

ACCORDO SUL TRATTAMENTO DEI DATI

Il presente Accordo sul trattamento dei dati ("DPA") è l'accordo delle parti in merito al Trattamento dei dati personali e integra tutti i Contratti di licenza, Sottoscrizioni, Servizi o altri accordi scritti o elettronici (i "**Contratti**") tra Trimble e il Cliente per l'acquisto di servizi (incluso il Software as a Service, le applicazioni offline o mobili Trimble associate e il supporto, e definiti come "Servizi" o altrimenti nel Contratto o nei seguenti termini) nel corso dei quali Trimble riceve i dati personali dal Cliente.

Il Cliente sottoscrive il presente DPA (i) firmando o accettando in altro modo il Contratto, (ii) firmandolo per proprio conto e come richiesto dalle Leggi e dai Regolamenti applicabili in materia di protezione dei dati, in nome e per conto degli Affiliati autorizzati, se e nella misura in cui Trimble tratta i Dati personali. Ai soli fini del presente DPA, e salvo diversa indicazione, il termine "Cliente" include i Clienti e gli Affiliati autorizzati.

Nel corso della fornitura dei Servizi al Cliente ai sensi del Contratto, Trimble può elaborare i Dati personali per conto del Cliente e le Parti accettano di rispettare le seguenti disposizioni in relazione a qualsiasi Dato personale.

COME ESEGUIRE QUESTO DPA:

- I. Questo DPA è costituito: dal corpo principale del DPA e dagli allegati da 1 a 3
- II. È stato pre-firmato per conto di Trimble. Le Clausole contrattuali standard (come definite di seguito) sono incorporate per riferimento.
- III. Se il Cliente desidera completare questo DPA, il Cliente deve:
 - a. Completare le informazioni nella casella della firma e firmare le pagina 6.
 - b. Completare le informazioni come esportatore di dati alle pagina 6.
- IV. Inviare il DPA compilato e firmato a Trimble tramite e-mail, indicando il numero di account cliente dell'organizzazione (come indicato nella fattura Trimble applicabile), a privacy@trimble.com.

COME SI APPLICA QUESTO DPA:

- Se l'entità del Cliente che accetta il presente DPA è parte di un Contratto, il presente DPA è un'appendice di e fa parte di tale Contratto e l'entità Trimble che è parte del Contratto è parte del presente DPA.
- Se l'entità del Cliente che firma il presente DPA ha inviato un ordine che è stato accettato da Trimble o da uno dei suoi affiliati, ma non è parte del Contratto, il presente DPA è un'appendice a tale ordine (incluso qualsiasi ordine di rinnovo) e l'entità Trimble a cui è stato effettuato tale ordine è parte del presente DPA.
- Se l'entità del Cliente che firma il DPA ha acquistato i servizi Trimble tramite un rivenditore autorizzato Trimble, il Cliente deve indicarlo a pagina 6 e fornire un numero cliente rilasciato da Trimble o dal rivenditore o, in mancanza di esso, la conferma da parte del rivenditore che il Cliente è abbonato a un servizio Trimble. In questo caso, il presente DPA sarà considerato come un accordo diretto tra il Cliente e Trimble.
- Se l'entità o l'individuo che firma il presente DPA non è né parte di un ordine né di un Contratto e non è un cliente indiretto tramite un rivenditore, il presente DPA non è valido e non è legalmente vincolante. Tale entità deve richiedere che la sua entità affiliata che è parte dell'Accordo esegua il presente DPA, o richieda per iscritto di entrare a far parte dell'Accordo.

Il presente DPA non sostituisce alcun diritto comparabile o aggiuntivo relativo al Trattamento dei Dati del Cliente contenuto nel Contratto (incluso qualsiasi addendum esistente al Contratto sul trattamento dei dati).

TERMINI DI TRATTAMENTO DEI DATI

1. DEFINIZIONI

Per "**Affiliato**" si intende qualsiasi entità che direttamente o indirettamente controlla, è controllata da, o è sotto il controllo comune con l'entità in questione. "Controllo", ai fini della presente definizione, indica la proprietà o il controllo diretto o indiretto di oltre il 50% delle partecipazioni con diritto di voto dell'entità interessata.

Per "**Affiliato autorizzato**" si intende qualsiasi Affiliato del Cliente che (i) sia soggetto a una o più Leggi sulla protezione dei dati e (ii) sia autorizzato a utilizzare i Servizi ai sensi del Contratto tra il Cliente e Trimble, ma non abbia firmato il proprio ordine con Trimble e non sia un "Cliente" come definito nel Contratto.

Per "**CCPA**" si intende il California Consumer Privacy Act, Cal. Civ. Code § 1798.100 e seguenti, e la sua attuazione normativa.

Per "**Titolare**" si intende l'entità che determina le finalità e i mezzi del Trattamento dei Dati personali.

Per "**Cliente**" si intende l'entità che ha stipulato il Contratto, insieme ai suoi Affiliati (per tutto il tempo in cui rimangono Affiliati) che hanno sottoscritto i Moduli d'Ordine.

Per "**Dati del cliente**" si intende ciò che è definito nel Contratto come "Dati del cliente" o "Dati dell'utente".

Per "**Leggi e regolamenti sulla protezione dei dati**" si intendono tutte le leggi e i regolamenti, comprese le leggi e i regolamenti dell'Unione Europea, dello Spazio economico europeo e dei loro stati membri, della Svizzera e del Regno Unito, dei paesi elencati nell'Allegato 3 e di tutti gli altri paesi in cui il Cliente o un affiliato del Cliente ha sede, tutti applicabili al Trattamento dei dati personali ai sensi del Contratto.

Per "**Soggetto dei dati**" si intende l'individuo a cui si riferiscono i Dati personali.

Per "**Europa**" si intende l'Unione Europea (UE), lo Spazio Economico Europeo (SEE) e la Svizzera.

Per "**GDPR**" si intende il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio.

Per "**Dati personali**" si intende qualsiasi informazione relativa a (i) una persona identificata o identificabile e (ii) una persona giuridica identificata o identificabile (laddove tali informazioni siano protette in modo analogo ai dati personali o alle informazioni di identificazione personale ai sensi delle leggi e dei regolamenti applicabili in materia di protezione dei dati), a condizione che tali dati siano Dati del cliente.

Per "**Trattamento**" si intende qualsiasi operazione o insieme di operazioni eseguite sui Dati Personali, con o senza mezzi automatizzati, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la divulgazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, l'allineamento o la combinazione, la limitazione, il blocco, la cancellazione o la distruzione.

Per "**Responsabile dei dati**" si intende l'entità che elabora i dati personali su istruzione e per conto del Titolare del trattamento, incluso, a seconda dei casi, qualsiasi "fornitore di servizi" secondo la definizione del CCPA.

Per "**Autorità Pubblica**" si intende un'agenzia governativa o un'autorità preposta all'applicazione della legge, comprese le autorità giudiziarie.

Per "**Clausole contrattuali standard UE**" si intende un accordo stipulato da e tra (i) un'Affiliato Trimble e Trimble Inc. o (ii) un Cliente e Trimble Inc., ciascuno ai sensi della decisione di attuazione (UE) 2021/914.

Per "**Sub-responsabile del trattamento**" si intende qualsiasi Responsabile del trattamento incaricato da Trimble o da un membro del Gruppo Trimble.

Per "**Trimble**" si intende l'entità Trimble che è parte del presente DPA, come specificato nella sezione "MODALITÀ DI APPLICAZIONE DEL PRESENTE DPA" di cui sopra. Le entità di Trimble che agiscono in qualità di responsabili del trattamento sono: Trimble Inc., una società costituita nel Delaware, Trimble Europe B.V., una società registrata nei Paesi Bassi, Trimble International B.V., una società costituita nei Paesi Bassi, Trimble UK Ltd, una società costituita in Inghilterra e Galles, Trimble Maps, Ltd, una società costituita in Inghilterra e Galles, Trimble Technologies Ireland Ltd, una società costituita in Irlanda, Trimble France SAS, una società costituita in Francia, Trimble Solutions Sandvika AS, una società costituita in Norvegia, Trimble Finland Corporation, una società costituita in Finlandia, Trimble Forestry Europe Corporation, una società costituita in Finlandia, Lakefield eTechnologies Ltd, una società costituita in Irlanda, Trimble GmbH, una società costituita in Germania, o Trimble Germany GmbH, una società costituita in Germania, a seconda dei casi.

Per "**Gruppo Trimble**" si intendono Trimble e i suoi affiliati impegnati nel Trattamento dei Dati personali.

2. TRATTAMENTO DEI DATI PERSONALI

2.1 Ruoli delle parti. Le parti riconoscono e accettano che, per quanto riguarda il Trattamento dei Dati personali, il Cliente è il Titolare del trattamento, Trimble è un Responsabile del trattamento e che Trimble o i membri del Gruppo Trimble si avvarranno di Sub-responsabili del trattamento in conformità ai requisiti stabiliti nella Sezione 5 di seguito, a condizione che per il Trattamento dei Dati dell'Account del Cliente, Trimble sia il Titolare del trattamento.

2.2 Trattamento dei dati personali da parte del Cliente. Il Cliente dovrà, nell'utilizzo dei Servizi, trattare i Dati personali in conformità con i requisiti delle Leggi e dei Regolamenti sulla protezione dei dati. A scanso di equivoci, le istruzioni del Cliente per il trattamento dei dati personali devono essere conformi alle leggi e ai regolamenti sulla protezione dei dati. Il Cliente sarà l'unico responsabile dell'accuratezza, della qualità e della legalità dei Dati personali e dei mezzi con cui il Cliente ha acquisito i Dati personali. Trimble informerà immediatamente il Cliente se, a suo avviso, un'istruzione viola le leggi e i regolamenti sulla protezione dei dati o altre disposizioni di legge.

2.3 Trattamento dei dati personali da parte di Trimble. Trimble elaborerà i Dati personali solo per conto e in conformità con le istruzioni del Cliente, anche per quanto riguarda i trasferimenti di Dati personali a un paese terzo o a un'organizzazione internazionale. Il Cliente richiede a Trimble di elaborare i Dati personali per le seguenti finalità: (i) Trattamento in conformità al Contratto e agli ordini applicabili; (ii) Trattamento avviato dagli utenti nell'utilizzo dei Servizi; (iii) Trattamento per conformarsi ad altre ragionevoli istruzioni fornite dal Cliente, laddove tali istruzioni siano coerenti con i termini del Contratto; e (iv) il trattamento ai fini dell'anonimizzazione in conformità con le Clausole di utilizzo dei dati nell'Accordo (e incluso nell'Allegato 1).

TRIMBLE NON AGISCE IN QUALITÀ DI RESPONSABILE PER I SEGUENTI DATI PERSONALI: Dati di accesso e di contatto dell'utente, dati sull'utilizzo del software e dati generati da misure di sicurezza ("dati dell'account cliente").

