

DATABEHANDLINGSAVTAL (DPA)

Detta databehandlingsavtal (eng. Data Processing Agreement, "DPA") utgör parternas avtal avseende behandling av personuppgifter. Det kompletterar alla licens-, abonnemangs-, tjänste- eller andra skriftliga eller elektroniska avtal ("**Avtalen**") som tecknas mellan Trimble och kunden vid inköp av tjänster (inklusive hyrprogram/program som nättjänst, dessas tillhörande offlinetjänster eller mobila applikationer från Trimble, samt support, och som i avtalet och hädanefter benämns "tjänster" eller liknande), och som innebär att Trimble erhåller personuppgifter från kunden.

Kunden godkänner detta DPA (i) genom att underteckna eller på annat sätt acceptera avtalet, (ii) när han eller hon undertecknar det för egen räkning och när så krävs enligt tillämpliga lagar och förordningar om dataskydd, som företrädare för och på uppdrag av behöriga närstående bolag, om och i den utsträckning Trimble behandlar personuppgifter. I detta DPA ska begreppet "kund", om inget annat anges, omfatta såväl kunden som dess behöriga närstående bolag.

Vid tillhandahållande av tjänsterna till kunden enligt avtalet kan Trimble komma att behandla personuppgifter för kundens räkning och parterna är överens om att följande bestämmelser ska följas med avseende på eventuella personuppgifter.

SÅ HÄR SKA DETTA DPA HANTERAS:

- I. Detta DPA består av: Huvuddokumentet för DPA, och bilagorna 1 till 4
- II. Det är signerat på förhand för Trimbles räkning. Standardavtalsklausulerna (som definieras nedan) införlivas genom hänvisning. .
- III. Om kunden vill fylla i detta DPA måste kunden:
 - a. Fylla i uppgifterna i rutan för signatur och signera på sidan 6.
 - b. Fylla i uppgifterna som uppgiftsutförare på sidan 6.
- IV. Skicka det ifyllda och undertecknade DPA-avtalet till Trimble via e-post, med uppgift om er organisations kundnummer (som framgår av tillämplig faktura från Trimble), till privacy@trimble.com.

SÅ HÄR SKA DETTA DPA TIILLÄMPAS:

- If the Customer entity accepting this DPA is a party to an Agreement, this DPA is an addendum to and forms part of that Agreement and the Trimble entity that is party to the Agreement is party to this DPA. Om den enhet hos kunden som accepterar detta DPA är part i ett Avtal, gäller detta DPA som ett tillägg till och utgör en del av det avtalet. Den enhet hos Trimble som är motpart i det avtalet är också motpart i detta DPA.
- If the Customer entity accepting this DPA is a party to an Agreement, this DPA is an addendum to and forms part of that Agreement and the Trimble entity that is party to the Agreement is party to this DPA. Om den enhet hos kunden som undertecknar detta DPA har lämnat in en beställning som har godkänts av Trimble eller något av dess närstående bolag, men inte själv är part i avtalet, utgör detta DPA ett tillägg till den beställningen (inklusive eventuell förnyad beställning) och den enhet hos Trimble som beställningen har placerats hos är motpart i detta DPA.
- If the Customer entity accepting this DPA is a party to an Agreement, this DPA is an addendum to and forms part of that Agreement and the Trimble entity that is party to the Agreement is party to this DPA. Om den enhet hos kunden som undertecknar DPA-avtalet har köpt tjänster från Trimble via en av Trimbles auktoriserade återförsäljare, måste kunden ange detta på sidan 6 och ange ett kundnummer som utfärdats av Trimble eller återförsäljaren. Om inget sådant kundnummer finns, bifogas en bekräftelse från återförsäljaren på att kunden prenumererar på en tjänst från Trimble. I sådana fall kommer detta DPA att betraktas som ett direkt avtal mellan kunden och Trimble.
- If the Customer entity accepting this DPA is a party to an Agreement, this DPA is an addendum to and forms part of that Agreement and the Trimble entity that is party to the Agreement is party to this DPA. Om den enhet eller den person som signerar detta DPA varken är part i en beställning eller ett avtal och inte heller är en indirekt kund via en återförsäljare, är detta DPA inte giltigt och därmed inte juridiskt bindande. En sådan enhet bör begära att dess närstående enhet som är part i Avtalet undertecknar detta DPA, eller skriftligen begär att bli en del av Avtalet.

