ACCORD DE TRAITEMENT DES DONNÉES

Le présent Accord de traitement des données ("ATD") est l'accord des parties en ce qui concerne le traitement des données à caractère personnel et complète tous les accords de licence, d'abonnement, de services ou autres accords écrits ou électroniques (les "**Accords**") entre Trimble et Client pour l'achat de services (y compris des logiciels en tant que Service, leurs applications hors ligne ou mobiles Trimble associées, et l'assistance, et définis comme "Services" ou autrement dans l'Accord ou ci-après) au cours desquels Trimble reçoit des données à caractère personnel de la part de Client.

Client conclut le présent ATD (i) en signant ou en acceptant autrement l'Accord, (ii) en le signant en son nom propre et comme requis par les Lois et règlements applicables sur la protection des données, au nom et pour le compte des affiliés autorisés, si et dans la mesure où Trimble traite les données à caractère personnel. Aux fins du présent ATD uniquement, et sauf indication contraire, le terme "Client" comprend Client et les affiliés autorisés.

Dans le cadre de la fourniture des Services à Client conformément à l'Accord, Trimble peut traiter les données à caractère personnel au nom de Client et les parties conviennent de se conformer aux dispositions suivantes en ce qui concerne toutes les données à caractère personnel.

COMMENT EXÉCUTER LE PRÉSENT ATD :

I. Le présent ATD se compose du corps principal de l'ATD et des Annexes 1 à 3
II. Il a été pré-signé au nom de Trimble. Les Clauses contractuelles types (telles que définies ci-dessous) sont incorporées par référence.
III. Si Client souhaite compléter le présent ATD, Client doit :
    a. Compléter les informations dans le champ de signature et signer à la page 6.
    b. Compléter les informations en tant qu'exportateur de données à la page 6.
IV. Envoyer l'ATD complété et signé à Trimble par courriel, en indiquant le numéro de compte client de son organisation (tel que configuré sur la facture Trimble applicable), à l'adresse privacy@trimble.com.

COMMENT LE PRÉSENT ATD S'APPLIQUE :

- Si l'entité Client qui accepte le présent ATD est partie à un Accord, le présent ATD est un addendum à cet Accord et en fait partie, et l'entité Trimble qui est partie à l'Accord est partie au présent ATD.
- Si l'entité Client signant le présent ATD a soumis une commande qui a été acceptée par Trimble ou l'un de ses affiliés, mais n'est pas elle-même partie à l'Accord, le présent ATD est un addendum à cette commande (y compris toute commande de renouvellement) et l'entité Trimble sur laquelle cette commande a été placée est partie au présent ATD.
- Si l'entité Client qui signe l'ATD a acheté des services Trimble par l'intermédiaire d'un revendeur autorisé de Trimble, Client doit l'indiquer à la page 6 et fournir un numéro de client émis par Trimble ou par le revendeur, ou, à défaut, une confirmation du revendeur que Client est abonné à un service Trimble. Dans ce cas, le présent ATD sera considéré comme un accord direct entre Client et Trimble.
- Si l'entité ou la personne qui signe le présent ATD n'est pas partie à une commande ou à un Accord et n'est pas un client indirect par l'intermédiaire d'un revendeur, le présent ATD n'est pas valide et n'est pas juridiquement contraignant. Cette entité doit demander à son entité affiliée qui est partie à l'Accord de signer le présent ATD ou de demander par écrit à faire partie de l'Accord.

Le présent ATD ne remplace pas les droits comparables ou supplémentaires relatifs au traitement des données de Client contenus dans l'Accord (y compris tout addendum à l'Accord existant relatif au traitement des données).

LES TERMES DU TRAITEMENT DES DONNÉES

1. DÉFINITIONS

"**Société affiliée**" désigne toute entité qui contrôle directement ou indirectement l'entité concernée, qui est contrôlée par elle ou qui est sous contrôle commun avec elle. Aux fins de la présente définition, on entend par "contrôle" la propriété ou le contrôle direct ou indirect de plus de 50 % des droits de vote en circulation de l'entité concernée.

"**Affilié autorisé**" désigne tout affilié de Client qui (i) est soumis à une ou plusieurs Lois sur la protection des données et (ii) est autorisé à utiliser les Services conformément à l'Accord entre Client et Trimble, mais n'a pas signé sa propre commande avec Trimble et n'est pas un "Client" tel que défini dans l'Accord.

"**CCPA**" désigne la Loi californienne sur la protection de la vie privée des consommateurs, Cal. Civ. Code § 1798.100 et seq., et ses règlements
d'application.

"**Responsable du traitement**" désigne l'entité qui détermine les objectifs et les moyens du traitement des données à caractère personnel.

"Client" désigne l'entité qui a signé l'Accord, ainsi que ses sociétés affiliées (pour autant qu'elles restent des sociétés affiliées) qui ont signé des bons de commande.

"**Données du client**" signifie ce qui est défini dans l'Accord comme "Données du client" ou "Vos données."

"**Lois et règlements sur la protection des données**" désignent toutes les lois et règlements, y compris les lois et règlements de l'Union européenne, de l'Espace économique européen et de leurs États membres, de la Suisse et du Royaume-Uni, les pays énumérés à l'annexe 3 et tous les autres pays dans lesquels le client ou une société affiliée au client a un siège, tous comme applicables au traitement des données à caractère personnel en vertu de l'Accord.

"**Personne concernée**" désigne la personne à laquelle se rapportent les données à caractère personnel.

"Europe**" désigne l'Union européenne (UE), l'Espace économique européen (EEE) et la Suisse.**

"**RGPD**" désigne le Règlement (UE) 2016/679 du Parlement européen et du Conseil.

"**Données à caractère personnel**" signifie toute information concernant (i) une personne identifiée ou identifiable et (ii) une entité juridique identifiée ou identifiable (lorsque ces informations sont protégées de la même manière que les données à caractère personnel ou les informations personnellement identifiables en vertu des lois et règlements applicables en matière de protection des données), pour autant que ces données soient des données de Client.

"**Traitement**" désigne toute opération ou ensemble d'opérations effectuées sur les données à caractère personnel, à l'aide ou non de procédés automatisés, telles que la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou la combinaison, la restriction, le blocage, l'effacement ou la destruction.

«**Sous-traitant**» désigne l'entité qui traite les données à caractère personnel sur instruction et pour le compte du Responsable du traitement, y compris, le cas échéant, tout «fournisseur de service» tel que ce terme est défini par la CCPA.

"Autorité publique" désigne une agence gouvernementale ou une autorité chargée de l'application de la loi, y compris les autorités judiciaires.

" **Clauses contractuelles types de l'UE**" désigne un accord exécuté par et entre (i) une société affiliée de Trimble et Trimble Inc. ou (ii) Client et Trimble Inc. conformément à la décision d'application (UE) 2021/914.

"Sous-traitant ultérieur**" désigne tout sous-traitant engagé par Trimble ou un membre du Trimble Group.**

"**Trimble**" désigne l'entité Trimble qui est partie à du présent ATD, comme spécifié dans la section "COMMENT LE PRÉSENT ATD S'APPLIQUE" ci-dessus. Les entités Trimble agissant en tant que Sous-traitants sont : Trimble Inc, une société constituée dans le Delaware, Trimble Europe B.V., une société enregistrée aux Pays-Bas, Trimble International B.V., une société constituée aux Pays-Bas, Trimble International B.V., une société enregistrée aux Pays-Bas, Trimble UK Ltd, une société constituée en Angleterre et au Pays de Galles, Trimble Maps, Ltd, une société constituée en Angleterre et au Pays de Galles, Trimble Technologies Ireland Ltd, une société constituée en Irlande, Trimble France SAS, une société constituée en France, Trimble Solutions Sandvika AS, une société constituée en Norvège, Trimble Finland Corporation, une société constituée en Finlande, Trimble Forestry Europe Corporation, une société constituée en Finlande, Lakefield eTechnologies Ltd, une société constituée en Irlande, Trimble GmbH, une société constituée en Allemagne, ou Trimble Germany GmbH, une société constituée en Allemagne, selon le cas.

"**Trimble Group**" désigne Trimble et ses sociétés affiliées engagés dans le traitement des données à caractère personnel.

2. TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

2.1 Rôles des parties. Les parties reconnaissent et conviennent qu'en ce qui concerne le traitement des données à caractère personnel, Client est le responsable du traitement, Trimble est un sous-traitant et que Trimble ou les membres du Trimble Group engageront des sous-traitants ultérieurs conformément aux exigences énoncées dans la section 5 ci-dessous, à condition que pour le traitement des données du compte de Client, Trimble soit le responsable du traitement.

2.2 Traitement des données à caractère personnel par Client. Dans le cadre de son utilisation des Services, Client traitera les données à caractère personnel conformément aux exigences des Lois et règlements sur la protection des données. Pour éviter toute ambiguïté, les instructions de Client concernant le traitement des données à caractères personnel doivent être conformes aux Lois et règlements sur la protection des données. Client est seul responsable de l'exactitude, de la qualité et de la légalité des données à caractère personnel et des moyens par lesquels Client a acquis les données à caractère personnel. Trimble informera immédiatement Client si, à son avis, une instruction enfreint les Lois et règlements sur la protection des données ou d'autres dispositions légales.

2.3 Traitement des données à caractère personnel par Trimble. Trimble ne traitera les données à caractère personnel que pour le compte et conformément aux instructions de Client, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale. Client donne instruction à Trimble de traiter les données à caractère personnel aux fins suivantes : (i) Traitement conformément à l'Accord et aux ordonnances applicables ; (ii) Traitement initié par les utilisateurs dans leur utilisation des Services ; (iii) Traitement pour se conformer à d'autres instructions raisonnables fournies par Client lorsque ces instructions sont compatibles avec les conditions de l'Accord ; et (iv) Traitement à des fins d'anonymisation en conformité avec les Clauses d'utilisation des données dans l'Accord (et inclus dans dans l'Annexe 1).

TRIMBLE N'AGIT PAS EN TANT QUE SOUS-TRAITANT POUR LES DONNÉES À CARACTÈRE PERSONNEL SUIVANTES : Les données de connexion et de contact de l'utilisateur, les données d'utilisation du logiciel et les données générées par les mesures de sécurité (“**Données du compte client**)”.