2.4 Ambito e finalità; Categorie di dati personali e soggetti. L'oggetto del Trattamento dei Dati personali da parte di Trimble è l'esecuzione dei Servizi ai sensi del Contratto. I tipi di Dati personali e le categorie di soggetti interessati trattati ai sensi del presente DPA sono ulteriormente specificati nell'Allegato 1 (Descrizione del trattamento) del presente DPA.

3. DIRITTI DEI SOGGETTI INTERESSATI

3.1 Diritti dell'interessato. Tenendo conto della natura del Trattamento, Trimble assiste il Cliente fornendo misure tecniche e organizzative adeguate, per quanto possibile, per l'adempimento dell'obbligo del Cliente di rispondere alle richieste degli Interessati per l'esercizio dei propri diritti ai sensi delle Leggi e dei Regolamenti sulla protezione dei dati. Nella misura in cui il Cliente, nell'utilizzo dei Servizi, non abbia la possibilità di esercitare tali diritti, Trimble soddisferà qualsiasi richiesta commercialmente ragionevole del Cliente di facilitare tali azioni nella misura in cui Trimble sia legalmente autorizzata a farlo. Nella misura consentita dalla legge, il Cliente sarà responsabile di tutti i costi derivanti dalla fornitura di tale assistenza da parte di Trimble.

3.2 Richieste dirette dei soggetti interessati. Nella misura consentita dalla legge, Trimble informerà tempestivamente il Cliente qualora riceva una richiesta da parte dell'interessato per l'esercizio dei propri diritti di interessato ai sensi della Sezione 3.1. Trimble non risponderà a tali richieste dell'interessato senza il previo consenso del Cliente in forma scritta, salvo per confermare che la richiesta si riferisce al Cliente e che il Cliente accetta con il presente documento.

4. TRIMBLE E IL PERSONALE DEL CLIENTE

4.1 Generale. Trimble e il Cliente adotteranno misure per garantire che qualsiasi persona fisica che agisca sotto la rispettiva autorità e che abbia accesso ai Dati del Cliente non elabori i Dati del Cliente se non su istruzione del Cliente, a meno che non sia richiesto dalle Leggi e dai Regolamenti sulla protezione dei dati.

4.2 Riservatezza. Trimble garantirà che il proprio personale addetto al Trattamento dei Dati Personali sia informato della natura riservata dei Dati Personali, abbia ricevuto un'adeguata formazione sulle proprie responsabilità e abbia rispettato gli impegni scritti di riservatezza. Trimble garantirà che tali obblighi di riservatezza sopravvivano alla cessazione del rapporto di lavoro.

4.3 Affidabilità. Trimble adotterà misure commercialmente ragionevoli per garantire l'affidabilità di qualsiasi personale di Trimble coinvolto nel Trattamento dei Dati personali.

4.4 Limitazione dell'accesso. Trimble garantirà che l'accesso del personale ai Dati personali sia limitato al personale che esegue i Servizi in conformità al Contratto.

5. SUB-RESPONSABILI DEL TRATTAMENTO

5.1 Nomina di Sub-responsabili del trattamento. Il Cliente riconosce e accetta che (i) gli affiliati di Trimble possono essere mantenuti come Sub-responsabili del trattamento; e (ii) Trimble e gli Affiliati di Trimble possono rispettivamente avvalersi di Sub-responsabili del trattamento di terze parti in relazione alla fornitura dei Servizi. In tal caso, Trimble e gli affiliati di Trimble imporranno a qualsiasi Sub-responsabile del trattamento obblighi di protezione dei dati sostanzialmente simili a quelli stabiliti nel presente DPA mediante contratto o altro atto giuridico. Il contratto o altro atto giuridico deve contenere garanzie sufficienti che qualsiasi Sub-responsabile del trattamento implementi misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti delle Leggi e dei Regolamenti sulla protezione dei dati.

5.2 Elenco degli attuali Sub-responsabili del trattamento e notifica di nuovi Sub-responsabili del trattamento. L'elenco aggiornato dei Sub-responsabili del trattamento dei Dati personali per l'esecuzione di ciascun Servizio applicabile, inclusa una descrizione delle loro attività di trattamento e dei paesi di ubicazione, è riportato in <https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center> sotto "Risorse aggiuntive" ("Elenco Sub-responsabili"). Il Cliente acconsente a tali Sub-responsabili

del trattamento, alla loro ubicazione e alle attività di trattamento relative ai loro Dati personali e istruisce Trimble di conseguenza. Trimble informerà in merito alle modifiche apportate ai sub-responsabili del trattamento nelle note di rilascio, negli aggiornamenti dei clienti o in comunicazioni analoghe, che saranno considerate comunicazioni ai fini della [Sezione 9.2 delle Clausole contrattuali standard dell'UE].

5.3 Diritto di opposizione per i nuovi sub-responsabili del trattamento. Al fine di esercitare il proprio diritto di opporsi all'utilizzo da parte di Trimble di un nuovo Sub-responsabile del trattamento, il Cliente dovrà informare tempestivamente Trimble in forma scritta inviata a privacy@trimble.com entro trenta (30) giorni lavorativi dal ricevimento della notifica di Trimble in conformità con il meccanismo stabilito nella Sezione 5.2. Nel caso in cui il Cliente si opponga a un nuovo Sub-responsabile del trattamento e tale obiezione non sia irragionevole, Trimble compirà ogni ragionevole sforzo per rendere disponibile al Cliente una modifica dei Servizi o raccomandare una modifica commercialmente ragionevole alla configurazione o all'utilizzo dei Servizi da parte del Cliente per evitare il Trattamento dei Dati personali da parte del nuovo Sub-responsabile del trattamento contestato senza gravare irragionevolmente sul Cliente. Se Trimble non è in grado di rendere disponibile tale modifica entro un periodo di tempo ragionevole, che non deve superare i sessanta (60) giorni, il Cliente può risolvere gli ordini e i Contratti applicabili solo in relazione a quei Servizi che non possono essere forniti da Trimble senza l'utilizzo del nuovo Sub-responsabile contestato fornendo una comunicazione scritta a Trimble. Trimble rimborserà al Cliente eventuali tariffe prepagate che coprono il resto della durata di tali ordini successivi alla data effettiva di risoluzione in relazione a tali Servizi terminati.

5.4 Responsabilità. Trimble sarà responsabile per gli atti e le omissioni dei suoi Sub-responsabili del trattamento nella stessa misura in cui Trimble sarebbe responsabile se eseguisse i servizi di ciascun Sub-responsabile del trattamento direttamente ai sensi dei termini del presente DPA, salvo quanto diversamente stabilito nel Contratto.

6. SICUREZZA, AUDIT E ASSISTENZA

6.1 Sicurezza del trattamento. Trimble adotterà misure di sicurezza amministrative, fisiche e tecniche per la protezione della sicurezza, della riservatezza e dell'integrità dei Dati del Cliente, inclusi i Dati personali, come indicato nell'Allegato 1. Trimble monitora regolarmente il rispetto di queste misure di sicurezza. Trimble non ridurrà in modo sostanziale la sicurezza complessiva dei Servizi durante il periodo di validità del Contratto.

6.2 Audit. Trimble esegue di volta in volta audit e ispezioni (incluse, se ragionevoli, audit da parte di revisori esterni) per garantire la conformità alle Leggi sulla protezione dei dati e al presente DPA, nonché laddove ragionevole con gli standard di settore come ISO 27001. Trimble metterà a disposizione del Cliente, su richiesta, tutte le informazioni necessarie (inclusi tali rapporti di audit) per dimostrare la conformità agli obblighi derivanti dalla Legge sulla protezione dei dati applicabile e dal presente DPA. A seconda delle informazioni richieste, Trimble può richiedere al Cliente di firmare un NDA.

6.3 Assistenza al Cliente. Trimble assisterà il Cliente nel garantire il rispetto degli obblighi in materia di sicurezza del Trattamento, notifica e comunicazione delle violazioni dei Dati personali, valutazioni d'impatto sulla protezione dei dati e consultazioni preliminari con l'autorità di vigilanza ai sensi delle Leggi e dei Regolamenti sulla protezione dei dati.

6.4 Gestione e notifica delle violazioni della sicurezza. In caso di violazione dei Dati personali ai sensi delle Leggi e dei Regolamenti sulla protezione dei dati, Trimble adotta politiche e procedure di gestione degli incidenti di sicurezza e, nella misura consentita dalla legge, informerà il Cliente di tale violazione senza indebito ritardo.

7. RESTITUZIONE E CANCELLAZIONE DEI DATI DEI CLIENTI

Trimble, al termine della fornitura dei Servizi, a scelta del Cliente, restituirà i Dati del Cliente al Cliente e/o cancellerà i Dati del Cliente in conformità con le procedure e i tempi specificati nel Contratto o nella relativa descrizione del Servizio, a meno che la legislazione imposta al Cliente non richieda la conservazione dei Dati del Cliente.

8. RICHIESTE DI ACCESSO DA PARTE DEL GOVERNO

8.1 Salvo quanto vietato dalla legge applicabile, Trimble informerà il Cliente in termini generali in merito a richieste, ordini o richieste simili da parte di un tribunale, di un'autorità competente, di forze dell'ordine o di altri enti governativi ("Richiesta di applicazione della legge") relativi al trattamento dei dati personali ai sensi delle presenti Clausole.

8.2 Trimble obietterà e contesterà qualsiasi richiesta delle forze dell'ordine adottando rimedi legali nella misura in cui siano ragionevoli date le circostanze. Se obbligata a divulgare i dati personali trasferiti ai sensi delle presenti Clausole da una richiesta delle forze dell'ordine, Trimble, a meno che non sia vietato dalla legge

applicabile, fornirà al Cliente un preavviso ragionevole per consentirgli di richiedere un'ordinanza cautelare o un altro rimedio appropriato, a meno che non sia legalmente vietato a Trimble di farlo.

8.3 Nel caso in cui Trimble renda disponibili i dati personali ai sub-responsabili del trattamento, Trimble selezionerà i sub-responsabili del trattamento in un paese al di fuori dello Spazio economico europeo che non è soggetto a un accertamento di adeguatezza da parte della Commissione dell'Unione europea, solo dopo una due diligence che comporta (i) una revisione di eventuali rapporti sulla trasparenza resi disponibili dai sub-responsabili del trattamento, (ii) e l'esecuzione di una valutazione del rischio di trasferimento.

