le Client fournit au Prestataire. Le Client assume l'entière responsabilité de la protection de la confidentialité des identifiants et mots de passe de chaque utilisateur et de la gestion des accès de chaque utilisateur aux Services.

7.2 CONTACT DE SÉCURITÉ. Le Client accepte d'identifier et de maintenir un ou des contact(s) de sécurité appropriés pour tous les incidents de sécurité de l'information et les communications liées à la sécurité de l'information dans le Portail d'assistance.

7.3 LIMITATIONS. Nonobstant toute disposition contraire dans les présentes MSD ou d'autres parties du Contrat, les obligations du Prestataire aux présentes ne s'appliquent qu'aux Services. Les présentes MSD ne s'appliquent pas : (i) aux informations partagées avec le Prestataire qui ne sont pas des Données du client ; (ii) aux données contenues dans le VPN du Client ou un réseau tiers ; et (iii) à toutes les données traitées par le Client ou ses utilisateurs en violation du Contrat ou des présentes MSD.

ANNEXE B

Sous-traitant/Pays	Services
Amazon Web Services, Inc. (« AWS ») États-Unis d'Amérique, Australie, Canada, Irlande (UE), Singapour et Royaume-Uni	Service d'hébergement cloud
Microsoft Corporation États-Unis d'Amérique Irlande, Canada et Australie	Service d'hébergement cloud
Microsoft Corporation, États-Unis d'Amérique	Intégration du calendrier Outlook
Nournet Company, Arabie Saoudite	Service d'hébergement cloud en Arabie saoudite
Affiliés du prestataire • Ungerboeck Systems International, LLC, États-Unis d'Amérique et Nouvelle-Zélande • Ungerboeck Software International, Pty Ltd., Australie et Nouvelle-Zélande • Oletha Pyt Ltd, Inde • Ungerboeck Systems International GmbH, Royaume-Uni	Assistance client liée à l'exécution du contrat et aux services
AC PM, LLC, États-Unis d'Amérique	Prestataire de services de messagerie (Postmark)

Atlassian US, Inc. États-Unis d'Amérique	Plateforme logicielle de collaboration
Caffeinated Corporation, États-Unis d'Amérique	Assistance client automatisée assistée par l'IA pour rationaliser et automatiser l'assistance
Datadog, Inc. États-Unis d'Amérique	Surveillance des performances du réseau et de l'infrastructure

DELIGHTED, LLC, États-Unis d'Amérique	Outil de gestion des commentaires des clients
DocuSign Inc., États-Unis d'Amérique	Intégration de la signature électronique et provisionnement de l'enveloppe
Dynatrace, LLC, États-Unis d'Amérique	Plateforme de surveillance et de journalisation tierce
Flowgear LLC, États-Unis d'Amérique	Plateforme d'intégration en tant que service
Google, États-Unis d'Amérique	Intégration SSO SAML 2.0, cartes et calendrier
Jotform, Inc., États-Unis d'Amérique	Intégration des formulaires en ligne
Okta, Inc., États-Unis d'Amérique	Fournisseur d'identité
Pendo.io, Inc., États-Unis d'Amérique	Outil d'analyse utilisateur
Productboard, Inc., États-Unis d'Amérique	Logiciel de suivi des produits
Signiant Inc., États-Unis d'Amérique	Intégration du service Media Shuttle pour le transfert de données
Stripe, Inc., États-Unis d'Amérique	Organisme de traitement des paiements
Twilio Inc., États-Unis d'Amérique	Intégration de la solution de messagerie SendGrid
Validity, Inc. États-Unis d'Amérique	Plateforme d'intégrité des données
Wiz Inc., États-Unis d'Amérique	Plateforme de sécurité cloud
Zendesk, Inc. États-Unis d'Amérique	Centre d'assistance et base de connaissances ; Système d'émission de tickets pour l'assistance client
Full Story, Inc. États-Unis d'Amérique	Outil d'analyse des utilisateurs
CheifSight Corporation États-Unis d'Amérique	Outil d'analyse commerciale
Fivetran, Inc. États-Unis d'Amérique	Plateforme de transfert de données automatisée.
Snowflake, Inc. États-Unis d'Amérique	Plateforme d'entrepôt de données basée sur le cloud