2.4 Champ d'application et objectif ; Catégories de données à caractère personnel et personne concernée. L'objet du traitement des données à caractère personnel par Trimble est l'exécution des Services conformément à l'Accord. Les types de données à caractère personnel et les catégories de personnes concernées dans le cadre du présent ATD sont spécifiés dans l'Annexe 1 (Détails du traitement/transfert) du présent ATD.

3. DROITS DES PERSONNES CONCERNÉES

3.1 Droits des personnes concernées. En tenant compte de la nature du traitement, Trimble aide Client en fournissant des mesures techniques et organisationnelles appropriées, dans la mesure où cela est possible, pour l'accomplissement de l'obligation de Client de répondre aux demandes des Personnes concernées pour l'exercice de leurs droits de personnes concernées conformément aux Lois et règlements sur la protection des données. Dans la mesure où Client, dans son utilisation des Services, n'a pas la capacité d'exercer ces droits lui-même, Trimble se conformera à toute demande commercialement raisonnable de Client pour faciliter de telles actions dans la mesure où Trimble est légalement autorisée à le faire. Dans la mesure où cela est légalement autorisé, Client sera responsable de tous les coûts découlant de la fourniture d'une telle assistance par Trimble.

3.2 Demandes directes de la personne concernée. Trimble doit, dans la mesure où cela est légalement autorisé, notifier rapidement Client si elle reçoit une demande d'une personne concernée pour exercer ses droits de personne concernée conformément à la section 3.1. Trimble ne répondra pas à une telle demande d'une personne concernée sans le consentement préalable de Client sous forme de texte, sauf pour confirmer que la demande concerne Client, à laquelle Client consent par la présente.

4. PERSONNEL DE TRIMBLE ET DU CLIENT

4.1 Généralités. Trimble et Client prendront des mesures pour s'assurer que toute personne physique agissant sous leur autorité respective qui a accès aux données du client ne traite pas les données de Client sauf sur instructions de Client, à moins qu'elle ne soit tenue de le faire par les Lois et règlements sur la protection des données.

4.2 Confidentialité. Trimble s'assurera que son personnel engagé dans le traitement des données à caractère personnel est informé de la nature confidentielle des données à caractère personnel, a reçu une formation appropriée sur ses responsabilités et a signé des engagements de confidentialité écrits. Trimble s'assurera que ces obligations de confidentialité survivent à la fin de l'engagement du personnel.

4.3 Fiabilité. Trimble prendra des mesures commercialement raisonnables pour assurer la fiabilité de tout personnel de Trimble engagé dans le traitement des données à caractère personnel.

4.4 Limitation de l'accès. Trimble s'assurera que l'accès du personnel aux données à caractère personnel est limité au personnel exécutant les services conformément à l'Accord.

5. SOUS-TRAITANTS ULTÉRIEURS

5.1 Nomination de Sous-traitants ultérieurs. Client reconnaît et accepte que (i) les affiliés de Trimble peuvent être retenus comme sous-traitants ultérieurs ; et (ii) Trimble et les affiliés de Trimble respectivement peuvent engager des sous-traitants ultérieurs tiers dans le cadre de la fourniture des Services. Dans ce cas, Trimble et l'affilié de Trimble doivent imposer à tout sous-traitant ultérieur des obligations de protection des données matériellement similaires à celles énoncées dans le présent ATD par le biais d'un contrat ou d'un autre acte juridique. Le contrat ou autre acte juridique doit contenir des garanties suffisantes pour que tout sous-traitant ultérieur mette en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le Traitement réponde aux exigences des Lois et règlements sur la protection des données.

5.2 Liste des Sous-traitants ultérieurs actuels et notification des nouveaux Sous-traitants ultérieurs. La liste actuelle des Sous-traitants ultérieurs engagés dans le 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 résidence est énumérée à l'adresse https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center sous “Additional Resources” (Ressources supplémentaires) (“Sub-processor Lists” (Listes de sous-traitants ultérieurs)). Client consent par la présente à ces Sous-traitants ultérieurs, à leurs pays de résidence et à leurs activités de traitement en ce qui concerne leurs données à caractère personnel, et donne des instructions à Trimble en conséquence. Trimble informera des changements de sous-traitants ultérieurs dans ses notes de version, ses mises à jour clients ou des communications similaires qui seront considérées comme un avis aux fins de la [Section 9.2 des Clauses contractuelles types de l'UE].

5.3 Droit d'objection pour les nouveaux Sous-traitants ultérieurs. Afin d'exercer son droit de s'opposer à l'utilisation par Trimble d'un nouveau Sous-traitant ultérieur, Client doit notifier Trimble rapidement sous forme de texte envoyé à privacy@trimble.com dans les trente (30) jours ouvrables après réception de l'avis de Trimble conformément au mécanisme qui figure dans la Section 5.2. Dans le cas où Client s'oppose à un nouveau Sous-traitant ultérieur, et que cette objection n'est pas déraisonnable, Trimble fera des efforts raisonnables pour mettre à la disposition de Client un changement dans les Services ou recommander un changement commercialement raisonnable à la configuration ou à l'utilisation des Services par Client pour éviter le traitement des données à caractère personnel par le nouveau Sous-traitant ultérieur objecté sans imposer une charge déraisonnable au Client. Si Trimble n'est pas en mesure de rendre disponible un tel changement dans un délai raisonnable, qui ne doit pas dépasser soixante (60) jours, Client peut résilier la (les) commande(s) applicable(s) et les Accords en ce qui concerne uniquement les Services qui ne peuvent pas être fournis par Trimble sans l'utilisation du nouveau Sous-traitant ultérieur objecté en fournissant un avis écrit à Trimble. Trimble remboursera à Client tous les frais prépayés couvrant le reste de la durée de cette (ces) commande(s) après la date effective de résiliation en ce qui concerne ces Services résiliés.

5.4 Responsabilité. Trimble sera responsable des actes et omissions de ses sous-traitants ultérieurs dans la même mesure que Trimble serait responsable si elle exécutait les services de chaque sous-traitant directement selon les termes du présent ATD, sauf disposition contraire de l'Accord.

6. SÉCURITÉ, AUDITS ET ASSISTANCE

6.1 Sécurité du traitement. Trimble maintiendra des mesures de protection administratives, physiques et techniques pour la protection de la sécurité, de la confidentialité et de l'intégrité des données des clients, y compris les données à caractère personnel, comme décrites dans l'Annexe 1. Trimble contrôle régulièrement la conformité avec ces mesures de protection. Trimble ne réduira pas matériellement la sécurité globale des Services pendant la durée de l'Accord.

6.2 Audits. Trimble effectue de temps en temps des audits et des inspections (y compris, lorsque cela est raisonnable, des audits par des auditeurs externes) pour assurer la conformité avec les lois sur la protection des données et le présent ATD ainsi que, lorsque cela est raisonnable, avec les normes industrielles telles que ISO 27001. Trimble mettra à la disposition du client, sur demande, toutes les informations nécessaires (y compris de tels rapports d'audit) pour démontrer la conformité avec son obligation en vertu de la Loi sur la protection des données applicable et du présent ATD. En fonction des informations demandées, Trimble peut exiger du client qu'il signe un AND.

6.3 Assistance à Client. Trimble assistera Client en assurant la conformité avec les obligations concernant la sécurité du traitement, la notification et la communication des violations des données à caractère personnel, les évaluations de l'impact de la protection des données et les consultations préalables avec l'autorité de contrôle conformément aux Lois et règlements sur la protection des données.

6.4 Gestion et notification de la violation de la sécurité. En cas de violation des données à caractère personnel conformément aux Lois et règlements sur la protection des données, Trimble maintient des politiques et des procédures de gestion des incidents de sécurité et doit, dans la mesure autorisée par la loi, notifier à Client une telle violation dans un délai raisonnable.

7. RESTITUTION ET SUPPRESSION DES DONNÉES DE CLIENT

Trimble, après la fin de la fourniture des Services, au choix de Client, retournera les données de Client à Client et/ou supprimera les données de Client conformément aux procédures et aux délais spécifiés dans l'Accord ou dans sa description de Service, à moins que la législation imposée à Client n'exige le stockage des données de Client.

8. DEMANDES D'ACCÈS DU GOUVERNEMENT

8.1 Sauf si la loi applicable l'interdit, Trimble informera Client en termes généraux des demandes, ordonnances ou demandes similaires par un tribunal, une autorité compétente, un organisme d'application de la loi ou un autre organisme gouvernemental ("Demande d'application de la loi") concernant le traitement des données à caractère personnel en vertu de ces Clauses.

8.2 Trimble s'opposera et contestera toute Demande d'application de la loi en prenant des mesures légales dans la mesure où elles sont raisonnables compte tenu des circonstances. Si Trimble est contraint de divulguer des données à caractère personnel transférées en vertu de ces Clauses par une Demande d'application de la loi, Trimble, à moins que la loi applicable ne l'interdise, donnera Client un préavis raisonnable pour permettre Client de demander une ordonnance de protection ou un autre recours approprié, à moins que Trimble ne soit légalement empêché de le faire.

8.3 Dans le cas où Trimble met des données à caractère personnel à la disposition de sous-traitants ultérieurs, Trimble sélectionnera des sous-traitants ultérieurs dans un pays en dehors de l'Espace économique européen qui ne fait pas l'objet d'une décision d'adéquation par la Commission de l'Union européenne, uniquement après une diligence raisonnable qui implique (i) un examen de tous les rapports de transparence mis à disposition par le sous-traitant ultérieur, (ii) et la réalisation d'une évaluation du risque de transfert.

9. AFFILIÉS AUTORISÉS

9.1 **Relation contractuelle**. Le Client conclut l'ATD en son nom propre et,le cas échéant, au nom et pour le compte des affiliés autorisés, établissant ainsi un ATD séparé entre Trimble et chacun de ces affiliés autorisés. Chaque affilié autorisé est lié par les obligations du présent ATD. Pour éviter tout doute, un affilié autorisé n'est pas et ne devient pas une partie à l'Accord, mais est seulement une partie à l'ATD. Tout accès aux Services et toute utilisation de ceux-ci par les affiliés autorisés doivent être conformes aux conditions générales de l'Accord et toute violation des conditions générales de l'Accord par un affilié autorisé sera considérée comme une violation de la part de Client.