9. AFFILIATI AUTORIZZATI

9.1 Rapporto contrattuale. Il Cliente sottoscrive il DPA per l'approvazione delle informazioni personali per proprio conto e, a seconda dei casi, in nome e per conto degli Affiliati autorizzati, stabilendo in tal modo un'Autorità per le garanzie dei dati separata tra Trimble e ciascuno di tali Affiliati autorizzati. Ciascun Affiliato autorizzato è vincolato dagli obblighi previsti dal presente DPA. A scanso di equivoci, un Affiliato autorizzato non è e non diventa parte del Contratto, ma è solo una parte del DPA. Tutti gli accessi e l'utilizzo dei Servizi da parte degli Affiliati autorizzati devono essere conformi ai termini e alle condizioni dell'Accordo e qualsiasi violazione dei termini e delle condizioni dell'Accordo da parte di un Affiliato autorizzato sarà considerata una violazione da parte del Cliente.

9.2 Comunicazione. Il Cliente che è la parte contraente del Contratto rimarrà responsabile del coordinamento di tutte le comunicazioni con Trimble ai sensi del presente DPA e avrà il diritto di effettuare e ricevere qualsiasi comunicazione in relazione al presente DPA per conto dei suoi Affiliati autorizzati.

9.3 Diritti degli affiliati autorizzati. Nel caso in cui un affiliato autorizzato diventi parte del DPA con Trimble, nella misura richiesta dalle Leggi e dai Regolamenti applicabili in materia di protezione dei dati, avrà il diritto di esercitare i diritti e di cercare rimedi ai sensi del presente DPA. Se le leggi e i regolamenti sulla protezione dei dati richiedono all'Affiliato autorizzato di esercitare un diritto o di cercare qualsiasi rimedio ai sensi del presente DPA in qualità di Titolare del trattamento, l'Affiliato autorizzato autorizza il Cliente a esercitare tale diritto al posto dell'Affiliato autorizzato. Inoltre, il Cliente che è la parte contraente del contratto eserciterà tali diritti ai sensi del presente DPA non separatamente per ciascun Affiliato autorizzato individualmente, ma in modo combinato per tutti i suoi Affiliati autorizzati insieme.

10. Limitazione di responsabilità

La responsabilità di ciascuna parte e dei suoi affiliati derivante da o correlata al presente DPA e a tutti i DPA tra gli affiliati autorizzati e Trimble, sia per contratto, illecito civile o in base a qualsiasi altra teoria di responsabilità, è soggetta alla sezione "Limitazione di responsabilità" del Contratto e qualsiasi riferimento in tale sezione alla responsabilità di una parte indica la responsabilità complessiva di tale parte e dei suoi affiliati ai sensi del Contratto e di tutti i DPA nel loro insieme. A scanso di equivoci, la responsabilità totale di Trimble e dei suoi affiliati per tutte le rivendicazioni del Cliente e dei suoi affiliati autorizzati derivanti da o correlate al Contratto e a ciascun DPA si applicherà in aggregato a tutti i reclami ai sensi del Contratto e di tutti i DPA stabiliti ai sensi di tale Contratto, anche da parte di qualsiasi affiliato autorizzato e, in particolare, non deve essere inteso come applicabile individualmente e separatamente a ciascun affiliato autorizzato che è parte contrattuale di tale DPA. A scanso di equivoci, ogni riferimento al DPA nel presente DPA indica il presente DPA, inclusi i suoi Allegati e Appendici.

Se il Cliente ha sottoscritto o acquistato i Servizi tramite un rivenditore o un altro partner commerciale di Trimble, la responsabilità di Trimble e dei suoi Affiliati derivante da o correlata al presente DPA e a tutti i DPA tra gli affiliati autorizzati e Trimble, sia per contratto, illecito o in base a qualsiasi altra teoria di responsabilità, sarà limitata, nella misura consentita dalla legge, in aggregato al maggiore tra gli importi ricevuti da Trimble per tali Servizi o EUR 50.000.

11. DISPOSIZIONI INTERNAZIONALI

11.1 Meccanismo di trasferimento transfrontaliero. Nella misura in cui Trimble elabora dati personali provenienti da e protetti dalle Leggi e dai Regolamenti in materia di protezione dei dati in una delle giurisdizioni elencate nell'Allegato 3 (Meccanismo di trasferimento transfrontaliero) del presente DPA, si applicano i termini specificati nell'Allegato 3 in relazione alle giurisdizioni applicabili, in aggiunta ai termini del presente DPA.

11.2 Meccanismi di trasferimento transfrontaliero dei dati. Nella misura in cui l'utilizzo dei Servizi da parte del Cliente richieda un meccanismo di trasferimento successivo per trasferire legalmente i Dati personali da una giurisdizione (ad esempio, lo Spazio economico europeo, il Regno Unito, la Svizzera, la Turchia o un'altra giurisdizione elencata nell'Allegato 3 (Meccanismo di trasferimento transfrontaliero) del presente DPA) a Trimble situata al di fuori di tale giurisdizione ("Meccanismo di trasferimento"), si applicheranno i termini stabiliti nell'Allegato 4 (Meccanismi di trasferimento transfrontaliero) del presente DPA.

12. Miscellanea

12.1 Conflitto. In caso di conflitto o incoerenza tra i seguenti documenti, l'ordine di precedenza sarà: (1) i termini applicabili stabiliti nell'Allegato 4 (Meccanismo di trasferimento transfrontaliero) del presente DPA; (2) i termini del presente DPA al di fuori dell'Allegato 4 (Meccanismo di trasferimento transfrontaliero); e (3) il contratto.

12.2 Aggiornamenti. Trimble si riserva il diritto di aggiornare periodicamente i termini del presente DPA, a condizione tuttavia che fornisca al Cliente un preavviso scritto di almeno trenta (30) giorni qualora sia necessario un aggiornamento a seguito di (a) modifiche alle Leggi e ai Regolamenti in materia di protezione dei dati; (b) una fusione, un'acquisizione o un'altra transazione simile; o (c) il rilascio di nuovi prodotti o servizi o modifiche sostanziali a uno qualsiasi dei Servizi esistenti. I termini in vigore al momento del presente DPA sono disponibili all'indirizzo trimble.com/privacy

Nome legale del cliente: _____

Indirizzo _____

Numero cliente Trimble: _____

☐ Il Cliente ha acquistato i Servizi tramite il
Rivenditore autorizzato o il Business Partner di
Trimble
Nome Rivenditore _____
Indirizzo _____
Numero cliente rivenditore _____

☐ Per la fatturazione ai clienti in UE/SEE/UK. Il Cliente desidera stipulare le Clausole contrattuali standard dell'UE direttamente con Trimble Inc. Se questa casella non è selezionata, il meccanismo di trasferimento per il trasferimento a Trimble Inc. è quello descritto nella Sezione 2.2 dell'Allegato 4 o in qualsiasi altro meccanismo di trasferimento stabilito tra l'Affiliato di Trimble in Europa e Trimble Inc.

Se la casella precedente è selezionata: il Cliente considera applicabili i seguenti Moduli:

☐ Modulo 1/Contratto 1 ☐ Modulo 2/Contratto 2 ☐ Modulo 3/Contratto 3

☐ Il Cliente sceglie di sottoscrivere il presente DPA

I firmatari autorizzati delle parti hanno debitamente sottoscritto il presente Contratto

CLIENTE (firma il presente DPA)

Nome: _____

Titolo _____

Data: _____

Trimble Inc.

Firma: _____
Stampa nome: Jennifer Allison
Titolo: Vicepresidente senior e Consigliere generale
Data: 15.7.2024

Trimble Europe BV

Firma: _____
Nome in stampatello: RHH Reeder
Titolo: Direttore
Data: 15.7.2024

Trimble UK Limited

Firma: _____
Nome in stampatello: RHH Reeder
Titolo: Direttore
Data: 15.7.2024

Trimble France SAS

Firma: _____
Nome in stampatello: RHH Reeder
Titolo: Direttore
Data: 15.7.2024

Trimble Solutions Sandvika AS

Firma: _____
 Nome in stampatello: RHH Reeder
 Titolo: Direttore
 Data: 15.7.2024

Trimble Technologies Ireland Limited

Firma: _____
 Nome in stampatello: RHH Reeder
 Titolo: Direttore
 Data: 15.7.2024

Lakefield eTechnologies Limited

Firma: _____
 Nome in stampatello: RHH Reeder
 Titolo: Direttore
 Data: 15.7.2024

Trimble International BV

Firma: _____
 Nome in stampatello: RHH Reeder
 Titolo: Direttore
 Data: 15.7.2024

Trimble Finland Corporation

Firma: _____
 Stampa nome: Jürgen Kesper
 Titolo: Direttore
 Data: 15.7.2024

Trimble Germany GmbH

Firma: _____
 Nome in stampatello: RHH Reeder
 Titolo: Direttore
 Data: 15.7.2024

Trimble MAPS Limited.

Firma: _____
 Nome in stampatello: RHH Reeder
 Titolo: Direttore
 Data: 15.7.2024

Trimble Forestry Europe Corporation

Firma: _____
 Nome in stampatello: RHH Reeder
 Titolo: Direttore
 Data: 15.7.2024

Trimble GmbH

Firma: _____
 Stampa nome: Jürgen Kesper
 Titolo: Direttore
 Data: 15.7.2024

Dati di contatto per tutte le entità Trimble:

privacy@trimble.com

Indirizzi Trimble Entities	
Trimble Inc.	Trimble Europe B.V.
10368 Westmoor Drive Westminster, CO 80021, USA	Industrieweg 187a 5683CC Best, Paesi Bassi
Trimble UK Limited	Trimble France SAS
Trimble House, Gelderd Road, Gildersome, Leeds LS27 7JP Regno Unito	1 Quai Gabriel Péri 94340 Joinville-le-Pont, Francia
Trimble Solutions Sandvika AS	Trimble Technologies Ireland Limited

Leif Tronstads plass 4 1337 Sandvika, Norvegia	North Point Business Park, Unit 3d North Point House, New Mallow Rd, Cork, T23 AT2P, Irlanda
Lakefield eTechnologies Limited	Trimble International BV
North Point Business Park, Unit 3d North Point House, New Mallow Rd, Cork, T23 AT2P, Irlanda	Industrieweg 187a 5683CC Best, Paesi Bassi
Trimble Finland Corporation	Trimble Germany GmbH
Hatsinanpuisto 8, 02600 Espoo, Finlandia	Am Prime Parc 11, 65479 Raunheim
Trimble MAPS Limited.	Trimble Forestry Europe Corporation
53-64 Chancery Lane, Holborn, Londra Inghilterra WC2A 1QS Regno Unito	Hatsinanpuisto 8, 02600 Espoo, Finlandia
Trimble GmbH	
Am Prime Parc 11, 65479 Raunheim	