Detta DPA ersätter inte några jämförbara eller ytterligare rättigheter avseende behandling av kunddata som anges i avtalen (inklusive eventuella befintliga tillägg till avtalen angående databehandling).

DATABASEHANDLINGSVILLKOR

1. DEFINITIONER

"Närstående bolag" avser varje enhet som direkt eller indirekt kontrollerar, kontrolleras av, eller lyder under samma kontrollerande enhet som den aktuella enheten. "Kontroll" avser i denna definition direkt eller indirekt ägande av, eller kontroll över mer än 50 % av röstetalet i den berörda enheten.

"Behörigt närstående bolag" avser de av kundens närstående bolag som (i) lyder under en eller flera dataskyddslagar och (ii) har rätt att använda tjänsterna enligt avtalet mellan kunden och Trimble, men som inte har undertecknat någon egen beställning hos Trimble och därmed inte är att betrakta som "kund" enligt avtalet.

"CCPA" avser California Consumer Privacy Act, Cal Civ. Code 1798.100 ff., och dess tillämpningsbestämmelser. föreskrifter.

"Personuppgiftsansvarig" avser den enhet som bestämmer i vilket syfte och på vilket sätt personuppgifterna ska behandlas.

"Kund" avser den enhet som har expedierat avtalet, tillsammans med de av dess närstående bolag (så länge de kvarstår som närstående bolag) som har undertecknat beställningsformulär

"Kunddata" avser det som i Avtalet definierats som "kunddata" eller "dina uppgifter".

"Lagar och förordningar om dataskydd" avser alla lagar och förordningar, inklusive lagar och förordningar som utfärdats av Europeiska unionen, i Europeiska ekonomiska samarbetsområdet och deras medlemsstater, Schweiz och Storbritannien, de länder som anges i bilaga 3 och alla andra länder där kunden eller ett till kunden närstående bolag har säte, i den mån dessa berörs av behandling av personuppgifter enligt Avtalet.

"Registrerad" avser den person som personuppgifterna avser.

"Europa" avser Europeiska unionen (EU), Europeiska ekonomiska samarbetsområdet (EES) och Schweiz.

"GDPR" avser Europaparlamentets och rådets direktiv (EU) 2016/679.

"Personuppgifter" avser all information som rör (i) en identifierad eller identifierbar person, (ii) en identifierad eller identifierbar juridisk person (där sådan information skyddas på liknande sätt som personuppgifter eller personligt identifierbar information enligt tillämpliga lagar och förordningar om dataskydd), under förutsättning att sådana uppgifter är kunduppgifter.

"Behandling" avser varje åtgärd eller uppsättning åtgärder som utförs med personuppgifter, oavsett om det sker automatiskt eller inte, såsom insamling, registrering, organisering, strukturering, lagring, anpassning eller ändring, hämtning, konsulterande, användning, utlämning genom överföring, spridning eller på annat sätt tillgängliggörande, jämförande eller kombinerande, begränsning, blockering, radering eller förstörelse.

"Personuppgiftsbiträde" avser den enhet som behandlar personuppgifter på uppdrag av den personuppgiftsansvarige och för dennes räkning, inklusive, i förekommande fall, alla "tjänsteleverantörer", såsom denna term definieras av CCPA.

"Offentlig myndighet" avser en statlig myndighet eller brottsbekämpande myndighet, inklusive rättsliga myndigheter.

"EU:s standardavtalsklausuler" avser ett avtal som ingåtts av och mellan antingen (i) ett till Trimble närstående bolag och Trimble Inc. eller (ii) Kunden och Trimble Inc., vart och ett i enlighet med genomförandebeslutet (EU) 2021/914.

"Underentreprenör" avser ett personuppgiftsbiträde som anlitas av Trimble eller en medlem av Trimble-koncernen.