9.2 **Communication**. Le Client qui est la partie contractante de l'Accord restera responsable de la coordination de toute communication avec Trimble dans le cadre du présent ATD et sera autorisé à faire et à recevoir toute communication en rapport avec le présent ATD au nom de ses affiliés autorisés.

9.3 **Droits des affiliés autorisés**. Lorsqu'un affilié autorisé devient partie à l'ATD avec Trimble, il doit, dans la mesure requise par les Lois et règlements applicables en matière de protection des données, être autorisé à exercer les droits et à demander des réparations dans le cadre du présent ATD. Si les Lois et règlements sur la protection des données exigent que l'affilié autorisé exerce un droit ou cherche un recours en vertu du présent ATD en tant que Responsable du traitement, l' affilié autorisé autorise par la présente le Client à exercer un tel droit à la place de l'affilié autorisé. En outre, le Client qui est la partie contractante à l'Accord doit exercer ces droits en vertu du présent ATD non pas séparément pour chaque affilié autorisé, mais de manière combinée pour l'ensemble de ses affiliés autorisés.

10. Limite de responsabilité

La responsabilité de chaque partie et de ses affiliés découlant de ou liée au présent ATD et à tous les ATD entre les affiliés autorisés et Trimble, que ce soit dans le cadre d'un contrat, d'un délit ou de toute autre théorie de responsabilité, est soumise à la section "Limitation de responsabilité" de l'Accord, et toute référence dans cette section à la responsabilité d'une partie signifie la responsabilité globale de cette partie et de ses affiliés dans le cadre de l'Accord et de tous les ATD ensemble. Pour éviter toute ambiguïté, la responsabilité totale de Trimble et de ses affiliés pour toutes les réclamations de Client et de ses affiliés autorisés découlant de ou liées à l'Accord et à chaque ATD s'appliquera dans l'ensemble pour toutes les réclamations en vertu de l'Accord et de tous les ATD établis en vertu de cet Accord, y compris par tout affilié autorisé, et, en particulier, ne sera pas comprise comme s'appliquant individuellement et solidairement à chaque affilié autorisé qui est une partie contractuelle à tout ATD de ce type. Pour éviter toute autre ambiguïté, toute référence à l'ATD dans le présent ATD signifie le présent ATD, y compris ses annexes et ses appendices.

Si Client a souscrit ou acheté les Services par l'intermédiaire d'un revendeur ou d'un autre partenaire commercial de Trimble, la responsabilité de Trimble et de ses affiliés découlant de ou liée au présent ATD et à tous les ATD entre les affiliés autorisés et Trimble, que ce soit dans le cadre d'un contrat, d'un délit ou de toute autre théorie de

responsabilité, sera limitée, dans la mesure où cela est légalement permis, au plus élevé des montants reçus par Trimble pour ces Services ou à 50 000 euros.

11. DISPOSITIONS INTERNATIONALES

11.1 Mécanismes de transfert transfrontalier. Dans la mesure où Trimble traite des données à caractère personnel provenant de et protégées par les Lois et règlements sur la protection des données dans l'une des juridictions énumérées dans l'Annexe 3 (Mécanismes de transfert transfrontalier) du présent ATD, les conditions spécifiées dans l'Annexe 3 en ce qui concerne la/les juridiction(s) applicable(s) s'appliquent en plus des conditions du présent ATD.

11.2 Mécanismes de transfert transfrontalier de données. Dans la mesure où l'utilisation des Services par Client nécessite un mécanisme de transfert ultérieur pour transférer légalement des Données à Caractère Personne d'une juridiction (c'est-à-dire l'Espace économique européen, le Royaume-Uni, la Suisse, la Turquie ou une autre juridiction énumérée dans l'Annexe 3 (Mécanismes de transfert transfrontalier du présent ATD) à Trimble située en dehors de cette juridiction ("Mécanisme de transfert"), les conditions énoncées dans l'Annexe 4 (Mécanismes de transfert transfrontalier) du présent ATD s'appliqueront.

12. Divers

12.1 Conflit. En cas de conflit ou d'incohérence entre les documents suivants, l'ordre de préséance sera le suivant : (1) les conditions applicables figurant à l'Annexe 4 (Mécanismes de transfert transfrontalier) du présent ATD ; (2) les conditions du présent ATD ne figurant pas à l'Annexe 4 (Mécanismes de transfert transfrontalier) ; et (3) l'Accord.

12.2 Mises à jour. Trimble peut mettre à jour les conditions du présent ATD de temps à autre ; à condition, toutefois, que Trimble fournisse à Client un préavis écrit d'au moins trente (30) jours lorsqu'une mise à jour est nécessaire suite à (a) des modifications dans les Lois et réglementations sur la protection des données ; (b) une fusion, une acquisition ou une autre transaction similaire ; ou (c) la sortie de nouveaux produits ou services ou des changements matériels à l'un des Services existants. Les conditions alors en vigueur du présent ATD sont disponibles sur trimble.com/privacy.

Nom légal de Client : _____

Adresse

Numéro de client Trimble : _____

☐ Client a acheté les Services par l'intermédiaire d'un revendeur agréé de Trimble ou d'un partenaire commercial de Trimble.

Nom du revendeur

Adresse _____

Numéro de client du revendeur

☐ Pour la facturation aux clients de l'UE/EEE/Royaume-Uni. Client souhaite entrer dans des Clauses contractuelles types de l'UE directement avec Trimble Inc. Si cette case n'est pas cochée, le mécanisme de transfert pour le transfert à Trimble Inc. est celui décrit dans la Section 2.2 de l'Annexe 4 ou tout autre mécanisme de transfert établi entre l'affilié Trimble en Europe et Trimble Inc.

Si la case précédente est cochée : Client considère que les modules suivants sont applicables :

☐Module 1/Contrat 1 ☐ Module 2/Contrat 2 ☐ Module 3/Contrat 3

☐ Client choisit d'exécuter le présent ATD
Les signataires autorisés des parties ont dûment signé le présent Accord :

CLIENT (signe par la présente le présent ATD)

Nom :

Titre

Date :

Trimble Inc.

Signature : _____
Imprimer nom : Jennifer Allison
Titre : Premier vice-président et Chef du contentieux
Date :15.7.2024

Trimble Europe BV

Signature : _____
Imprimer le nom : RHH Reeder
Titre : Directeur
Date :15.7.2024

Trimble UK Limited

Signature : _____
Imprimer le nom : RHH Reeder
Titre : Directeur
Date :15.7.2024

Trimble France SAS

Signature : _____
Imprimer le nom : RHH Reeder
Titre : Directeur
Date :15.7.2024

Trimble Solutions Sandvika AS

Signature : _____
Imprimer le nom : RHH Reeder
Titre : Directeur
Date :15.7.2024

Trimble Technologies Ireland Limited

Signature : _____
Imprimer le nom : RHH Reeder
Titre : Directeur
Date :15.7.2024

Lakefield eTechnologies Limited

Signature : _____
Imprimer le nom : RHH Reeder
Titre : Directeur
Date :15.7.2024

Trimble International BV

Signature : _____
Imprimer le nom : RHH Reeder
Titre : Directeur
Date :15.7.2024

Trimble Finland Corporation

Signature : _____
Imprimer nom : Jürgen Kesper
Titre : Directeur
Date :15.7.2024

Trimble Germany GmbH

Signature : _____
Imprimer le nom : RHH Reeder
Titre : Directeur
Date :15.7.2024

Trimble MAPS Limited.

Signature : _____
Imprimer le nom : RHH Reeder
Titre : Directeur
Date :15.7.2024

Trimble Forestry Europe Corporation

Signature : _____
Imprimer le nom : RHH Reeder
Titre : Directeur
Date :15.7.2024

Trimble GmbH

Signature : _____
Imprimer nom : Jürgen Kesper
Titre : Directeur
Date :15.7.2024

Coordonnées de toutes les entités Trimble :

privacy@trimble.com

Adresses des entités Trimble	
Trimble Inc.	**Trimble Europe B.V.**
10368 Westmoor Drive Westminster, CO 80021, États-Unis	Industrieweg 187a 5683CC Best, Pays-Bas
Trimble UK Limited	**Trimble France SAS**
Trimble House, Gelderd Road, Gildersome, Leeds LS27 7JP UK	1 Quai Gabriel Péri 94340 Joinville-le-Pont, France
Trimble Solutions Sandvika AS	**Trimble Technologies Ireland Limited**
Leif Tronstads plass 4 1337 Sandvika, Norvège	North Point Business Park, Unit 3d North Point House, New Mallow Rd, Cork, T23 AT2P, Irlande
Lakefield eTechnologies Limited	**Trimble International BV**
North Point Business Park, Unit 3d North Point House, New Mallow Rd, Cork, T23 AT2P, Irlande	Industrieweg 187a 5683CC Best, Pays-Bas
Trimble Finland Corporation	**Trimble Germany GmbH**
Hatsinanpuisto 8, 02600 Espoo, Finlande	Am Prime Parc 11, 65479 Raunheim
Trimble MAPS Limited.	**Trimble Forestry Europe Corporation**
53-64 Chancery Lane, Holborn, Londres Angleterre WC2A 1QS UK	Hatsinanpuisto 8, 02600 Espoo, Finlande
Trimble GmbH	
Am Prime Parc 11, 65479 Raunheim	

ANNEXE 1 - DESCRIPTION DU TRAITEMENT

1. CATÉGORIES DE PERSONNES CONCERNÉES DONT LES DONNÉES À CARACTÈRE PERSONNEL SONT TRANSFÉRÉES

Client peut soumettre aux Services des données à caractère personnel, dont l'étendue sont déterminées et contrôlées par Client à sa seule discrétion, et qui peuvent inclure, sans s'y limiter, des données à caractère personnel relatives aux catégories suivantes de personnes concernées :

- Les employés, les dirigeants, les administrateurs et les sous-traitants de Client.
- Les clients de Client (qui sont des personnes physiques), souvent en leur qualité de destinataires d'expéditions, de services et de produits.
- Les employés, les agents, les conseillers, les indépendants des clients de Client, les vendeurs et les contreparties des transactions traitées par l'intermédiaire des Services.
- Les utilisateurs de Client autorisés par ce dernier à utiliser les Services.