ALLEGATO 1 - DESCRIZIONE DEL TRATTAMENTO

1. CATEGORIE DI SOGGETTI INTERESSATI I CUI DATI PERSONALI VENGONO TRASFERITI

Il Cliente può inviare Dati personali ai Servizi, la cui portata è determinata e controllata dal Cliente a sua esclusiva discrezione e che possono includere, a titolo esemplificativo ma non esaustivo, Dati personali relativi alle seguenti categorie di soggetti interessati:

- Dipendenti, funzionari, direttori e collaboratori del Cliente
- Clienti del Cliente (che sono persone fisiche), spesso nella loro qualità di destinatari di spedizioni, servizi e prodotti
- Dipendenti, agenti, consulenti, liberi professionisti dei clienti del Cliente, fornitori e controparti delle transazioni elaborate attraverso i Servizi
- Utenti del Cliente autorizzati dal Cliente a utilizzare i Servizi

2. CATEGORIE DI DATI PERSONALI TRASFERITI

Il Cliente può inviare Dati personali ai Servizi, la cui portata è determinata e controllata dal Cliente a sua esclusiva discrezione e che possono includere, a titolo esemplificativo ma non esaustivo, le seguenti categorie di Dati personali:

- Dati di contatto e anagrafici (Nome e cognome, Titolo, Posizione)
- Informazioni di contatto (azienda, e-mail, telefono, indirizzo fisico dell'azienda)
- Dati identificativi come passaporti, patenti di guida, indirizzi IP, identificatori univoci (UUID)
- Dati occupazionali e formativi (qualifiche, esperienze, competenze)
- Dati relativi al lavoro (servizi resi, contributi al progetto, lavori e compiti assegnati, dati relativi alle prestazioni, ore di servizio, spese)
- Dati di localizzazione
- Dati relativi al contratto (fatturazione, pagamento, cronologia delle transazioni)
- Cronologia delle interazioni

3. DATI SENSIBILI TRASFERITI (SE APPLICABILE)

Dati sensibili trasferiti (se applicabile) e restrizioni o garanzie applicate che tengono pienamente conto della natura dei dati e dei rischi connessi, come ad esempio una rigorosa limitazione delle finalità, restrizioni di accesso (compreso l'accesso solo per il personale che ha seguito una formazione specializzata), tenuta di un registro degli accessi ai dati, restrizioni per i trasferimenti successivi o misure di sicurezza aggiuntive:

L'esportatore dei dati può inviare ai Servizi categorie speciali di dati, la cui portata è determinata e controllata dall'esportatore dei dati a sua esclusiva discrezione e che, per motivi di chiarezza, sono Dati personali con informazioni che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale e l'elaborazione di dati genetici, dati biometrici allo scopo di identificare in modo univoco una persona fisica, dati relativi alla salute o dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica.

Le misure di sicurezza applicabili sono descritte nella Sezione 11 dell'Allegato 2 di seguito.

4. FREQUENZA DEL TRASFERIMENTO

La frequenza del trasferimento (ad es. indipendentemente dal fatto che i dati siano trasferiti una tantum o continuativamente):

Su base continuativa a seconda dell'utilizzo dei Servizi da parte del Cliente.

5. NATURA DEL TRATTAMENTO

La natura del Trattamento è l'esecuzione dei Servizi ai sensi del Contratto.

6. FINALITÀ DEL TRATTAMENTO, TRASFERIMENTO DEI DATI E ULTERIORE TRATTAMENTO

Trimble tratterà i Dati personali nella misura necessaria per l'esecuzione dei Servizi ai sensi del Contratto, come ulteriormente specificato nella Documentazione e come ulteriormente indicato dal Cliente nell'utilizzo dei Servizi. Trimble renderà ulteriormente anonimi i Dati personali al fine di condurre analisi dei dati e sviluppo dei servizi.

7. DURATA DEL TRATTAMENTO

Il periodo per il quale i Dati Personali saranno conservati o, se ciò non è possibile, i criteri utilizzati per determinare tale periodo:

Trimble tratterà i Dati personali come stabilito nel Contratto, salvo diverso accordo, ad esempio nella Sezione 9 del DPA.

8. TRASFERIMENTI A SUB-RESPONSABILI DEL TRATTAMENTO

Per i trasferimenti a (Sub-) responsabili del trattamento, specificare anche l'oggetto, la natura e la durata del trattamento:

Il sub-responsabile del trattamento tratterà i Dati personali nella misura necessaria per eseguire i Servizi ai sensi del contratto. Fatta salva la Sezione 9 del presente DPA, il Sub-responsabile del trattamento tratterà i Dati personali per la durata del contratto, salvo diverso accordo scritto.

Le identità dei Sub-responsabili del trattamento utilizzati per la fornitura dei Servizi e il loro paese di ubicazione sono elencati nella scheda Materiali aggiuntivi di trimble.com/privacy.

ALLEGATO 2 - Misure di sicurezza tecniche e organizzative

Ove applicabile, il presente Allegato 2 fungerà anche da Allegato II alle Clausole contrattuali standard dell'UE.

ALLEGATO 2 - Misure di sicurezza tecniche e organizzative

1. Misure di pseudo-anonimizzazione e crittografia dei dati personali

Ove possibile, Trimble crittografa i dati trasmessi tra i clienti e l'applicazione Trimble su reti pubbliche utilizzando TLS 1.2 o versioni successive. I dati dei clienti memorizzati sui sistemi gestiti da Trimble (per i prodotti certificati AICPA - vedere il punto 7 di seguito per ulteriori informazioni) sono crittografati utilizzando crittografie AES 256 o superiori.

2. Misure volte a garantire la riservatezza, l'integrità, la disponibilità e la resilienza costanti dei sistemi e dei servizi di trattamento

Trimble dispone di personale dedicato alla sicurezza informatica responsabile della supervisione della sicurezza e della privacy. Ha nominato la leadership per la sicurezza informatica e la privacy, oltre a un ufficio per la protezione dei dati, insieme a un Engineering Leadership Council che si riunisce trimestralmente per discutere i rischi per la privacy e la sicurezza gestiti all'interno dei portafogli di prodotti del settore. Inoltre, il rischio del prodotto viene monitorato in un portale interno con monitoraggio della conformità eseguito mensilmente.

3. Misure volte a garantire la capacità di ripristinare la disponibilità e l'accesso ai dati personali in modo tempestivo in caso di incidente fisico o tecnico

Al fine di supportare la disponibilità dei prodotti SaaS di Trimble, Trimble si avvale di fornitori di servizi cloud leader del settore (Amazon Web Services (AWS) e Microsoft Azure) per la scalabilità automatica, data center geograficamente diversificati, un ampio monitoraggio delle applicazioni e dell'infrastruttura e meccanismi di supporto 24 ore su 24, 7 giorni su 7.

Trimble mantiene backup degli archivi dati, inclusi i dati dei clienti, che supportano le funzionalità primarie delle applicazioni Trimble. I backup vengono archiviati in una posizione geograficamente separata dalla posizione di archiviazione dei dati primaria, ove possibile.

Oltre alle misure dei propri fornitori di servizi, Trimble mantiene una funzione di risposta agli incidenti di sicurezza che include una Politica di risposta agli incidenti documentata e un piano di valutazione degli eventi di sicurezza e degli incidenti che coinvolgono i Dati del Cliente. Questo definisce il protocollo di risposta come il contenimento, l'eliminazione, il ripristino e le attività di comunicazione per gli incidenti di sicurezza, nonché i ruoli e le responsabilità del personale Trimble e un requisito per le revisioni post-incidente con la gestione di Trimble.

4. Processi per testare, valutare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Trimble si avvale di terze parti indipendenti per condurre test di penetrazione periodici, tra cui audit Sarbanes-Oxley, PCI, SOC 1, Type II, SOC 2 Type II, ISO27001 o NIST 800-171 equivalenti su base annuale, ove richiesto per la conformità normativa. Inoltre, Trimble conduce regolarmente test interni di vulnerabilità e test di penetrazione su prodotti e piattaforme applicabili in combinazione con il programma di sicurezza informatica e i requisiti delle politiche di Trimble. Trimble può effettuare valutazioni di nuovi fornitori o partner se il rischio aziendale richiede una revisione. Trimble incoraggia le terze parti a segnalare eventuali problemi di sicurezza informatica, incidenti e vulnerabilità associati ai propri prodotti, servizi o siti Web.

5. Misure per l'identificazione e l'autorizzazione degli utenti

Per i prodotti che utilizzano l'ID Trimble (TID, Trimble Identity) per l'autenticazione, Trimble elabora la password in modo sicuro. Inoltre, alcuni prodotti Trimble possono supportare l'integrazione Single Sign On (SSO) con un provider di identità del cliente utilizzando SAML (Security Assertion Markup Language) e MFA (Autenticazione Multifattore).

6. Misure per la protezione dei dati durante la trasmissione

Come indicato al punto 1, Trimble crittografa i Dati del Cliente trasmessi su reti pubbliche tra i clienti e l'applicazione Trimble utilizzando cifrari di crittografia attuali ogniqualevolta possibile.

7. Misure per la protezione dei dati durante la conservazione

Come indicato al punto 1, i dati del cliente conservati nell'archivio dati gestito da Trimble sono crittografati utilizzando AES 256 o superiore per tutti i prodotti Trimble attualmente certificati AICPA SOC 1, Tipo II, SOC 2, Tipo II o NIST 800-171. Fare riferimento al punto 11 per informazioni più dettagliate.

8. Misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati

I prodotti, le applicazioni e i servizi SaaS di Trimble sono in genere ospitati con i Dati dei clienti archiviati all'interno di data center forniti da Amazon Web Services (AWS), Microsoft Azure o Google Cloud Platform (GCP). Pertanto, Trimble si affida ai controlli fisici, ambientali e infrastrutturali di queste piattaforme. Trimble esamina periodicamente le certificazioni e le attestazioni di terze parti fornite da questi fornitori in merito all'efficacia dei controlli dei loro data center.

9. Misure per garantire la registrazione degli eventi

Trimble conserva molti registri degli strumenti di sicurezza informatica e registri di controllo della sicurezza delle applicazioni e delle infrastrutture. I registri di sicurezza vengono analizzati utilizzando la tecnologia SIEM in combinazione con la correlazione degli eventi per rilevare attività anomale.

10. Misure per garantire la configurazione del sistema, compresa la configurazione standard

Trimble sfrutta gli standard comuni del settore per rafforzare la sicurezza informatica attraverso una configurazione sicura e una difesa approfondita. Trimble applica patch di sicurezza ai propri sistemi in conformità con la Trimble Secure Development Lifecycle Policy (TSDLCP).