"Trimble" avser den enhet inom Trimble som är part i detta DPA, enligt vad som anges i avsnittet "SÅ HÄR SKA DETTA DPA TILLÄMPAS" ovan. Enheter inom Trimble som fungerar som personuppgiftsbiträden är: Trimble Inc., ett aktiebolag registrerat i Delaware, Trimble Europe B.V., ett företag registrerat i Nederländerna, Trimble International B.V., ett aktiebolag registrerat i Nederländerna, Trimble UK Ltd, ett aktiebolag registrerat i England och Wales, Trimble Maps, Ltd, ett aktiebolag registrerat i England och Wales, Trimble Technologies Ireland Ltd, ett aktiebolag registrerat i Irland, Trimble France SAS, ett aktiebolag registrerat i Frankrike, Trimble Solutions Sandvika AS, ett aktiebolag registrerat i Norge, Trimble Finland Corporation, ett aktiebolag registrerat i Finland, Trimble Forestry Europe Corporation, ett aktiebolag registrerat i Finland, Lakefield eTechnologies Ltd, ett aktiebolag

registrerat i Irland, Trimble GmbH, ett aktiebolag registrerat i Tyskland, eller Trimble Germany GmbH, ett aktiebolag registrerat i Tyskland, där tillämpligt.

"**Trimble-koncernen**" avser Trimble och dess närstående bolag som ägnar sig åt behandlingen av personuppgifter.

2. BEHANDLING AV PERSONUPPGIFTER

2.1 Parternas roller. Parterna bekräftar och samtycker till att när det gäller behandling av personuppgifter är kunden personuppgiftsansvarig och Trimble är personuppgiftsbiträde. Parterna bekräftar och samtycker också till att Trimble eller medlemmar i Trimble-koncernen anlitar underentreprenörer i enlighet med de krav som anges i avsnitt 5 nedan, förutsatt att Trimble är personuppgiftsansvarig för behandlingen av data gällande kundens konto.

2.2 Kundens behandling av personuppgifter. Kunden ska, vid sin användning av tjänsterna, behandla personuppgifter i enlighet med kraven i lagar och förordningar om dataskydd. För att undvika osäkerhet ska kundens instruktioner för behandling av personuppgifter följa lagar och förordningar om dataskydd. Kunden ska ensam ansvara för personuppgifternas korrekthet, kvalitet och lagligenlighet, samt för det sätt på vilket kunden förvärvat personuppgifterna. Trimble ska omedelbart informera kunden om en instruktion, enligt Trimbles mening, bryter mot lagar och förordningar om dataskydd eller andra bestämmelser.

2.3 Trimbles behandling av personuppgifter. Trimble ska endast behandla personuppgifter på uppdrag av och i enlighet med kundens instruktioner, inklusive när det gäller överföring av personuppgifter till ett tredjeland eller en internationell organisation. Kunden instruerar Trimble att behandla personuppgifter för följande ändamål: (i) behandling i enlighet med Avtalet och tillämpliga beställningar; (ii) behandling som initierats av användare i deras användning av tjänsterna; (iii) behandling för att följa andra rimliga instruktioner som tillhandahålls av kunden där sådana instruktioner är förenliga med villkoren i Avtalet; och (iv) behandling i syfte att anonymisera i enlighet med Klausulerna för dataanvändning i Avtalet (och som inkluderas i bilaga 1).

TRIMBLE AGERAR INTE SOM PERSONUPPGIFTSBITRÄDE FÖR FÖLJANDE PERSONUPPGIFTER: Användares inloggnings- och kontaktuppgifter, användardata för programvaror och data som genereras genom säkerhetsåtgärder ("**Data gällande kundens konto**").

2.4 Omfattning och syfte; kategorier av personuppgifter och registrerade. Ändamålet med Trimbles behandling av personuppgifter är att kunna utföra av tjänsterna enligt Avtalet. De typer av personuppgifter och kategorier av registrerade som behandlas enligt detta DPA specificeras vidare i [bilaga 1](#) (Beskrivning av behandling), i detta DPA.

3. DE REGISTRERADES RÄTTIGHETER

3.1 De registrerades rättigheter. Mot bakgrund av behandlingens karaktär hjälper Trimble kunden genom att tillhandahålla lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, för att kunden ska kunna uppfylla sina skyldigheter att besvara förfrågningar från registrerade som vill utöva sina rättigheter som registrerade enligt lagar och förordningar om dataskydd. I det fall kunden, vid sin användning av tjänsterna, inte har möjlighet att utöva dessa rättigheter på egen hand, ska Trimble uppfylla alla kommersiellt rimliga krav från kunden för att underlätta sådana åtgärder i den utsträckning det är juridiskt tillåtet för Trimble att göra det. I det fall det är tillåtet enligt lag ansvarar kunden för eventuella kostnader som uppstår till följd av Trimbles tillhandahållande av sådan assistans.