2. CATÉGORIES DE DONNÉES À CARACTÈRE PERSONNEL TRANSFÉRÉES

Client peut soumettre aux Services des données à caractère personnel, dont l'étendue sont déterminées et contrôlées par Client à sa seule discrétion, et qui peuvent inclure, sans s'y limiter, des catégories suivantes de données à caractère personnel :
- Données de contact et données de référence (Nom et prénom, Titre, Poste)
- Coordonnées (entreprise, courriel, téléphone, adresse physique de l'entreprise)
- Données d'identification telles que les passeports, les permis de conduire, les adresses IP, les identifiants uniques (UUID).
- Données relatives à l'emploi et à l'éducation (qualifications, expériences, compétences).
- Données relatives à l'emploi (services rendus, contributions aux projets, emplois et tâches attribués, données relatives à la performance, heures de service, dépenses).
- Données de localisation
- Données liées au contrat (facturation, paiement, historique des transactions)
- Historique des interactions

3. DONNÉES SENSIBLES TRANSFÉRÉES (LE CAS ÉCHÉANT)

Les données sensibles transférées (le cas échéant) et restrictions ou garanties appliquées qui tiennent pleinement compte de la nature des données et des risques encourus, comme par exemple une limitation stricte de la finalité, des restrictions d'accès (y compris un accès réservé au personnel ayant suivi une formation spécialisée), la tenue d'un registre d'accès aux données, des restrictions pour les transferts ultérieurs ou des mesures de sécurité supplémentaires :
L'exportateur de données peut soumettre aux Services des catégories spéciales de données, dont l'étendue est déterminée et contrôlée par l'exportateur de données à sa seule discrétion, et qui sont, par souci de clarté, les données à caractère personnel contenant des informations qui révèlent l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins de l'identification unique d'une personne physique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.
Les mesures de sécurité applicables sont décrites dans la Section 11 de l'Annexe 2 ci-dessous.

4. FRÉQUENCE DU TRANSFERT

La fréquence du transfert (par ex. le fait que les données soient transférées de manière ponctuelle ou continue) :

En permanence, en fonction de l'utilisation des services par Client.

5. NATURE DU TRAITEMENT

La nature du traitement est l'exécution des Services conformément à l'Accord.

6. FINALITÉ DU TRAITEMENT, TRANSFERT DES DONNÉES ET TRAITEMENT ULTÉRIEUR

Trimble traitera les données à caractère personnel comme nécessaire pour exécuter les Services conformément à l'Accord, comme spécifié dans la documentation, et comme indiqué par Client dans son utilisation des Services. Trimble rendra encore plus anonymes les données à caractère personnel afin d'effectuer des analyses de données et de développer des services.

7. DURÉE DU TRAITEMENT

La durée de conservation des données à caractère personnel ou, si cela n'est pas possible, les critères utilisés pour déterminer cette durée :

Trimble traitera les données à caractère personnel comme indiqué dans l'Accord, sauf accord contraire, par exemple dans la section 9 de l'ATD.

8. TRANSFERTS AUX SOUS-TRAITANTS ULTÉRIEURS

Pour les transferts aux sous-traitants (ultérieurs), il faut également préciser l'objet, la nature et la durée du traitement :

Le sous-traitant ultérieur traitera les données à caractère personnel dans la mesure nécessaire à l'exécution des Services conformément à l'Accord. Sous réserve de la section 9 du présent ATD, le sous-traitant ultérieur traitera les données à caractère personnel pendant la durée de l'Accord, sauf accord écrit contraire.

Les identités des Sous-traitants ultérieurs utilisés pour la fourniture des Services et leur pays d'établissement sont répertoriés sous l'onglet Additional Materials (Matériaux supplémentaires) dans le site trimble.com/privacy.

ANNEXE 2 - Mesures de sécurité techniques et organisationnelles

Le cas échéant, cette Annexe 2 servira également d'Annexe II aux Clauses contractuelles types de l'UE.

Mesures de sécurité techniques et organisationnelles

1. Mesures de pseudonymisation et de cryptage des données à caractère personnel

Dans la mesure du possible, Trimble crypte les données transmises entre les clients et l'application Trimble sur les réseaux publics en utilisant TLS 1.2 ou plus. Les données des clients stockées sur les systèmes gérés par Trimble (pour les produits certifiés AICPA - voir le point 7 ci-dessous pour de plus amples informations) sont cryptées en utilisant AES 256 ou des chiffres plus puissants.

2. Mesures visant à garantir en permanence la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement

Trimble dispose d'un personnel dédié à la cybersécurité responsable de la surveillance de la sécurité et de la confidentialité. Elle a nommé des responsables de la cybersécurité et de la confidentialité, en plus d'un Bureau de la protection des données, ainsi qu'un Conseil de direction de l'ingénierie qui se réunit tous les trimestres pour discuter des risques liés à la confidentialité et à la sécurité gérés au sein des Portefeuilles de produits sectoriels. En outre, les risques liés aux produits sont suivis dans un portail interne avec un contrôle de conformité qui est effectué tous les mois.

3. Mesures visant à garantir la capacité de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci en temps utile en cas d'incident physique ou technique

Afin de soutenir la disponibilité des produits SaaS de Trimble, Trimble s'appuie sur des principaux fournisseurs de services en nuage (Amazon Web Services (AWS) et Microsoft Azure) pour une mise à l'échelle automatique, des centres de données géographiquement diversifiés, une surveillance étendue des applications et de l'infrastructure, et des mécanismes d'assistance 24 heures sur 24 et 7 jours sur 7.
Trimble maintient des sauvegardes des banques de données, y compris les données des clients, qui prennent en charge les fonctionnalités primaires des applications Trimble. Dans la mesure du possible, les sauvegardes sont stockées dans un endroit géographiquement séparé de l'endroit de stockage principal des données.
En plus des mesures de nos fournisseurs de services, Trimble maintient une fonction de réponse aux incidents de sécurité qui comprend une Planolitique de réponse aux incidents documentée et un plan pour trier les événements de sécurité et les incidents impliquant les données des clients. Celle-ci définit le protocole de réponse tel que les activités de confinement, d'éradication, de restauration et de communication pour les incidents de sécurité, ainsi que les rôles et les responsabilités du personnel de Trimble et l'exigence d'examens post-incidents avec la direction de Trimble.

4. Procédures permettant de tester, d'apprécier et d'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles afin d'assurer la sécurité du traitement.

Trimble emploie des tiers indépendants pour effectuer des tests de pénétration périodiques, y compris des audits Sarbanes-Oxley, PCI, SOC 1, Type II, SOC 2 Type II, ISO27001 ou NIST 800-171 équivalents sur une base

annuelle lorsque cela est nécessaire pour la conformité avec les réglementations. En outre, Trimble effectue régulièrement des tests de vulnérabilité internes et des tests de pénétration sur les produits et les plates-formes applicables, conformément au programme de cybersécurité de Trimble et aux exigences de la politique. Trimble peut effectuer des évaluations de nouveaux vendeurs ou partenaires si le risque commercial justifie un examen. Trimble encourage les tiers à signaler tous les problèmes, incidents et vulnérabilités de cybersécurité associés à nos produits, nos services ou nos sites Web.

5. Mesures d'identification et d'autorisation des utilisateurs

Pour les produits utilisant Trimble ID (TID, Trimble Identity) pour l'authentification, Trimble traite le mot de passe de manière sécurisée. En outre, certains produits Trimble peuvent prendre en charge l'intégration de l'authentification unique (SSO) avec un fournisseur d'identité client utilisant Security Assertion Markup Language (langage de marquage d'assertion de sécurité) (SAML) et l'authentification multi-facteurs (MFA).

6. Mesures de protection des données lors de leur transmission

Comme indiqué au point 1, Trimble crypte les données des clients transmises sur des réseaux publics entre les clients et l'application Trimble en utilisant des codes de cryptage courants dans la mesure du possible.

7. Mesures de protection des données lors de leur stockage

Conformément au point 1, les données des clients stockées sur un stockage de données géré par Trimble sont cryptées en utilisant AES 256 ou plus pour tous les produits Trimble actuellement certifiés AICPA SOC 1, Type II, SOC 2, Type II ou NIST 800-171. Consulter le point 11 pour des informations plus détaillées.

8. Mesures visant à assurer la sécurité physique des lieux où sont traitées les données à caractère personnel

Les produits, les applications et les services SaaS de Trimble sont généralement hébergés avec les données des clients stockées dans des centres de données fournis par Amazon Web Services (AWS), Microsoft Azure ou Google Cloud Platform (GCP). En conséquence, Trimble s'appuie sur les contrôles physiques, environnementaux et d'infrastructure de ces plates-formes. Trimble examine périodiquement les certifications et les attestations de tiers fournies par ces fournisseurs concernant l'efficacité des contrôles de leurs centres de données.

9. Mesures visant à garantir l'enregistrement des événements

Trimble maintient de nombreux journaux d'outils de cybersécurité et des journaux d'audit de sécurité des applications et de l'infrastructure. Les journaux de sécurité sont analysés en utilisant la technologie SIEM en combinaison avec la corrélation d'événements pour détecter les activités anormales.

10. Mesures visant à garantir la configuration du système, y compris la configuration par défaut

Trimble s'appuie sur des normes industrielles communes pour renforcer la cybersécurité grâce à une configuration sécurisée et une défense en profondeur. Trimble applique des correctifs de sécurité à ses systèmes conformément à la Trimble Secure Development Lifecycle Policy (Politique de cycle de vie de développement sécurisé de Trimble) (TSDLCP).