11. Misure per la governance e la gestione interna dell'informatica e della sicurezza informatica

Per i prodotti Trimble certificati SOC 1, Tipo II, SOC 2, Tipo II o NIST 800-171, il personale con accesso ai dati dei clienti sfrutta i principi basati sui ruoli e sui privilegi minimi per il controllo degli accessi. Al personale viene fornito un accesso sufficiente ai dati dei clienti solo per poter svolgere le proprie mansioni lavorative in modo sicuro. L'accesso remoto alla rete dei sistemi Trimble richiede una comunicazione crittografata tramite protocolli protetti e l'uso dell'autenticazione a più fattori. Trimble ha stabilito e manterrà procedure per la gestione delle password per questa fascia demografica del personale, progettate per garantire che le password siano uniche per ogni individuo e inaccessibili a persone non autorizzate, tra cui, come minimo:

- proteggere crittograficamente le password quando memorizzate in sistemi informatici o in transito su qualsiasi rete pubblica;
- modificare le password predefinite dei fornitori; e
- formazione sulle buone pratiche per le password, come l'uso di passphrase
- l'accesso del personale all'infrastruttura di produzione richiede l'autenticazione a più fattori (MFA).

Per garantire la conformità al certificato ISO 27001 e per garantire un uso corretto ed efficace della crittografia per proteggere la riservatezza e l'integrità dei dati posseduti o gestiti dalle divisioni Trimble In-Scope, i dati classificati come riservati o ristretti devono essere crittografati mediante l'uso di processi di crittografia validi per i dati inattivi e in movimento, come richiesto dalle normative e/o dalla valutazione del rischio. Ciò include, a titolo esemplificativo ma non esaustivo, le informazioni sensibili memorizzate su dispositivi mobili, unità rimovibili e computer portatili. Le divisioni Trimble In-Scope impiegheranno solo applicazioni di crittografia commerciali non modificate per crittografare i dati inattivi e/o in transito.

Il personale di Trimble è soggetto a obblighi di riservatezza e a varie politiche, come l'uso accettabile, la classificazione dei dati, la distruzione sicura e l'MFA. Trimble richiede al proprio personale di seguire una formazione sulla consapevolezza della sicurezza delle informazioni, sia all'inizio del rapporto di lavoro che

successivamente ogni anno. Trimble richiede inoltre al proprio personale di sottoporsi annualmente a una formazione sulla privacy (anche per conformarsi al GDPR).

Per i prodotti applicabili, Trimble ha implementato i principi di sicurezza e privacy by design, inclusi, a titolo esemplificativo ma non esaustivo, la modellazione delle minacce e i test di penetrazione delle applicazioni dei prodotti.

12. Misure per la certificazione/garanzia dei processi e dei prodotti

Trimble manterrà le certificazioni SOC 2, Tipo II, ISO 27001 o NIST 800-171, sottoponendosi a periodiche verifiche di sorveglianza esterna e di ricertificazione per garantire che il suo sistema di gestione della sicurezza delle informazioni (ISMS) soddisfi i requisiti di questo standard per i prodotti applicabili.

Trimble manterrà politiche di sicurezza delle informazioni che soddisfano i requisiti dello standard ISO 27001, un programma di audit interno che valuta l'ISMS e i controlli di sicurezza delle informazioni di Trimble e un comitato di gestione responsabile della supervisione del sistema di gestione della sicurezza delle informazioni (ISMS) di Trimble.

13. Misure per garantire la minimizzazione dei dati

Trimble può consentire ai visitatori di utilizzare determinate funzionalità di alcuni prodotti in modo anonimo e ridurre al minimo i dati richiesti ai clienti solo a quanto necessario per fornire il servizio richiesto ai sensi delle leggi e dei regolamenti localizzati.

14. Misure per garantire la qualità dei dati

Trimble garantisce la qualità dei propri dati attraverso vari meccanismi di verifica unici per i prodotti Trimble applicabili. Trimble può anche consentire agli utenti dei prodotti di aggiornare le informazioni nei loro account direttamente o tramite richieste alle sue funzioni di assistenza clienti.

15. Misure per garantire una conservazione limitata dei dati

Trimble può implementare la Politica di conservazione dei dati del Cliente che stabilisce i periodi di conservazione per vari tipi di dati.

16. Misure per consentire la portabilità dei dati e garantire la cancellazione

I prodotti Trimble applicabili prevedono una procedura per l'eliminazione dei Dati del Cliente entro 30 giorni dalla ricezione delle richieste scritte verificate dal Cliente e possono consentire il download dei Dati del Cliente da fornire a fornitori di servizi alternativi, come richiesto dal GDPR.

17. Controllo e gestione di terze parti (sub-responsabile del trattamento)

Trimble si avvale esclusivamente di sub-responsabili del trattamento che elaborano i dati personali per conto di Trimble nell'ambito dei servizi in abbonamento applicabili in conformità con le Leggi e i Regolamenti sulla protezione dei dati. Trimble verifica inoltre, prima di scegliere un sub-responsabile e trasferire qualsiasi dato, le misure tecniche e organizzative del sub-responsabile del trattamento per garantire un livello di sicurezza adeguato al rischio del trattamento dei dati dei propri clienti. Trimble adotta inoltre misure ragionevoli per garantire la sicurezza dei trasferimenti dei Dati del Cliente a Sub-responsabili del trattamento di terze parti. Come minimo, tali misure includono l'identificazione dei rischi per i diritti del Cliente e dell'Interessato in base alla natura, all'ambito e al contesto del trattamento; esaminare i controlli di sicurezza e protezione dei dati implementati dal Sub-responsabile del trattamento per proteggere i Dati del Cliente (inclusi i rapporti di audit SOC 2 di Tipo II e/o i certificati ISO 27001, a seconda dei casi); imporre condizioni contrattuali di protezione dei dati che proteggano i dati personali secondo standard uguali o simili che Trimble è obbligata a fornire ai propri clienti (inclusi meccanismi di trasferimento transfrontaliero validi, gestione dei sub-responsabili e programmi di conformità); richiedere al Sub-responsabile del trattamento di elaborare i Dati del Cliente solo per conto di Trimble e dei suoi clienti e limitare il trattamento dei Dati del Cliente all'ambito delle istruzioni di Trimble.

ALLEGATO 3 – Meccanismo di trasferimento transfrontaliero

1. Spazio economico europeo (SEE):

1.1 La definizione di "Leggi e regolamenti sulla protezione dei dati" include il Regolamento generale sulla protezione dei dati (UE 2016/679) ("**GDPR**").

1.2 Quando Trimble si avvale di un sub-responsabile del trattamento ai sensi della Sezione 5.1 (Nomina di Sub-responsabili del trattamento) del presente Addendum (DPA), si impegna a:

(a) richiedere a qualsiasi sub-responsabile nominato di proteggere i Dati del Cliente secondo gli standard richiesti dalle Leggi e dai Regolamenti sulla protezione dei dati e imporre gli stessi obblighi in materia di protezione dei dati di cui all'articolo 28, paragrafo 3, del GDPR, in particolare fornendo garanzie sufficienti per implementare misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR, e

(b) richiedere a qualsiasi sub-responsabile nominato di (i) accettare per iscritto di trattare i dati personali solo in un paese che l'Unione Europea ha dichiarato di avere un livello di protezione "adeguato" o (ii) trattare i dati personali solo sulla base delle Clausole contrattuali standard dell'UE o ai sensi delle Norme vincolanti d'impresa approvate dalle autorità competenti per la protezione dei dati dell'Unione europea.

1.3 In deroga a qualsiasi disposizione contraria contenuta nel presente DPA o nel Contratto (inclusi, a titolo esemplificativo, gli obblighi di indennizzo di ciascuna delle parti), nessuna delle parti sarà responsabile per eventuali sanzioni pecuniarie del GDPR emesse o rimosse ai sensi dell'articolo 83 del GDPR nei confronti dell'altra parte da un'autorità di regolamentazione o da un ente governativo in relazione alla violazione del GDPR da parte di tale altra parte.

1.4 Il Cliente riconosce che Trimble, in qualità di titolare del trattamento, potrebbe essere tenuta a notificare a un'autorità di regolamentazione gli Incidenti di sicurezza relativi ai Dati di utilizzo del Cliente. Nel caso in cui un'autorità di regolamentazione richieda a Trimble di informare gli interessati con i quali Trimble non ha un rapporto diretto (ad esempio, gli utenti finali del Cliente), Trimble informerà il Cliente di tale requisito. Il Cliente fornirà un'assistenza ragionevole a Trimble per informare gli interessati interessati.

2. Regno Unito (UK):

2.1 I riferimenti al "GDPR" contenuti nel presente DPA saranno considerati riferimenti alle leggi e ai regolamenti corrispondenti del Regno Unito, inclusi, a titolo esemplificativo, il GDPR del Regno Unito e il Data Protection Act 2018.

2.2 Quando Trimble si avvale di un sub-responsabile del trattamento ai sensi della Sezione 5.1 (Nomina di Sub-responsabili del trattamento) del presente DPA, si impegna a:

(a) richiedere a qualsiasi sub-responsabile nominato di proteggere i Dati del Cliente secondo gli standard richiesti dalle Leggi e dai Regolamenti sulla protezione dei dati, ad esempio includendo gli stessi obblighi in materia di protezione dei dati di cui all'articolo 28(3) del GDPR del Regno Unito, in particolare fornendo garanzie sufficienti per implementare misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR del Regno Unito, e

(b) richiedere a qualsiasi sub-responsabile nominato di (i) accettare per iscritto di trattare i dati personali solo in un paese che il Regno Unito ha dichiarato di avere un livello di protezione "adeguato" o (ii) trattare i dati personali solo a condizioni equivalenti all'Accordo sul trasferimento internazionale dei dati del Regno Unito o alle Clausole contrattuali standard dell'UE e all'Addendum sul trasferimento internazionale dei dati del Regno Unito o ai sensi delle Norme vincolanti d'impresa approvate dalle autorità competenti per la protezione dei dati del Regno Unito.

2.3 In deroga a qualsiasi disposizione contraria contenuta nel presente DPA o nel Contratto (inclusi, a titolo esemplificativo, gli obblighi di indennizzo di ciascuna delle parti), nessuna delle parti sarà responsabile per eventuali multe del GDPR del Regno Unito emesse o rimosse ai sensi dell'articolo 83 del GDPR del Regno Unito nei confronti dell'altra parte da un'autorità di regolamentazione o da un ente governativo in relazione alla violazione del GDPR del Regno Unito da parte di tale altra parte.

2.4 Il Cliente riconosce che Trimble, in qualità di titolare del trattamento, potrebbe essere tenuta a notificare a un'autorità di regolamentazione gli Incidenti di sicurezza relativi ai Dati di utilizzo del Cliente. Nel caso in cui un'autorità di regolamentazione richieda a Trimble di informare gli interessati con i quali Trimble non ha un rapporto diretto (ad esempio, gli utenti finali del Cliente), Trimble informerà il Cliente di tale requisito. Il Cliente fornirà un'assistenza ragionevole a Trimble per informare gli interessati interessati.