3.2 Direkta förfrågningar från den registrerade. Trimble ska, i den utsträckning det är tillåtet enligt lag, omedelbart meddela kunden om Trimble tar emot en begäran från en registrerad om att utöva sina rättigheter enligt avsnitt 3.1. Trimble ska inte svara på en sådan begäran från en registrerad utan att kunden först skriftligen samtyckt därtill, förutom för att bekräfta att begäran avser kunden, vilket kunden härmed samtycker till.

4. TRIMBLES OCH KUNDENS PERSONAL

4.1 Allmänt. Trimble och kunden ska vidta åtgärder för att säkerställa att varje fysisk person som agerar under deras bemyndigande och som har tillgång till kunddata, inte behandlar dessa kunddata annat än enligt instruktioner från kunden, såvida han eller hon inte är skyldig att göra det enligt lagar och förordningar om dataskydd.

4.2 Sekretess. Trimble ska se till att dess personal som arbetar med behandling av personuppgifter är informerade om personuppgifternas konfidentiella karaktär, har fått lämplig utbildning om sitt ansvar och har bekräftat sina sekretessåtaganden skriftligt. Trimble ska se till att sådana sekretesskyldigheter fortsätter att gälla även efter det att personalen avslutat sin tjänst.

4.3 Tillförlitlighet. Trimble ska vidta kommersiellt rimliga åtgärder för att säkerställa tillförlitligheten hos all personal hos Trimble som arbetar med behandling av personuppgifter.

4.4 Begränsning av tillgång. Trimble ska se till att personalens åtkomst till personuppgifter begränsas till de personer som utför tjänster i enlighet med Avtalet.

5. UNDERENTREPRENÖRER

5.1 Anlitande av underentreprenörer. Kunden bekräftar och samtycker till att (i) närstående bolag till Trimble kan anlitas som underentreprenörer, och att (ii) Trimble och Trimbles närstående bolag kan anlita tredjeparts-underentreprenörer i samband med tillhandahållandet av tjänsterna. I sådana fall ska Trimble och Trimbles närstående bolag, i ett kontrakt eller annan rättslig handling, ålägga underentreprenören dataskyddsskyldigheter som i allt väsentligt liknar dem som anges i detta DPA. Kontraktet eller annan form av rättslig handling ska ge tillräckliga garantier för att underentreprenören implementerar tillräckliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen kommer att uppfylla kraven i lagar och förordningar om dataskydd.

5.2 Förteckning över aktuella underentreprenörer och meddelande om nya underentreprenörer. Den aktuella förteckningen över underentreprenörer som anlitas för behandling av personuppgifter vid utförandet av varje aktuell tjänst, inklusive en beskrivning av på vilket sätt de behandlar uppgifter och vilket land de är lokaliserade i, finns på <https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center> under "Ytterligare resurser" ("Listor över underentreprenörer"). Kunden godkänner härmed dessa underentreprenörer, deras lokalisering och behandlingsaktiviteter när det gäller kundens personuppgifter och instruerar Trimble i enlighet därmed. Trimble kommer att informera om förändringar i förteckningen över underentreprenörer i sin versionsinformation ("release notes"), kunduppdateringar eller liknande kommunikation som ska betraktas som meddelande i enlighet med avsnitt [9.2 i EU:s standardavtalsklausuler].

5.3 Rätt att invända mot nya underentreprenörer. För att utöva sin rätt att invända mot Trimbles användande av en ny underentreprenör ska kunden utan dröjsmål meddela Trimble skriftligen till adressen privacy@trimble.com inom trettio (30) arbetsdagar efter mottagandet av Trimbles meddelande i enlighet med den mekanism som anges i avsnitt 5.2. Om kunden har invändningar mot en ny underentreprenör och invändningen inte är orimlig, kommer Trimble att vidta rimliga åtgärder för att göra en förändring av tjänsterna tillgänglig för kunden, eller rekommendera en kommersiellt rimlig ändring av kundens konfiguration eller användning av tjänsterna, för att undvika att den nya underentreprenören, som kunden invänt mot, behandlar personuppgifter. Dessa åtgärder ska inte belasta kunden på något orimligt sätt. Om Trimble inte kan göra en sådan ändring tillgänglig inom en rimlig tidsperiod, som inte får överstiga sextio (60) dagar, har kunden rätt att säga upp aktuell(a) beställning(ar) och avtal med avseende endast på de tjänster som inte kan tillhandahållas av Trimble utan användning av den nya underentreprenör som kunden invänt mot, genom att skriftligt upplysa Trimble om detta. Eventuella förutbetalda avgifter som gäller återstoden av löptiden för en sådan beställning, efter det datum då den i realiteten upphör att gälla, kommer Trimble att återbetala till kunden.