11. Mesures concernant la gouvernance et à la gestion internes des technologies de l'information et de la sécurité informatique

Pour les produits certifiés SOC 1, Type II, SOC 2, Type II ou NIST 800-171 de Trimble, le personnel ayant accès aux données des clients utilise des principes de contrôle d'accès basés sur les rôles et les moindres privilèges. Le personnel n'est fourni d'accès aux données des clients que dans la mesure où cela lui permet de s'acquitter de ses tâches en toute sécurité. L'accès à distance aux systèmes Trimble nécessite une communication cryptée via des protocoles sécurisés et l'utilisation d'une authentification multi-facteurs. Trimble a établi et maintiendra des procédures de gestion des mots de passe pour ce personnel démographique, conçues pour garantir que les mots de passe sont uniques pour chaque individu, et inaccessibles aux personnes non autorisées, y compris au minimum :

- la protection cryptographique des mots de passe lorsqu'ils sont stockés dans des systèmes informatiques ou qu'ils transitent par un réseau public ;
- la modification des mots de passe par défaut des fournisseurs ; et
- l'éducation aux bonnes pratiques en matière de mots de passe, telles que l'utilisation de phrases de passe
- l'accès du personnel à l'infrastructure de production nécessite une authentification multi-facteurs (MFA).

Pour la conformité à la certification ISO 27001 et pour garantir une utilisation correcte et efficace de la cryptographie afin de protéger la confidentialité et l'intégrité des données détenues ou gérées par Trimble, les données classées comme confidentielles ou restreintes doivent être cryptées par l'utilisation de processus de cryptage valides pour les données au repos et en mouvement, comme l'exige la réglementation et/ou l'évaluation des risques. Cela inclut, sans s'y limiter, les informations sensibles stockées sur des appareils mobiles, des disques amovibles et des ordinateurs portables. Trimble n'utilisera que des applications de cryptographie commerciales non modifiées pour crypter les données au repos et/ou en transit.

Le personnel de Trimble est soumis à des obligations de confidentialité et à diverses politiques, telles que l'utilisation acceptable, la classification des données, la destruction sécurisée et la MFA. Trimble demande à son personnel de suivre une formation de sensibilisation à la sécurité de l'information, à la fois au début de leur emploi et chaque année par la suite. Trimble demande également à son personnel de suivre une formation annuelle sur la protection de la vie privée (notamment pour se conformer au RGPD).

Pour les produits applicables, Trimble a mis en place des principes de sécurité et de protection de la vie privée dès la conception, y compris, mais sans s'y limiter, la modélisation des menaces et les tests de pénétration de l'application du produit.

12. Mesures de certification/assurance des processus et des produits

Trimble maintiendra les certifications SOC 2, Type II, ISO 27001 ou NIST 800-171, en subissant une surveillance externe périodique et des audits de recertification pour s'assurer que son Information Security Management System (Système de gestion de la sécurité de l'information) (ISMS) répond aux exigences de cette norme pour les produits applicables.

Trimble maintiendra des politiques de sécurité de l'information qui répondent aux exigences de la norme ISO 27001, un programme d'audit interne qui évalue le Système de gestion de la sécurité de l'information (ISMS) de Trimble et les contrôles de sécurité de l'information, et un comité de gestion qui est responsable de la surveillance du Information Security Management System (Système de gestion de la sécurité de l'information) (ISMS) de Trimble.

13. Mesures visant à assurer la minimisation des données

Trimble peut permettre aux visiteurs d'utiliser certaines fonctionnalités de certains produits de manière anonyme et minimise les données qu'elle exige des clients à ce qui est nécessaire pour fournir le service demandé en vertu des lois et réglementations locales.

14. Mesures visant à garantir la qualité des données

Trimble garantit la qualité de ses données par le biais de divers mécanismes de vérification propres aux produits Trimble concernés. Trimble peut également permettre aux utilisateurs de produits de mettre à jour les informations dans leurs comptes eux-mêmes ou par le biais de demandes à ses fonctions d'assistance à la clientèle.

15. Mesures visant à garantir la conservation limitée des données

Trimble peut mettre en œuvre la Politique de conservation des données du client qui définit les périodes de conservation des différents types de données.

16. Mesures visant à permettre la portabilité des données et à garantir leur effacement

Les produits Trimble applicables disposent d'un processus de suppression des données des clients dans les 30 jours suivant la réception des demandes écrites vérifiées des clients et peuvent permettre le téléchargement des données des clients pour les fournir à d'autres fournisseurs de services, comme l'exige le RGPD.

17. Contrôle et gestion des tiers (Sous-traitant ultérieur)

Trimble n'emploie que des sous-traitants ultérieurs qui traitent les données à caractère personnel au nom de Trimble dans le cadre des services d'abonnement applicables en conformité avec les Lois et règlements sur la protection des données. Trimble vérifie également, avant de choisir un sous-traitant ultérieur et de transférer des données, les mesures techniques et organisationnelles du sous-traitant ultérieur pour assurer un niveau de sécurité approprié au risque de traitement des données de ses clients. Trimble prend également des mesures raisonnables pour garantir la sécurité des transferts des données des clients à des sous-traitants ultérieurs tiers. Au minimum, ces mesures comprennent l'identification des risques pour les droits de Client et de la Personne concernée en fonction de la nature, de la portée et du contexte du traitement ; l'examen des contrôles de sécurité et de protection des données mis en œuvre par le Sous-traitant ultérieur pour protéger les données du client (y compris les rapports d'audit SOC 2 de type II et/ou les certificats ISO 27001, le cas échéant) ; imposer des conditions contractuelles de protection des données qui protègent les données à caractère personnel de manière identique ou similaire que

Trimble est obligée de fournir à ses clients (y compris des mécanismes de transfert transfrontalier valides, la gestion des sous-traitants ultérieurs et des programmes de conformité) ; exiger que le Sous-traitant ultérieur traite uniquement les données du client au nom de Trimble et de ses clients et, limiter son traitement des données du client à la portée des instructions de Trimble.

ANNEXE 3 - Mécanisme de transfert transfrontalier

1. Espace économique européen (EEE) :

1.1 La définition des "Lois et règlements sur la protection des données" inclut le Règlement général sur la protection des données (UE 2016/679) ("***RGPD***").

1.2 Lorsque Trimble engage un sous-traitant ultérieur en vertu de la section 5.1 (Nomination de Sous-traitants ultérieurs) du présent ATD, il :

(a) exigera de tout sous-traitant ultérieur désigné qu'il protège les données du client au niveau requis par les Lois et règlements sur la protection des données et impose les mêmes obligations en matière de protection des données que celles visées à l'article 28, paragraphe 3, du RGPD, en particulier en fournissant des garanties suffisantes pour mettre en œuvre les mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD, et

(b) exigera de tout sous-traitant ultérieur désigné (i) qu'il s'engage par écrit à ne traiter les données à caractère personnel que dans un pays que l'Union européenne a déclaré avoir un niveau de protection "adéquat" ou (ii) qu'il ne traite les données à caractère personnel que sur la base des Clauses contractuelles types de l'UE ou conformément aux Règles d'entreprise contraignantes approuvées par les autorités compétentes de l'Union européenne en matière de protection des données.

1.3 Nonobstant toute disposition contraire du présent ATD ou de l'Accord (y compris, sans limitation, les obligations d'indemnisation de l'une ou l'autre des parties), aucune des parties ne sera responsable des amendes RGPD émises ou perçues en vertu de l'article 83 du RGPD à l'encontre de l'autre partie par une autorité réglementaire ou un organisme gouvernemental en rapport avec la violation du RGPD par cette autre partie.

1.4 Client reconnaît que Trimble, en tant que responsable du traitement, peut être tenu, en vertu des Lois et règlements sur la protection des données, de notifier à une autorité réglementaire les incidents de sécurité impliquant les données d'utilisation du client. Si une autorité réglementaire exige que Trimble notifie les personnes concernées impactées avec lesquels Trimble n'a pas de relation directe (par exemple, les utilisateurs finaux de Client), Trimble notifiera cette exigence à Client. Client fournira une assistance raisonnable à Trimble pour notifier les personnes concernées impactées.

2. Royaume-Uni (UK) :

2.1 Dans le présent ATD, les références au "RGPD" seront considérées comme des références aux lois et réglementations correspondantes du Royaume-Uni, y compris, sans limitation, le UK GDPR and Data Protection Act 2018 .

2.2 Lorsque Trimble engage un sous-traitant ultérieur en vertu de la section 5.1 (Nomination de Sous-traitants ultérieurs) du présent ATD, il :

(a) exigera de tout sous-traitant ultérieur désigné qu'il protège les données du client au niveau requis par les Lois et règlements sur la protection des données, tel que l'inclusion des mêmes obligations en matière de protection des données que celles visées à l'article 28(3), du RGPD du Royaume-Uni, en particulier en fournissant des garanties suffisantes pour mettre en œuvre les mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD du Royaume-Uni, et

(b) exigera de tout sous-traitant ultérieur désigné (i) qu'il s'engage par écrit à ne traiter les données à caractère personnel que dans un pays que le Royaume-Uni a déclaré avoir un niveau de protection "adéquat" ou (ii) qu'il ne traite les données à caractère personnel que dans des conditions équivalentes à l'Accord international de transfert de données du Royaume-Uni ou des Clauses contractuelles types de l'UE et à l'Addendum international de transfert de données du Royaume-Uni ou conformément aux Règles d'entreprise contraignantes approuvées par les autorités compétentes du Royaume-Uni en matière de protection des données.

2.3 Nonobstant toute disposition contraire du présent ATD ou de l'Accord (y compris, sans limitation, les obligations d'indemnisation de l'une ou l'autre des parties), aucune des parties ne sera responsable des amendes RGPD du Royaume-Uni émises ou perçues en vertu de l'article 83 du RGPD du Royaume-Uni à l'encontre de l'autre partie par une autorité réglementaire ou un organisme gouvernemental en rapport avec la violation du RGPD du Royaume-Uni par cette autre partie.

2.4 Client reconnaît que Trimble, en tant que responsable du traitement, peut être tenu, en vertu des Lois et règlements sur la protection des données, de notifier à une autorité réglementaire les incidents de sécurité impliquant les données d'utilisation du client. Si une autorité réglementaire exige que Trimble notifie les personnes concernées impactées avec lesquels Trimble n'a pas de relation directe (par exemple, les utilisateurs finaux de Client), Trimble notifiera cette exigence à Client. Client fournira une assistance raisonnable à Trimble pour notifier les personnes concernées impactées.