3. Svizzera:

3.1 La definizione di "Leggi e regolamenti sulla protezione dei dati" comprende la Legge federale svizzera sulla protezione dei dati, come riveduta ("**LPD**").

3.2 Quando Trimble si avvale di un sub-responsabile del trattamento ai sensi della Sezione 5.1 (Nomina di Sub-responsabili del trattamento) del presente DPA, si impegna a:

(a) richiedere a qualsiasi sub-responsabile nominato di proteggere i Dati del Cliente secondo gli standard richiesti dalle Leggi e dai Regolamenti sulla protezione dei dati, in particolare, fornendo garanzie sufficienti per implementare misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della LPD, e

(b) richiedere a qualsiasi sub-responsabile nominato di (i) accettare per iscritto di trattare i dati personali solo in un paese che la Svizzera ha dichiarato di avere un livello di protezione "adeguato" o (ii) trattare i dati personali solo a condizioni equivalenti alle Clausole contrattuali standard dell'UE, comprese le modifiche menzionate nella Sezione 3.3, o ai sensi delle Norme vincolanti d'impresa approvate dalle autorità competenti dell'Unione Europea o svizzera per la protezione dei dati.

3.3 Nella misura in cui i trasferimenti di dati personali dalla Svizzera sono soggetti alle clausole contrattuali standard dell'UE in conformità con la sezione 2.3 dell'allegato 3 (Clausole contrattuali standard dell'UE), le parti convengono che tutte le modifiche alle clausole contrattuali standard dell'UE ritenute necessarie dall'Incaricato federale della protezione dei dati e della trasparenza riterranno necessarie. Nello specifico, si tratta al momento della conclusione del DPA:

a) i riferimenti a "Stato membro dell'UE" e "Stato membro" saranno interpretati in modo da includere la Svizzera, e

b) nella misura in cui il trasferimento o i trasferimenti successivi sono soggetti alla LPD:

i) i riferimenti al "regolamento (UE) 2016/679" devono essere interpretati come riferimenti alla LPD;

ii) l'"autorità di controllo competente" di cui all'allegato I, parte C, sarà l'Incaricato federale svizzero della protezione dei dati e della trasparenza;

(iii) nella Clausola 17 (Opzione 1), le Clausole contrattuali standard dell'UE saranno disciplinate dalle leggi della Svizzera; e

(iv) nella clausola 18(b) delle clausole contrattuali standard dell'UE, le controversie saranno risolte dinanzi ai tribunali della Svizzera.

(v) Si applica la clausola 18(c) delle clausole contrattuali standard dell'UE, mentre l'interessato può anche intentare un'azione legale contro l'esportatore e/o l'importatore dei dati dinanzi ai tribunali della Svizzera in cui l'interessato ha la residenza abituale.

4. Stati Uniti d'America:

4.1 Per "**Leggi sulla privacy degli Stati Uniti**" si intendono tutte le leggi statali relative alla protezione e al trattamento dei dati personali in vigore negli Stati Uniti d'America, che possono includere, a titolo esemplificativo, il California Consumer Privacy Act, come modificato dal California Privacy Rights Act ("**CCPA**"), il Virginia Consumer Data Protection Act, il Colorado Privacy Act, il Connecticut Data Privacy Act, e la legge sulla privacy dei consumatori dello Utah.

4.2 La definizione di "Leggi e regolamenti sulla protezione dei dati" include le leggi sulla privacy degli Stati Uniti.

4.3 Le seguenti condizioni si applicano nel caso in cui Trimble elabori i Dati personali soggetti al CCPA:

(a) Il termine "**informazioni personali**", come utilizzato nella presente Sezione 4.3, avrà il significato previsto nel CCPA;

(b) Trimble è un fornitore di servizi per il trattamento dei Dati del Cliente. Trimble elaborerà le informazioni personali contenute nei Dati del Cliente solo per le finalità commerciali indicate nel Contratto, incluse le finalità del Trattamento e le attività di trattamento indicate nel presente DPA ("**Finalità**"). In qualità di fornitore di servizi, Trimble non venderà o condividerà i Dati del Cliente né conserverà, utilizzerà o divulgherà i Dati del Cliente (i) per motivi diversi dalla Finalità, inclusa la conservazione, l'utilizzo o la divulgazione dei Dati del Cliente per motivi commerciali diversi dalla Finalità o come altrimenti consentito dal CCPA; o (ii) al di fuori del rapporto commerciale diretto tra il Cliente e Trimble;

(c) Trimble (i) rispetterà gli obblighi ad essa applicabili in qualità di fornitore di servizi ai sensi del CCPA e (ii) fornirà informazioni personali con lo stesso livello di protezione della privacy richiesto dal CCPA. Il Cliente è responsabile di garantire di aver rispettato, e continuerà a rispettare, i requisiti del CCPA nell'utilizzo dei Servizi e nel proprio Trattamento delle informazioni personali;

(d) il Cliente avrà il diritto di adottare misure ragionevoli e appropriate per garantire che Trimble utilizzi le informazioni personali in modo coerente con gli obblighi del Cliente ai sensi del CCPA;

(e) Trimble informerà il Cliente qualora ritenga di non essere più in grado di adempiere ai propri obblighi in qualità di fornitore di servizi ai sensi del CCPA;

(f) Previa notifica, il Cliente avrà il diritto di adottare misure ragionevoli e appropriate in conformità con il Contratto per interrompere e rimediare all'uso non autorizzato delle informazioni personali;

(g) Trimble fornirà un'assistenza supplementare e tempestiva ragionevole per assistere il Cliente nell'adempimento dei propri obblighi in relazione alle richieste dei consumatori come stabilito nel Contratto;

(h) Per i Sub-responsabili del trattamento utilizzati da Trimble per il trattamento dei dati personali soggetti al CCPA, Trimble garantirà che l'accordo stipulato con tale Sub-responsabile sia conforme al CCPA, inclusi, a titolo esemplificativo, i requisiti contrattuali per i fornitori di servizi e gli appaltatori;

(i) Trimble non combinerà i Dati del Cliente ricevuti da o per conto del Cliente con le informazioni personali che riceve da o per conto di un'altra persona o di altre persone, o raccoglie dalla propria interazione con il consumatore, a meno che tale combinazione non sia necessaria per l'esecuzione di qualsiasi scopo commerciale consentito dal CCPA, incluse le relative normative, o da regolamenti adottati dall'Agenzia della protezione della privacy della California; e

(j) Trimble certifica di comprendere e di rispettare i propri obblighi ai sensi del CCPA.

4.4 Trimble riconosce e conferma di non ricevere i Dati del Cliente come corrispettivo per i Servizi forniti al Cliente.

5. Australia:

5.1 La definizione di "Leggi e regolamenti sulla protezione dei dati" include gli Australian Privacy Principles e l'Australian Privacy Act (1988).

5.2 La definizione di "Dati personali" include le "Informazioni personali" come definite dalle leggi e dai regolamenti sulla protezione dei dati.

5.3 La definizione di "Dati sensibili" include le "Informazioni sensibili" come definite dalle leggi e dai regolamenti sulla protezione dei dati.

6. Brasile:

6.1 La definizione di "Leggi e regolamenti sulla protezione dei dati" include la Lei Geral de Proteção de Dados (Legge generale sulla protezione dei dati personali).

6.2 La definizione di "Incidente di sicurezza" include un incidente di sicurezza che può comportare un rischio o un danno rilevante per i soggetti interessati.

6.3 La definizione di "Responsabile dei dati" include le "Operatore" come definito dalle leggi e dai regolamenti sulla protezione dei dati.

7. Canada:

7.1 La definizione di "Leggi e regolamenti sulla protezione dei dati" include la legge federale sulla protezione delle informazioni personali e dei documenti elettronici.

7.2 I Sub-responsabili del trattamento di Trimble, come indicato nella Sezione 5 (Sub-responsabili del trattamento) del presente DPA, sono terze parti ai sensi delle Leggi e dei Regolamenti in materia di protezione dei dati, con i

quali Trimble ha stipulato un contratto scritto che include termini sostanzialmente simili al presente DPA. Trimble ha condotto un'adeguata due diligence sui propri Sub-responsabili del trattamento.

7.3 Trimble adotterà le misure tecniche e organizzative di cui all'Articolo 11 dell'Allegato 2 (Sicurezza) del presente DPA.

8. Israele:

8.1 La definizione di "Leggi e regolamenti sulla protezione dei dati" include le leggi sulla protezione della privacy.

8.2 La definizione di "Controllore" include "Proprietario di database" come definito dalle leggi e dai regolamenti sulla protezione dei dati.

8.3 La definizione di "Responsabile del trattamento" include "Detentore" come definito dalle leggi e dai regolamenti sulla protezione dei dati.

8.4 Trimble richiederà che il personale autorizzato al trattamento dei Dati del Cliente rispetti il principio della segretezza dei dati e sia stato debitamente istruito in merito alle Leggi e ai Regolamenti in materia di protezione dei dati. Tale personale firma accordi di riservatezza con Trimble in conformità con la Sezione 6 (Riservatezza) del presente DPA.

8.5 Trimble deve adottare misure sufficienti per garantire la privacy dei Soggetti Interessati implementando e mantenendo le misure di sicurezza specificate nella Sezione 11 dell'Allegato 2 (Sicurezza) del presente DPA e rispettando i termini del Contratto.

8.6 Trimble deve garantire che i Dati personali non saranno trasferiti a un Sub-responsabile del trattamento, a meno che tale Sub-responsabile non abbia stipulato un accordo con Trimble ai sensi della Sezione 5.1 (Nomina di Sub-responsabili del trattamento) del presente DPA.

9. Giappone:

9.1 La definizione di "Leggi e regolamenti sulla protezione dei dati" include la legge sulla protezione delle informazioni personali ("**APPI**").

9.2 La definizione di "Dati personali" include le informazioni relative a una persona fisica specifica applicabile ai sensi della Sezione 2(1) dell'APPI, che il Cliente affida a Trimble durante la fornitura dei Servizi al Cliente da parte di Trimble.