5.4 Ansvar. Trimble är ansvarigt för sina underentreprenörers handlingar och försummelser i samma utsträckning som om Trimble skulle ha utfört varje underentreprenörs tjänster direkt enligt villkoren i detta DPA, såvida ingenting annat sägs i Avtalet.

6. SÄKERHET, REVISIONER OCH HJÄLP

6.1 Säkerhet vid databehandling. Trimble ska upprätthålla administrativa, fysiska och tekniska skyddsåtgärder för att skydda säkerhet, konfidentialitet och integritet för kunddata, inklusive personuppgifter, enligt [bilaga 1](#). Trimble följer regelbundet upp efterlevnaden av dessa skyddsåtgärder. Trimble kommer inte att väsentligt minska den totala säkerheten för tjänsterna under Avtalets löptid.

6.2 Revisioner. Trimble arrangerar från tid till annan revisioner och inspektioner (inklusive, där det är rimligt, revisioner utförda externa revisorer) för att säkerställa efterlevnad av dataskyddslagar och detta DPA samt, om det är rimligt, branschstandarder som ISO 27001. Trimble ska på begäran göra all information som krävs (inklusive sådana revisionsrapporter) tillgängliga för kunden för att visa att Trimble uppfyller sina skyldigheter enligt tillämplig dataskyddslagstiftning och detta DPA. Beroende på vilken information som begärs ut kan Trimble kräva att kunden undertecknar ett sekretessavtal.

6.3 Hjälptill kunden. Trimble ska bistå kunden med att säkerställa uppfyllandet av skyldigheterna avseende säkerhet vid behandling, anmälan och kommunikation av personuppgiftsincidenter, konsekvensbedömning avseende dataskydd och förhandssamråd med tillsynsmyndigheten i enlighet med lagar och förordningar om dataskydd.

6.4 Hantering av och information om brott mot säkerheten. I händelse av en personuppgiftshändelse enligt lagar och förordningar om dataskydd upprätthåller Trimble policyer och förfaranden

för hantering av säkerhetsincidenter och ska, i den utsträckning det är tillåtet enligt lag, utan onödigt dröjsmål meddela kunden om sådan incident.

7. ÅTERLÄMNANDE OCH RADERING AV KUNDUPPGIFTER

När tjänsten inte längre tillhandahålls ska Trimble, efter kundens eget val, återlämna och/eller radera kunddata i enlighet med de procedurer och tidsramar som anges i Avtalet eller dess tjänstebeskrivning, såvida inte lagstiftning som åläggs kunden kräver lagring av kundens data.

8. BEGÄRAN OM ÅTKOMST FRÅN MYNDIGHETER

8.1 Såvida det inte är förbjudet enligt tillämplig lag ska Trimble informera kunden i allmänna ordalag ifall förfrågningar, beställningar eller liknande krav framförs av en domstol, behörig myndighet, brottsbekämpande myndighet eller annat statligt organ ("begäran från rättsvårdande myndighet") tas emot som rör behandlingen av personuppgifter enligt dessa klausuler.

8.2 Trimble kommer att invända mot och bestrida alla begäranden från rättsvårdande myndigheter genom att vidta rättsliga åtgärder i den utsträckning som de är rimliga med tanke på omständigheterna. Om Trimble genom en begäran från rättsvårdande myndigheter tvingas lämna ut personuppgifter som överförs enligt dessa klausuler, kommer Trimble, om det inte är förbjudet enligt tillämplig lag, att ge kunden information om detta i rimlig tid för att ge kunden möjlighet att skydda informationen eller vidta andra lämpliga åtgärder såvida inte Trimble är juridiskt förbjudet att göra detta.