3. La Suisse :

3.1 La définition des "Lois et règlements sur la protection des données" comprend la Loi fédérale suisse sur la protection des données, telle que révisée ("***LPD***")**.**

3.2 Lorsque Trimble engage un sous-traitant ultérieur en vertu de la section 5.1 (Nomination de Sous-traitants ultérieurs) du présent ATD, il :

(a) exigera de tout sous-traitant ultérieur désigné qu'il protège les données du client au niveau requis par les Lois et règlements sur la protection des données, en particulier en fournissant des garanties suffisantes pour mettre en œuvre les mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences de la LPD, et

(b) exigera de tout sous-traitant ultérieur désigné (i) qu'il s'engage par écrit à ne traiter les données à caractère personnel que dans un pays que la Suisse a déclaré avoir un niveau de protection "adéquat" ou (ii) qu'il ne traite les données à caractère personnel que sur la base similaire aux Clauses contractuelles types de l'UE y compris les modifications mentionnées à la section 3.3 ou conformément aux Règles d'entreprise contraignantes approuvées par les autorités compétentes de l'Union européenne ou la Suisse en matière de protection des données.

3.3 Dans la mesure où les transferts de données à caractère personnel depuis la Suisse sont soumis aux Clauses contractuelles types de l'UE conformément à la section 2.3 de l'Annexe 3 (Clauses contractuelles types de l'UE), les parties conviennent que toutes les modifications jugées nécessaires par le Préposé fédéral suisse à la protection des données et de l'information seront apportées aux Clauses contractuelles types de l'UE. Plus précisément, il s'agit de la date de conclusion de l'ATD :

(a) les références à "État membre de l'UE" et "État membre" seront interprétées comme incluant la Suisse, et

(b) dans la mesure où le transfert ou les transferts ultérieurs sont soumis à la LPD :

"(i) les références au "Règlement (UE) 2016/679" doivent être interprétées comme des références à la LPD ;

(ii) l'"autorité de contrôle compétente" visée à l'Annexe I, Partie C, est le Préposé fédéral suisse à la protection des données et de l'information ;

(iii) dans la Clause 17 (Option 1), les Clauses contractuelles types de l'UE seront régies par le droit suisse ; et

(iv) dans la Clause 18(b) des Clauses contractuelles types de l'UE, les litiges seront résolus devant les tribunaux suisses.

(v) la Clause 18(c) des Clauses contractuelles types de l'UE s'applique alors qu'une personne concernée peut également intenter une action en justice contre l'exportateur et/ou l'importateur de données devant les tribunaux suisses où la personne concernée a sa résidence habituelle.

4. États-Unis d'Amérique :

4.1 "***Lois des États américains sur la protection de la vie privée***" désigne toutes les lois des États relatives à la protection et au traitement des données à caractère personnel en vigueur aux États-Unis d'Amérique, qui peuvent inclure, sans s'y limiter, 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 ("***CCPA***"), la Loi de Virginie sur la protection des données des consommateurs, la Loi sur la protection de la vie privée au Colorado, la Loi sur la protection des données du Connecticut, et la Loi sur la protection de la vie privée des consommateurs de l'Utah.

4.2 La définition des "Lois et règlements sur la protection des données" inclut les Lois sur la protection de la vie privée des États-Unis.

4.3 Les termes suivants s'appliquent lorsque Trimble traite les données à caractère personnel soumises à la CCPA :

(a) Le terme "***informations personnelles***", tel qu'il est utilisé dans la présente section 4.3, aura la signification prévue dans la CCPA ;

(b) Trimble agit en tant qu'un fournisseur de services lors du traitement des données du client. Trimble traitera toute information personnelle contenue dans les données du client uniquement pour les objectifs commerciaux prévus dans l'Accord, y compris l'objectif du traitement et les activités de traitement prévus dans le présent ATD ("***Objectif***"). En tant que fournisseur de services, Trimble ne vendra pas et ne partagera pas les données du client et ne conservera pas, n'utilisera pas et ne divulguera pas les données du client (i) à des fins autres que l'Objectif, y compris la conservation, l'utilisation ou la divulgation des données du client à des fins commerciales autres que l'Objectif, ou autrement autorisées par la CCPA ; ou (ii) en dehors de la relation d'affaires directe entre Client et Trimble ;

(c) Trimble (i) se conformera aux obligations qui lui sont applicables en tant que fournisseur de services en vertu de la CCPA et (ii) fournira des informations personnelles avec le même niveau de protection de la vie privée que celui exigé par la CCPA. Il est de la responsabilité de Client de s'assurer qu'il s'est conformé et qu'il continuera à se conformer aux exigences de la CCPA dans le cadre de son utilisation des Services et de son propre traitement des informations personnelles ;

(d) Client aura le droit de prendre des mesures raisonnables et appropriées pour aider à garantir que Trimble utilise les informations personnelles d'une manière compatible avec les obligations de Client en vertu de la CCPA ;

(e) Trimble informera Client si elle détermine qu'elle ne peut plus remplir ses obligations en tant que fournisseur de services en vertu de la CCPA ;

(f) Sur notification, Client aura le droit de prendre des mesures raisonnables et appropriées, conformément à l'Accord, pour mettre fin à l'utilisation non autorisée des informations personnelles et y remédier ;

(g) Trimble fournira une assistance supplémentaire raisonnable et opportune pour aider Client à se conformer à ses obligations en ce qui concerne les demandes des consommateurs comme indiqué dans l'Accord ;

(h) Pour tout Sous-traitant ultérieur utilisé par Trimble pour traiter les informations personnelles soumises à la CCPA, Trimble s'assurera que l'accord de Trimble avec un tel sous-traitant ultérieur est conforme à la CCPA, y compris, sans limitation, les exigences contractuelles pour les fournisseurs de services et les entrepreneurs ;

(i) Trimble ne combinera pas les données de Client qu'elle reçoit de, ou au nom de Client, avec des informations personnelles qu'elle reçoit de, ou au nom d'une autre personne ou d'autres personnes, ou qu'elle recueille à partir de sa propre interaction avec le consommateur, à moins qu'une telle combinaison ne soit nécessaire pour réaliser un objectif commercial tel qu'autorisé par la CCPA, y compris toute réglementation y afférente, ou par les réglementations adoptées par l'Agence californienne de protection de la vie privée ; et

(j) Trimble certifie qu'elle comprend et qu'elle se conformera à ses obligations en vertu de la CCPA.

4.4 Trimble reconnaît et confirme qu'elle ne reçoit pas les données de Client en contrepartie des services fournis à Client.

5. Australie :

5.1 La définition des "Lois et règlements sur la protection des données" inclut les Principes australiens de protection de la vie privée et la Loi australienne sur la protection de la vie privée (1988).

5.2 La définition des "Données à caractère personnel" comprend les "Informations personnelles" telles que définies par les Lois et règlements sur la protection des données.

5.3 La définition des "données sensibles" comprend les "Informations sensibles" telles que définies par les Lois et règlements sur la protection des données.

6. Brésil :

6.1 La définition des "Lois et règlements sur la protection des données" comprend la Lei Geral de Proteção de Dados (Loi générale sur la protection des données à caractère personnel).

6.2 La définition d'un "Incident de sécurité" comprend un incident de sécurité susceptible d'entraîner un risque ou
6.3 La définition de "Sous-traitant" comprend un "opérateur" telle que définie par les Lois et règlements sur la protection des données.

7. Canada :

7.1 La définition des "Lois et règlements sur la protection des données" comprend la Loi fédérale sur la protection des renseignements personnels et les documents électroniques.

7.2 Les sous-traitants ultérieurs de Trimble, comme indiqués dans la section 5 (Sous-traitants ultérieurs) du présent ATD, sont des tiers en vertu des Lois et règlements sur la protection des données, avec lesquels Trimble a conclu un contrat écrit qui comprend des conditions substantiellement similaires au présent ATD. Trimble a procédé à une vérification appropriée de ses sous-traitants ultérieurs.

7.3 Trimble mettra en œuvre des mesures techniques et organisationnelles comme indiquées dans la section 11 de l'Annexe 2 (Sécurité) du présent ATD.

8. Israël :

8.1 La définition des "Lois et règlements sur la protection des données" inclut la Loi sur la protection de la vie privée.

8.2 La définition de "Responsable du traitement" comprend le "Propriétaire de base de données" telle que définie par les Lois et règlements sur la protection des données.

8.3 La définition de "Sous-traitant" comprend un "Titulaire" telle que définie par les Lois et règlements sur la protection des données.

8.4 Trimble exigera que tout le personnel autorisé à traiter les données du client respecte le principe de la confidentialité des données et ait été dûment instruit au sujet des Lois et règlements sur la protection des données. De tel personnel signe des accords de confidentialité avec Trimble conformément à la section 6 (Confidentialité) du présent ATD.

8.5 Trimble doit prendre des mesures suffisantes pour assurer la confidentialité des personnes concernées en mettant en œuvre et en maintenant les mesures de sécurité telles que spécifiées dans la Section 11 de l'Annexe 2 (Sécurité) du présent ATD et en se conformant aux termes de l'Accord.

8.6 Trimble doit s'assurer que les données à caractère personnel ne seront pas transférées à un Sous-Traitant ultérieur à moins que ce Sous-Traitant ultérieur n'ait signé un accord avec Trimble conformément à la Section 5.1 (Nomination de Sous-traitants ultérieurs) du présent ATD.

9. Japon :

9.1 La définition des "Lois et règlements sur la protection des données" inclut la Loi sur la protection des informations personnelles (“***APPI***”).

9.2 La définition de "Données à caractère personnel" comprend les informations sur un individu spécifique applicables en vertu de l'article 2(1) de l'APPI, que Client confie à Trimble au cours de la fourniture par Trimble des services à Client.