9.3 Trimble accetta di avere e di mantenere un programma di privacy conforme agli standard prescritti dalle norme della Commissione per la protezione dei dati personali in materia di trattamento dei dati personali ai sensi delle disposizioni del Capitolo 4 dell'APPI. In accordo:

(a) Trimble (i) tratterà i Dati personali nella misura necessaria per fornire i Servizi al Cliente in conformità al Contratto e come indicato nell'Allegato 1 (Descrizione del trattamento) del presente DPA ("*Finalità del trattamento*") e (ii) non tratterà i Dati personali per scopi diversi dalla Finalità del trattamento senza il consenso del Cliente;

(b) Trimble implementerà e manterrà misure appropriate e necessarie per prevenire la divulgazione non autorizzata e la perdita di Dati personali e per la gestione sicura dei Dati personali in conformità con l'APPI, come stabilito nell'Allegato 2 (Misure tecniche e organizzative) del presente DPA;

(c) Trimble informerà il Cliente in caso di (i) mancato rispetto della Sezione 9.3(a) del presente Allegato 3 o (ii) della scoperta da parte di Trimble di un Incidente di sicurezza che ha un impatto sui Dati del Cliente, in entrambi i casi, in conformità con la Sezione 6.4 del presente DPA. Trimble fornirà un'assistenza ragionevole al Cliente nel caso in cui al Cliente sia richiesto di informare un'autorità di regolamentazione o qualsiasi Soggetto Interessato impattato da un Incidente di sicurezza;

(d) Trimble garantirà che tutti i propri dipendenti che hanno accesso ai Dati personali (i) abbiano stipulato contratti con i dipendenti che richiedono loro di mantenere riservati tali Dati personali e (ii) che violino la riservatezza saranno soggetti ad azioni disciplinari e a possibili licenziamenti; (iii) svolgere un'adeguata supervisione e formazione dei dipendenti per la gestione sicura dei Dati personali; e (iv) limitare il numero di personale autorizzato, inclusi i dipendenti di Trimble, che ha accesso ai Dati personali e controllare tale accesso in modo che sia consentito solo per il periodo di tempo necessario per la finalità del trattamento;

(e) Trimble non divulgherà i Dati personali a terzi, ad eccezione dei casi in cui il Cliente abbia autorizzato Trimble a farlo nel Contratto. Nell'incaricare i Sub-responsabili del trattamento, Trimble rispetterà gli obblighi di cui alla Sezione 9 (Sub-responsabili del trattamento) del presente ATD per garantire l'adozione di procedure atte a mantenere la riservatezza e la sicurezza dei Dati personali;

(f) Trimble conserverà un registro del trattamento dei Dati personali ad essa affidato dal Cliente ed eseguito per conto del Cliente;

(g) Il Cliente può valutare la conformità di Trimble ai propri obblighi ai sensi delle Leggi e dei Regolamenti in materia di protezione dei dati e come stabilito nella Sezione 6 del presente DPA.

(h) Trimble fornirà una ragionevole collaborazione al Cliente su richiesta scritta, qualora il Cliente stia segnalando alla Commissione per la protezione dei dati personali o ad altre autorità di regolamentazione; e

(i) Le principali strutture di elaborazione di Trimble si trovano negli Stati Uniti d'America e, a seconda dell'utilizzo dei Servizi da parte del Cliente, nelle sedi indicate ai sensi di <https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center> sotto "Risorse aggiuntive" ("Elenchi dei sub-responsabili"). Trimble informerà il Cliente di qualsiasi modifica e fornirà al Cliente la possibilità di opporsi in conformità con la Sezione 9 del presente DPA. Nel caso in cui Trimble elabori i Dati personali in un paese diverso dal Giappone, Trimble garantirà la conformità al proprio programma sulla privacy come descritto nel presente DPA.

9.4 Si applicano i seguenti termini di consenso dei soggetti interessati:

(a) Il Cliente affida a Trimble i Dati personali per la finalità del trattamento. Il Cliente accetta che Trimble non è una "terza parte" in quanto il termine è utilizzato nelle disposizioni APPI che limitano la fornitura di Dati personali a terzi. Pertanto, non si applica l'obbligo di ottenere preventivamente il consenso del soggetto interessato;

(b) se è richiesto il consenso del soggetto interessato ai sensi dell'Articolo 4 del Telecommunications Business Act, il Cliente rispetterà tutti i requisiti di consenso specifici per l'utilizzo dei Servizi.

10. Messico:

10.1 La definizione di "Leggi e regolamenti sulla protezione dei dati" include la legge federale per la protezione dei dati personali detenuti da parti private e i suoi regolamenti.

10.2 Quando Responsabile del trattamento, Trimble si impegna a:

(a) trattare i Dati personali in conformità con le istruzioni del Cliente di cui alla Sezione 5 del presente DPA;

(b) trattare i Dati Personali solo nella misura necessaria per fornire i Servizi;

(c) implementare misure di sicurezza in conformità con le leggi e i regolamenti sulla protezione dei dati e l'Allegato 2 (Misure tecniche e organizzative) del presente DPA;

(d) mantenere la riservatezza in merito ai Dati personali trattati in conformità con l'Accordo;

(e) eliminare tutti i Dati personali al momento della risoluzione del Contratto in conformità con la Sezione 10 (Restituzione o cancellazione dei Dati del cliente) del presente DPA; e

(f) trasferire i Dati personali a Sub-responsabili del trattamento solo in conformità con la Sezione 9 (Sub-responsabili del trattamento) del presente DPA.

11. Singapore:

11.1 La definizione di "Leggi e regolamenti sulla protezione dei dati" include il Regolamento generale sulla protezione dei dati 2012 ("**PDPA**").

11.2 Trimble tratterà i Dati personali secondo uno standard di protezione conforme al PDPA implementando misure tecniche e organizzative adeguate, come stabilito nell'Allegato 2 (Misure tecniche e organizzative) del presente DPA e rispettando i termini del Contratto.

12. Repubblica di Turchia

12.1 La definizione di "Leggi e regolamenti sulla protezione dei dati" include (i) la legge sulla protezione dei dati personali ("PDPL"), legge n. 6698, dal 24 marzo 2016, come modificata dalla legge sull'interpretazione delle modifiche al codice di procedura penale e altre leggi, legge n. 7499, dal 2 marzo 2024 e (ii) il regolamento sui principi relativi alle procedure e alle regole per il trasferimento di dati personali all'estero dall'Autorità per la protezione dei dati personali come: pubblicato sulla Gazzetta Ufficiale il 10 luglio, numero 32598.

12.2 Il Cliente riconosce che Trimble, in qualità di titolare del trattamento, potrebbe essere tenuta ai sensi delle Leggi e dei Regolamenti sulla protezione dei dati a notificare a un'autorità di regolamentazione gli Incidenti di sicurezza che coinvolgono i Dati di utilizzo del Cliente. Nel caso in cui un'autorità di regolamentazione richieda a Trimble di informare gli interessati con i quali Trimble non ha un rapporto diretto (ad esempio, gli utenti finali del Cliente), Trimble informerà il Cliente di tale requisito. Il Cliente fornirà un'assistenza ragionevole a Trimble per informare gli interessati interessati.

ALLEGATO 4 - MECCANISMO DI TRASFERIMENTO TRANSFRONTALIERO (Si applica ai dati trasferiti dall'UE, dal SEE, dal Regno Unito e dalla Svizzera)

1. Definizioni

- **Per "Clausole contrattuali standard dell'UE"** si intendono le Clausole contrattuali standard approvate dalla Commissione europea con la decisione 2021/914.
- **Per "Accordo sul trasferimento internazionale dei dati del Regno Unito"** si intende l'Addendum sul trasferimento internazionale dei dati alle Clausole contrattuali standard della Commissione UE emesse dall'Information Commissioner del Regno Unito, versione B1.0, in vigore il 21 marzo 2022.
- **Per "Quadro normativo sulla privacy dei dati"** si intende il programma di autocertificazione del quadro normativo sulla privacy dei dati UE-USA e/o Svizzera-USA gestito dal Dipartimento del Commercio degli Stati Uniti.
- **Per "Principi sulla privacy dei dati"** si intendono i principi del Quadro sulla privacy dei dati (come integrati dai Principi supplementari).
- **Per "Clausole contrattuali standard turche"** si intende il Contratto standard da utilizzare per il trasferimento di dati personali all'estero da 1 a 4, come accettato dalla decisione 2024/959 del 4 giugno 2024 dell'Autorità turca per la protezione dei dati personali.

2. Meccanismi di trasferimento transfrontaliero dei dati

2.1 Ordine di precedenza. Nel caso in cui i Servizi siano coperti da più di un Meccanismo di trasferimento, il trasferimento dei Dati personali sarà soggetto a un unico Meccanismo di trasferimento, a seconda dei casi, e in conformità con il seguente ordine di precedenza: (a) il Quadro sulla privacy dei dati come indicato nella Sezione 2.2 (Quadro sulla privacy dei dati) del presente Allegato; (b) le Clausole contrattuali standard dell'UE di cui alla Sezione 2.3 (Clausole contrattuali standard dell'UE) del presente Allegato; (c) l'Addendum sul trasferimento internazionale dei dati del Regno Unito come indicato nella Sezione 2.4 (Addendum sul trasferimento internazionale dei dati del Regno Unito) del presente Allegato; e, se né (a), (b), (c), (d) né (e) sono applicabili, (f) altri meccanismi di trasferimento dei dati applicabili consentiti dalle leggi e dai regolamenti sulla protezione dei dati.

2.2 Quadro normativo sulla protezione dei dati. Nella misura in cui Trimble Inc. elabora i Dati personali tramite i Servizi provenienti dal SEE o dalla Svizzera, Trimble Inc. è autocertificata ai sensi del Quadro sulla privacy dei dati e rispetta i Principi sulla privacy dei dati durante il trattamento di tali dati personali. Nella misura in cui il Cliente (a) si trova negli Stati Uniti d'America e si autocertifica ai sensi del Quadro normativo sulla privacy dei dati o (b) si trova nel SEE o in Svizzera, Trimble accetta inoltre (i) di fornire almeno lo stesso livello di protezione dei Dati personali richiesto dai Principi sulla privacy dei dati; (ii) di informare il Cliente per iscritto, senza indebito ritardo, se la sua autocertificazione relativa al Quadro sulla privacy dei dati viene ritirata, terminata, revocata o altrimenti invalidata (nel qual caso, si applicherà un Meccanismo di trasferimento alternativo in conformità con l'ordine di precedenza di cui alla Sezione 2.1 (Ordine di precedenza) del presente Allegato 4; e (iii) previa comunicazione scritta, collaborare con il Cliente per adottare misure ragionevoli e appropriate per interrompere e porre rimedio a qualsiasi trattamento non autorizzato di dati personali.