9.3 Trimble convient qu'elle a et maintiendra un programme de protection de la vie privée conforme aux normes prescrites par les règles de la Commission de protection des informations personnelles concernant le traitement des données à caractère personnel conformément aux dispositions du chapitre 4 de l'APPI. En conséquence :

(a) Trimble (i) traitera les données à caractère personnel comme nécessaire pour fournir les services à Client conformément à l'Accord et comme indiqué dans l'Annexe 1 (Description du traitement) du présent ATD ("*Objectif de l'utilisation*") et (ii) ne traitera pas les données à caractère personnel pour tout autre objectif que l'Objectif du traitement sans le consentement de Client ;

(b) Trimble mettra en œuvre et maintiendra des mesures appropriées et nécessaires pour empêcher la divulgation non autorisée et la perte des données à caractère personnel et pour la gestion sécurisée des données à caractère personnel conformément à l'APPI comme indiqué dans l'Annexe 2 (Mesures techniques et organisationnelles) du présent ATD ;

(c) Trimble notifiera Client pour (i) un manquement à l'obligation de se conformer à la section 9.3(a) de cette Annexe 3 ou (ii) la découverte par Trimble d'un incident de sécurité ayant un impact sur les données du client, dans les deux cas, conformément à la section 6.4 du présent ATD. Trimble fournira une assistance raisonnable à Client dans le cas où Client est tenu de notifier une autorité réglementaire ou toute personne concernée affectée par un incident de sécurité ;

(d) Trimble s'assurera que tous ses employés qui ont accès aux données à caractère personnel (i) ont signé des accords d'employés exigeant qu'ils gardent ces données à caractère personnel confidentielles et (ii) qui violent la confidentialité seront soumis à des mesures disciplinaires et éventuellement à un licenciement ; (iii) effectuent une supervision et une formation appropriées des employés pour la gestion sécurisée des données à caractère personnel ; et (iv) limitent le nombre de personnel autorisé, y compris les employés de Trimble, qui ont accès aux données à caractère personnel et contrôlent un tel accès de telle sorte qu'il n'est autorisé que pour la période de temps nécessaire pour l'Objectif du traitement ;

(e) Trimble ne divulguera pas les données à caractère personnel à un tiers, sauf si Client a autorisé Trimble à le faire dans l'accord. Lors de l'engagement des Sous-Traitants ultérieurs, Trimble se conformera aux obligations de la Section 9 (Sous-Traitants ultérieurs) du présent ATD pour s'assurer que des procédures sont en place pour maintenir la confidentialité et la sécurité des données à caractère personnel ;

(f) Trimble conservera des dossiers sur le traitement des données à caractère personnel qui lui ont été confiées par Client et effectuées pour lui ;

(g) Client peut évaluer la conformité de Trimble avec ses obligations en vertu des Lois et règlements sur la protection des données et comme indiqué dans la section 6 du présent ATD.

(h) Trimble fournira une coopération raisonnable à Client sur demande écrite, lorsque Client fait un rapport à la Commission de protection des informations à caractère personnel ou à d'autres autorités réglementaires ; et

(i) Les installations de traitement primaires de Trimble sont situées aux États-Unis d'Amérique et, en fonction de l'utilisation des services par Client, à partir des endroits indiqués sur le site https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center sous “Additional Resources” (Ressources supplémentaires) ("Sub-Processor Lists") (Listes de sous-traitants ultérieurs). Trimble informera Client de tout changement et donnera à Client la possibilité de s'opposer conformément à la Section 9 du présent ATD. Lorsque Trimble traite les données à caractère personnel dans un pays autre que le Japon, Trimble s'assurera qu'il se conforme à son programme de protection de la vie privée tel que décrit dans le présent ATD.

9.4 Les conditions suivantes relatives au consentement de la personne concernée s'appliquent :

(a) Client confie à Trimble les données à caractère personnel pour l'Objectif du traitement. Client convient que Trimble n'est pas un "tiers" tel que le terme est utilisé dans les dispositions de l'APPI qui limitent la fourniture des données à caractère personnel à des tiers. En conséquence, l'obligation d'obtenir le consentement préalable de la personne concernée ne s'applique pas ;

(b) si le consentement de la personne concernée est requis en vertu de l'article 4 de la Loi sur les entreprises de télécommunications, Client se conformera à toute exigence de consentement spécifique à son utilisation des services.

10. Mexique :

10.1 La définition des "Lois et règlements sur la protection des données" inclut la Loi fédérale sur la protection des données à caractère personnel détenues par des personnes privées et ses règlements.

10.2 Lorsqu'elle agit en tant que Sous-traitant, Trimble :

(a) traitera les données à caractère personnel conformément aux instructions du client comme indiqué dans la section 5 du présent ATD ;

(b) traitera les données à caractère personnel uniquement dans la mesure nécessaire à la fourniture des services ;

(c) mettra en œuvre des mesures de sécurité conformément aux Lois et règlements sur la protection des données et à l'Annexe 2 (Mesures techniques et organisationnelles) du présent ATD ;

(d) préservera la confidentialité des données à caractère personnel traitées conformément à l'Accord ;

(e) supprimera toutes les données à caractère personnel à la fin de l'Accord conformément à la section 10 (Restitution ou suppression des données de Client) du présent ATD ; et

(f) ne transférera les données à caractère personnel à des sous-traitants ultérieurs que conformément à la section 9 (Sous-traitants ultérieurs) du présent ATD.

11. Singapour :

11.1 La définition des "Lois et règlements sur la protection des données" inclut la Loi sur la protection des données à caractère personnel 2012 ("***RGPD***").

11.2 Trimble traitera les données à caractère personnel selon une norme de protection conforme à la RGPD en mettant en œuvre des mesures techniques et organisationnelles adéquates comme indiqué dans l'Annexe 2 (Mesures techniques et organisationnelles) du présent ATD et en se conformant aux termes de l'Accord.

12. République de Turquie

12.1 La définition des "Lois et règlements sur la protection des données" inclut (i) la Loi sur la protection des données à caractère personnel ("PDPL"), Loi numéro 6698, du 24 mars 2016, telle qu'amendée par la Loi sur l'élaboration des amendements au Code de procédure pénale et autres lois, Loi numéro 7499, du 2 mars 2024 et (ii) le Règlement sur les principes concernant les procédures et les règles pour le transfert des données à caractère personnel à l'étranger de l'Autorité de protection des données à caractère personnel, tel que publié dans le Journal officiel du 10 juillet, numéro 32598.

12.2 Client reconnaît que Trimble, en tant que Responsable du traitement, peut être tenu, en vertu des Lois et règlements sur la protection des données, de notifier à une autorité réglementaire les incidents de sécurité impliquant les données d'utilisation du client. Si une autorité réglementaire exige que Trimble notifie les personnes concernées impactées avec lesquels Trimble n'a pas de relation directe (par exemple, les utilisateurs finaux de Client), Trimble notifiera cette exigence à Client. Client fournira une assistance raisonnable à Trimble pour notifier les personnes concernées impactées.

ANNEXE 4 - MÉCANISME DE TRANSFERT TRANSFRONTALIER
(S'applique aux données transférées depuis l'UE, l'EEE, le Royaume-Uni et la Suisse)

1. Définitions

- ***"Clauses contractuelles types de l'UE"*** désigne les Clauses contractuelles types approuvées par la Commission européenne dans sa décision 2021/914.
- ***"Accord international de transfert de données du Royaume-Uni"*** désigne l'Addendum sur le transfert international de données aux Clauses contractuelles types de la Commission européenne publié par le Commissaire à l'information du Royaume-Uni, version B1.0, en vigueur le 21 mars 2022.
- ***"Cadre de protection des données"*** désigne le programme d'auto-certification du Cadre de protection des données UE-États-Unis et/ou Suisse-États-Unis géré par le Département du commerce des États-Unis.
- ***"Principes de confidentialité des données"*** désigne les principes du Cadre de protection des données (complétés par les principes supplémentaires).
- ***"Clauses contractuelles types de la Turquie"*** signifie le Contrat type à utiliser dans le Transfert de données à caractère personnel à l'étranger 1 – 4, tel qu'accepté par la décision 2024/959 du 4 juin 2024 de l'Autorité turque de protection des données à caractère personnel.

2. Mécanismes de transfert transfrontalier de données

2.1 Ordre de préséance. Dans le cas où les services sont couverts par plus d'un mécanisme de transfert, le transfert de Données à caractère personnel sera soumis à un seul mécanisme de transfert, le cas échéant, et conformément à l'ordre de préséance suivant : (a) le Cadre de protection des données tel que mentionné à la section 2.2 (Cadre de protection des données) de la présente Annexe ; (b) les Clauses contractuelles types de l'UE telles que mentionnées à la section 2.3 (Clauses contractuelles types de l'UE) de la présente Annexe ; (c) l'Addendum sur le transfert international de données du Royaume-Uni mentionné à la section 2.4 (Addendum sur le transfert international de données du Royaume-Uni) de la présente Annexe ; et, si ni (a), ni (b), ni (c), ni (c),ni (e) ne sont applicables, alors (f) d'autres mécanismes de transfert de données applicables autorisés en vertu des Lois et règlements sur la protection des données.

2.2 Cadre de protection des données. Dans la mesure où Trimble Inc. traite des données à caractère personnel via les Services provenant de l'EEE ou de la Suisse, Trimble Inc. est auto-certifié en vertu du Cadre de protection des données et se conforme aux Principes de protection des données lors du traitement de ces données à caractère personnel. Dans la mesure où Client est (a) situé aux États-Unis et est également auto-certifié en vertu du Cadre de protection des données ou (b) situé dans l'EEE ou en Suisse, Trimble accepte en outre (i) de fournir au moins le même niveau de protection à toutes les données à caractère personnel que celui exigé par les Principes de protection des données ; (ii) de notifier Client par écrit, sans retard excessif, si son auto-certification au Cadre de protection des données est retirée, résiliée, révoquée ou autrement invalidée (dans ce cas, un mécanisme de transfert alternatif s'appliquera conformément à l'ordre de préséance dans la Section 2.1 (Ordre de préséance) de la présente Annexe 4 ; et (iii) sur notification écrite, à collaborer avec Client pour prendre des mesures raisonnables et appropriées afin d'arrêter et de remédier à tout traitement non autorisé de données à caractère personnel.