2.3 Clausole contrattuali standard dell'UE. Le Clausole contrattuali standard dell'UE si applicheranno ai Dati personali trasferiti tramite i Servizi dal SEE, dalla Svizzera o dal Regno Unito, direttamente o tramite trasferimento successivo, a qualsiasi paese o destinatario al di fuori del SEE, della Svizzera o del Regno Unito che non sia riconosciuto dall'autorità competente pertinente come in grado di fornire un livello adeguato di protezione dei dati personali. Per i trasferimenti di dati soggetti alle Clausole contrattuali standard dell'UE, le Clausole contrattuali standard dell'UE saranno considerate stipulate e incorporate nel presente ATD per riferimento e completate come segue:

(a) Il Modulo Uno (da Titolare del trattamento a Titolare del trattamento) delle Clausole contrattuali standard dell'UE si applicherà nel caso in cui (i) Trimble elabori i Dati dell'Account del Cliente e (ii) il Cliente sia un titolare del trattamento dei Dati di utilizzo del Cliente e Trimble elabori i Dati di utilizzo del Cliente;

(b) Il Modulo Due (da Titolare del trattamento a Responsabile del trattamento) delle Clausole contrattuali standard dell'UE si applicherà nel caso in cui il Cliente sia un titolare del trattamento dei Dati personali e Trimble tratti i Dati personali per conto del Cliente;

(c) il Modulo Tre (da Responsabile del trattamento a Responsabile del trattamento) delle Clausole contrattuali standard dell'UE si applicherà nel caso in cui il Cliente sia un responsabile del trattamento dei Dati personali e Trimble esegua il trattamento in qualità di Sub-responsabile del trattamento per conto del Cliente; e

d) Per ciascun modulo, dove applicabile:

(i) nella clausola 7 delle clausole contrattuali standard dell'UE, la docking clause opzionale non si applica;

(ii) nella Clausola 9 delle Clausole contrattuali standard dell'UE, si applicherà l'Opzione 2 e il periodo di tempo per la notifica scritta preventiva delle modifiche ai sub-responsabili del trattamento sarà quello stabilito nella Sezione 5.2 (Elenco degli attuali Sub-responsabili del trattamento e notifica di nuovi Sub-responsabili del trattamento) del presente DPA;

(iii) nella clausola 11 delle clausole contrattuali standard dell'UE, la lingua facoltativa non si applicherà;

(iv) Identificare la/e autorità di vigilanza competente/i in conformità alla clausola 13;

(v) nella Clausola 17 (Opzione 1), le Clausole contrattuali standard dell'UE saranno disciplinate dalla legge olandese;

(vi) nella Clausola 18(b) delle Clausole contrattuali standard dell'UE, le controversie saranno risolte dinanzi ai tribunali di Amsterdam, Paesi Bassi;

(viii) nell'allegato I, parte B, delle clausole contrattuali standard dell'UE:

Esportatore dati: Cliente (se la casella a pagina 6 è selezionata).

Dati di contatto: l'indirizzo e-mail o gli indirizzi e-mail indicati dal Cliente nell'account del Cliente tramite le sue preferenze di notifica.

Ruolo dell'esportatore dati: Il ruolo dell'esportatore dei dati è indicato a pagina 6

Firma e data: Con la sottoscrizione del contratto, si ritiene che l'esportatore dati abbia firmato le presenti Clausole contrattuali standard dell'UE, qui incorporate, inclusi i relativi allegati, a partire dalla data di entrata in vigore del contratto;

Importatore dati: Trimble Inc.

Dati di contatto: Trimble Privacy Team - privacy@Trimble.com

Ruolo dell'importatore dati: Il ruolo dell'importatore dei dati è indicato a pagina 6

Firma e data: Con la sottoscrizione del contratto, si ritiene che l'Importatore dati abbia firmato le presenti Clausole contrattuali standard dell'UE, qui incorporate, inclusi i relativi allegati, a partire dalla data di entrata in vigore dell'Accordo;

(viii) nell'allegato I, parte B, delle clausole contrattuali standard dell'UE:

Le categorie degli interessati sono stabilite nella Sezione 1 dell'Allegato 1 (Descrizione del trattamento) del presente DPA.

I Dati sensibili trasferiti sono indicati nella Sezione 3 dell'Allegato 1 (Descrizione del trattamento) del presente DPA.

La frequenza del trasferimento è continuativa per tutta la durata del Contratto.

La natura del trattamento è stabilito nella Sezione 5 dell'Allegato 1 (Descrizione del trattamento) del presente DPA.

La natura del trattamento è stabilito nella Sezione 5 dell'Allegato 1 (Descrizione del trattamento) del presente DPA.

Il periodo per il quale i dati personali saranno conservati è stabilito nella Sezione 7 dell'Allegato 1 (Descrizione del trattamento) del presente DPA.

Per i trasferimenti ai Sub-responsabili del trattamento, l'oggetto, la natura e la durata del Trattamento sono indicati in <https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center> sotto "Risorse aggiuntive" ("Elenchi dei Sub-responsabili del trattamento").

(ix) nell'allegato I, parte C delle clausole contrattuali standard dell'UE: ove applicabile, la Commissione olandese per la protezione dei dati sarà l'autorità di controllo capofila. Altrimenti, se un'entità di Trimble residente nell'UE è l'esportatore di dati, l'autorità di vigilanza competente è l'autorità di vigilanza dello stato membro in cui risiede l'entità di Trimble. Nel caso in cui il Cliente sia l'esportatore dei dati, l'autorità di vigilanza competente è l'autorità di vigilanza dello Stato membro in cui risiede il cliente.

(x) L'Allegato 2 (Misure di sicurezza tecniche e organizzative) del presente DPA funge da Allegato II delle Clausole contrattuali standard dell'UE.

2.4 Estensione del Regno Unito al Data Privacy Framework e all'Addendum sul trasferimento internazionale dei dati. Il Cliente e Trimble concordano che si applicherà l'Estensione del Regno Unito al Quadro sulla privacy dei dati e, in assenza di ciò, le Clausole contrattuali standard dell'UE e l'Appendice sul trasferimento internazionale dei dati del Regno Unito alle Clausole contrattuali standard della Commissione UE nella sua versione più recente si applicheranno ai Dati personali trasferiti tramite i Servizi dal Regno Unito, direttamente o tramite trasferimento successivo, in qualsiasi paese o destinatario al di fuori del Regno Unito che non sia riconosciuto dall'autorità di regolamentazione competente del Regno Unito o dall'ente governativo del Regno Unito come in grado di fornire un livello adeguato di protezione dei Dati personali. Per i trasferimenti di dati dal Regno Unito soggetti alle Clausole contrattuali standard dell'UE e all'Addendum sul trasferimento internazionale dei dati del Regno Unito, le Clausole contrattuali standard dell'UE saranno considerate stipulate e incorporate nel presente DPA come descritto nella Sezione 2.3 della presente Sezione 4 e l'Addendum sul trasferimento internazionale dei dati del Regno Unito sarà considerato stipulato, e incorporato nel presente DPA con il presente riferimento, e completato come segue:

(a) Nella Tabella 1 dell'Addendum sul trasferimento internazionale dei dati per il Regno Unito, i dettagli e le informazioni di contatto chiave del Cliente e di Trimble sono riportati nella Sezione 2.3 (e)(vii) del presente Allegato 3;

(b) Nella Tabella 2 dell'Addendum sul trasferimento internazionale dei dati del Regno Unito, le informazioni sulla versione delle Clausole contrattuali standard dell'UE e sulle clausole selezionate a cui è allegato l'Addendum sul trasferimento internazionale dei dati del Regno Unito sono riportate nella Sezione 2.3 (Clausole contrattuali standard dell'UE) del presente Allegato 4;

(c) Nella tabella 3 dell'Addendum sul trasferimento internazionale dei dati del Regno Unito:

(i) L'elenco delle Parti è riportato nella Sezione 2.3(e)(vii) del presente Allegato 3.

(ii) La descrizione del trasferimento è riportata nella Sezione 1 (Natura e finalità del trattamento) dell'Allegato 1 (Descrizione del trattamento).

(iii) L'Allegato II si trova nell'Allegato 2 (Misure di sicurezza tecniche e organizzative) del presente DPA.

(iv) L'elenco dei Sub-responsabili del trattamento è riportato su <https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center> sotto "Risorse aggiuntive" ("Elenchi dei Sub-responsabili del trattamento"); e

(d) Nella Tabella 4 dell'Addendum sul trasferimento internazionale dei dati del Regno Unito, sia l'Importatore che l'Esportatore possono rescindere l'Accordo sul trasferimento internazionale dei dati del Regno Unito in conformità con i termini dell'Addendum sul trasferimento internazionale dei dati del Regno Unito.

2.5 Clausole contrattuali standard della Turchia. Le Clausole contrattuali standard dell'UE si applicheranno ai Dati personali trasferiti tramite i Servizi dal SEE, dalla Svizzera o dal Regno Unito, direttamente o tramite trasferimento successivo, a qualsiasi paese o destinatario al di fuori del SEE, della Svizzera o del Regno Unito che non sia riconosciuto dall'autorità competente pertinente come in grado di fornire un livello adeguato di protezione dei dati personali. Per i trasferimenti di dati soggetti alle Clausole contrattuali standard della Turchia, le Clausole contrattuali standard della Turchia saranno considerate stipulate e incorporate nel presente DPA per riferimento e completate come segue:

Per ciascun modulo, dove applicabile:

(i) nell'Articolo 8 del Contratto 2 e Contratto 3 delle Clausole contrattuali standard dell'a Turchia, si applicherà l'Opzione 2 e il periodo di tempo per la notifica scritta preventiva delle modifiche ai sub-responsabili del trattamento sarà quello stabilito nella Sezione 5.2 (Elenco degli attuali Sub-responsabili del trattamento e notifica di nuovi Sub-responsabili del trattamento) del presente DPA;

(ii) Le parti concordano che il Cliente informerà l'Autorità turca competente per la protezione dei dati personali entro cinque (5) giorni lavorativi per informare della conclusione delle Clausole contrattuali standard turche.

(iii) L'Importatore dei dati sarà: Trimble con Indirizzi, Nome e Cognome, Titolo e Informazioni di contatto di Trimble e Firmatario come indicato nel DPA.

(iv) Firma e data: Con la sottoscrizione del contratto, si ritiene che sia Trimble che l'esportatore dati abbiano firmato le presenti Clausole contrattuali standard della Turchia, qui incorporate, inclusi i relativi allegati, a partire dalla data di entrata in vigore del contratto;

(v) Le informazioni di cui all'Allegato I delle Clausole contrattuali standard turche sono riportate nell'Allegato 1:

(vi) L'Allegato 2 (Misure di sicurezza tecniche e organizzative) del presente DPA funge da Allegato II delle Clausole contrattuali standard turche.

(vii) L'elenco dei Sub-responsabili del trattamento è riportato su <https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center> sotto "Risorse aggiuntive" ("Elenchi dei Sub-responsabili del trattamento").

2.6 Conflitto. Nella misura in cui vi sia un conflitto o un'incoerenza tra le Clausole contrattuali standard dell'UE o l'Accordo sul trasferimento internazionale dei dati del Regno Unito e qualsiasi altro termine del presente DPA, incluso l'Allegato 4 (Meccanismo di trasferimento transfrontaliero), prevarranno il contratto, le disposizioni delle Clausole contrattuali standard dell'UE o l'Addendum sul trasferimento internazionale dei dati del Regno Unito, a seconda dei casi.