2.3 Clauses contractuelles types de l'UE. Les Clauses contractuelles types de l'UE s'appliqueront aux données à caractère personnel qui sont transférées via les Services à partir de l'EEE, de la Suisse ou du Royaume-Uni, soit directement, soit par transfert ultérieur, vers tout pays ou destinataire en dehors de l'EEE, de la Suisse ou du Royaume-Uni qui n'est pas reconnu par l'autorité compétente concernée comme assurant un niveau de protection adéquat des données à caractère personnel. Pour les transferts de données soumis aux Clauses contractuelles types de l'UE, les Clauses contractuelles types de l'UE seront réputées conclues et incorporées au présent ATD par cette référence, et complétées comme suit :

(a) Module 1 (Responsable du traitement à Responsable du traitement) des Clauses Contractuelles types de l'UE s'appliquera lorsque (i) Trimble traite les données de compte client et (ii) Client est un responsable du traitement des données d'utilisation du client et Trimble traite les données d'utilisation du client ;

(b) Module 2 (Responsable du traitement à Sous-traitant) des Clauses contractuelles types de l'UE s'appliquera lorsque Client est un responsable du traitement des Données à caractère personnel et que Trimble traite les Données à caractère personnel au nom de Client ;

(c) Module 3 (Sous-traitant à Sous-traitant) des Clauses contractuelles types de l'UE s'appliquera lorsque Client est un sous-traitant des Données à caractère personnel et que Trimble les traite en tant que Sous-traitant ultérieur au nom de Client ; et

(d) Pour chaque module, le cas échéant :

(i) dans la Clause 7 des Clauses contractuelles types de l'UE, la clause d'adhésion facultatif ne s'applique pas ;

(ii) dans la clause 9 des Clauses contractuelles types de l'UE, l'option 2 s'appliquera et le délai de notification écrite préalable des changements de sous-traitants ultérieurs sera celui indiqué à la section 5.2 (Liste des Sous-traitants ultérieurs actuels et notification des nouveaux Sous-traitants ultérieurs) du présent ATD ;

(iii) dans la Clause 11 des Clauses contractuelles types de l'UE, la langue optionnelle ne s'applique pas ;

(iv) Identifier la ou les autorités de contrôle compétentes conformément à la clause 13 ;

(v) dans la Clause 17 (Option 1), les Clauses contractuelles types de l'UE seront régies par le droit belge ;

(vi) dans la Clause 18(b) des Clauses contractuelles types de l'UE, les litiges seront résolus devant les tribunaux d'Amsterdam, Pays-Bas ;

(vii) à l'Annexe I, partie A, des Clauses contractuelles types de l'UE :

Exportateur de données : Client (si la case à la page 6 est cochée).

Coordonnées : La(les) adresse(s) courriel désignée par Client dans son compte via ses préférences de notification.

Rôle de l'exportateur de données : Le rôle de l'Exportateur de données est décrit à la page 6.

Signature et date : En concluant l'Accord, l'Exportateur de données est réputé avoir signé les présentes Clauses contractuelles types de l'UE qui y sont incorporées, y compris leurs Annexes, à la date d'entrée en vigueur de l'Accord.

Importateur de données : Trimble Inc.

Coordonnées : Trimble Privacy Team - privacy@Trimble.com

Rôle de l'Importateur de données : Le rôle de l'Importateur de données est décrit à la page 6.

Signature et date : En concluant l'Accord, l'Importateur de données est réputé avoir signé les présentes Clauses contractuelles types de l'UE qui y sont incorporées, y compris leurs Annexes, à la date d'entrée en vigueur de l'Accord.

(viii) à l'Annexe I, partie B, des Clauses contractuelles types de l'UE :

Les catégories de personnes concernées sont décrites à la Section 1 de l'Annexe 1 (Description du traitement) du présent ATD.

Les données sensibles transférées sont décrites dans la Section 3 de l'Annexe 1 (Description du traitement) du présent ATD.

La fréquence du transfert est continue pendant toute la durée de l'Accord.

La nature du traitement figure dans la Section 5 de l'Annexe 1 (Description du traitement) du présent ATD.

La finalité du Traitement figure dans la Section 6 de l'Annexe 1 (Description du traitement) du présent ATD.

La durée de conservation des données à caractère personnel figure dans la Section 7 de l'Annexe 1 (Description du traitement) du présent ATD.

Pour les transferts aux Sous-traitants ultérieurs, l'objet, la nature et la durée du traitement sont indiqués à l'adresse https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center sous “Additional Resources” (Ressources supplémentaires) ("Sub-processor lists") (listes des sous-traitants ultérieurs).

(ix) dans l'Annexe I, Partie C des Clauses contractuelles types de l'UE : La cas échéant, la Commission néerlandaise de protection des données sera l'autorité de contrôle pricipale. Autrement, lorsqu'une entité Trimble résidant dans l'UE est l'exportateur de données, l'autorité de contrôle compétente est l'autorité de contrôle de l'État membre dans lequel l'entité Trimble réside. Lorsque Client est l'exportateur de données, l'autorité de contrôle compétente est l'autorité de contrôle de l'État membre dans lequel Client Trimble réside.

(x) Annexe 2 (Mesures de sécurité techniques et organisationnelles) du présent ATD constitue l'Annexe II des Clauses contractuelles types de l'UE.

2.4 Extension au Royaume-Uni du cadre de protection des données et de l'Addendum sur le transfert international de données. Client et Trimble conviennent que l'Extension au Royaume-Uni du cadre de protection des données s'appliquera, et en l'absence d'une telle extension, les Clauses contractuelles types de l'UE et l'Addendum sur le transfert international de Données du Royaume-Uni aux Clauses contractuelles types de la Commission européenne dans sa version la plus récente s'appliqueront aux données à caractère personnel qui sont transférées via les Services depuis le Royaume-Uni, soit directement, soit via un transfert ultérieur, vers tout pays ou destinataire en dehors du Royaume-Uni qui n'est pas reconnu par l'autorité réglementaire compétente du Royaume-Uni ou l'organisme gouvernemental du Royaume-Uni comme fournissant un niveau adéquat de protection pour les Données à caractère personnel. Pour les transferts de données en provenance du Royaume-Uni qui sont soumis aux Clauses contractuelles types de l'UE et à l'Addendum sur le transfert international de données du Royaume-Uni, les Clauses contractuelles types de l'UE seront réputées conclues et incorporées dans le présent ATD comme décrit à la Section 2.3 de la présente Annexe 4 et l'Addendum sur le transfert international de données du Royaume-Uni sera réputé conclu et incorporé dans le présent ATD par cette référence, et complété comme suit :

(a) Dans le tableau 1 de l'Addendum sur le transfert international de données du Royaume-Uni, les coordonnées et les informations de contact clés de Client et de Trimble figurent dans la Section 2.3 (e)(vii) de la présente Annexe 3 ;

(b) Dans le tableau 2 de l'Addendum sur le transfert international de données du Royaume-Uni, des informations sur la version des Clauses contractuelles types de l'UE et sur certaines clauses auxquelles l'Addendum sur le transfert international de données du Royaume-Uni est annexé figurent dans la Section 2.3 (Clauses contractuelles types de l'UE) de la présente Annexe 4 ;

(c) Dans le tableau 3 de l'Addendum sur le transfert international de données du Royaume-Uni :

(i) La liste des Parties figure dans la Section 2.3(e)(vii) de la présente Annexe 3.

(ii) La description du transfert figure à la Section 1 (Nature et finalité du traitement) de l'Annexe 1 (Description du traitement).

(iii) L'Annexe II se trouve dans l'Annexe 2 (Mesures de sécurité techniques et organisationnelles) du présent ATD.

(iv) La liste des Sous-traitants ultérieurs est indiquée à l'adresse https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center sous “Additional Resources” (Ressources supplémentaires) ("Sub-processor lists") (listes des sous-traitants ultérieurs) et

(d) Dans le tableau 4 de l'Addendum sur le transfert international de données du Royaume-Uni, l'importateur et l'exportateur peuvent tous deux mettre fin à l'Accord international de transfert de données du Royaume-Uni conformément aux dispositions de l'Addendum sur le transfert international de données du Royaume-Uni.

2.5 Clauses contractuelles types de la Turquie. Les Clauses contractuelles types de la Turquie s'appliqueront aux données à caractère personnel qui sont transférées via les Services à partir de la Turquie, soit directement, soit par transfert ultérieur, vers tout pays ou destinataire en dehors de la Turquie qui n'est pas reconnu par l'autorité compétente comme assurant un niveau de protection adéquat des données à caractère personnel. Pour les transferts de données soumis aux Clauses contractuelles types de la Turquie, les Clauses contractuelles types de la Turquie seront réputées conclues et incorporées au présent ATD par cette référence, et complétées comme suit :

Pour chaque module, le cas échéant :

(i) dans l'Article 8 du Contrat 2 et du Contrat 3 des Clauses contractuelles types de la Turquie, l'option 2 s'appliquera et le délai de notification écrite préalable des changements de Sous-traitants ultérieurs sera celui indiqué à la section 5.2 (Liste des Sous-traitants ultérieurs actuels et notification des nouveaux Sous-traitants ultérieurs) du présent ATD ;

(ii) Les parties conviennent que le client doit informer l'Autorité turque sur la protection des données à caractère personnel dans un délai de cinq (5) jours ouvrables pour l'informer de la conclusion des Clauses contractuelles types de la Turquie.

(iii) L'importateur de données sera : Trimble avec les adresses, le nom et le prénom, le titre et les informations de contact de Trimble et du signataire comme indiqué dans le présent ATD.

(iv) Signature et date : En concluant l'Accord, Trimble et l'Exportateur de données sont réputés avoir signé les présentes Clauses contractuelles types de la Turquie qui y sont incorporées, y compris leurs Annexes, à la date d'entrée en vigueur de l'Accord.

(v) Les informations prévues à l'Annexe I des Clauses contractuelles types de la Turquie sont indiquées dans l'Annexe 1 :

(vi) Annexe 2 (Mesures de sécurité techniques et organisationnelles) du présent ATD constitue l'Annexe II des Clauses contractuelles types de la Turquie.

(vii) La liste des Sous-traitants ultérieurs est indiquée à l'adresse https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center sous “Additional Resources” (Ressources supplémentaires) ("Sub-processor lists") (listes des sous-traitants ultérieurs).

2.6 Conflit. En cas de conflit ou d'incohérence entre les Clauses contractuelles types de l'UE, l'Accord de transfert international de données du Royaume-Uni ou les Clauses contractuelles types de la Turquie et toute autre disposition du présent ATD, y compris l'Annexe 4 (Mécanisme de transfert transfrontalier), l'Accord, les dispositions des Clauses contractuelles types de l'UE, de l'Addendum de transfert international de données du Royaume-Uni et les Clauses contractuelles types de la Turquie, selon le cas, prévaudront.