8.3 Om Trimble gör personuppgifter tillgängliga för underentreprenörer kommer Trimble inte att välja underentreprenörer i ett land utanför Europeiska ekonomiska samarbetsområdet och som därmed inte är föremål för bedömning av adekvat skyddsnivå utifrån Europeiska unionens kommission, utan att först ha genomfört en företagsbesiktning som inkluderar (i) en granskning av eventuella transparensrapporter som görs tillgängliga av underentreprenören, och (ii) en bedömning av riskerna med överföringen.

9. BEHÖRIGA NÄRSTÅENDE BOLAG

9.1 Avtalsförhållande. Kunden går in i DPA-avtalet för egen räkning och, i förekommande fall, för behöriga närstående bolags räkning. Genom detta etableras ett separat DPA mellan Trimble och varje sådant behörigt närstående bolag. Varje behörigt närstående bolag är bundet av skyldigheterna enligt detta avtal. För att undvika tveksamheter är eller blir ett behörigt närstående bolag inte en part i Avtalet, utan endast en part i detta DPA. All tillgång till och användning av tjänsterna av behöriga närstående bolag måste följa villkoren i Avtalet. Varje överträdelse av villkoren i Avtalet av ett behörigt närstående bolag ska bedömas så som en överträdelse av kunden.

9.2 Kommunikation. Den kund som är avtalspart i Avtalet ska förbli ansvarig för att samordna all kommunikation med Trimble enligt detta DPA och ha rätt att kommunicera och ta emot information gällande detta DPA för sina behöriga närstående bolags räkning.

9.3 Behöriga närstående bolags rättigheter. Om ett behörigt närstående bolag blir en part i DPA-avtalet med Trimble ska det, i den utsträckning som krävs enligt tillämpliga lagar och förordningar om dataskydd tillskrivas de rättigheter och möjligheter att söka rättelse som föreskrivs i detta DPA. Om lagar och förordningar om dataskydd kräver att det behöriga närstående bolaget utövar en rättighet eller söker rättelse enligt detta DPA som personuppgiftsansvarig, ger det behöriga närstående bolaget härmed rätt till kunden att utöva sådana rättigheter å det behöriga närstående bolagets vägnar. Dessutom ska den kund som är avtalspart i Avtalet utöva sådana rättigheter som följer av detta DPA inte för varje behörigt närstående bolag individuellt, utan på ett samordnat sätt för alla dess behöriga närstående bolag tillsammans.

10. ANSVARBEGRÄNSNING

Varje ansvar som tillkommer parterna och dess närstående bolag till följd av detta DPA och alla andra DPA-avtal mellan behöriga närstående bolag och Trimble, oavsett om det grundar sig på kontrakt, skadeståndsansvar eller någon annan ansvarsgrund, omfattas av avsnittet "Ansvarsbegränsning" i Avtalet, och alla referenser till en parts ansvar i sådana avsnitt avser det sammantagna ansvaret för denna part och dess närstående bolag enligt Avtalet och alla DPS-avtal tillsammans. För att undvika tveksamheter ska Trimbles och dess närstående bolags totala ansvar för alla anspråk från kunden och dess behöriga närstående bolag som uppstår ur eller är relaterade till Avtalet och varje DPA gälla sammantaget för alla anspråk enligt både Avtalet och alla DPA som upprättats under sådant Avtal, inklusive av något behörigt närstående bolag, och ska, i synnerhet, inte tolkas som att gälla individuellt och solidariskt för varje behörigt närstående bolag som är kontraktspart i något sådant DPA-avtal. För att ytterligare undvika tveksamheter, avser varje referens till DPA i detta DPA just detta DPA och dess bilagor och appendix.

Om kunden har abonnerat på, eller köpt, tjänsterna genom en återförsäljare eller annan affärspartner till Trimble, är Trimbles och dess närstående bolags ansvar utifrån eller i samband med detta DPA och alla DPA-avtal mellan

behöriga närstående bolag och Trimble, oavsett om det gäller kontrakt, skadeståndsansvar eller någon annan ansvarsgrund, begränsat till (i den utsträckning det är tillåtet enligt lag) summan av de belopp som Trimble erhållit för dessa tjänster, dock maximalt 50 000 euro.

11. INTERNATIONELLA BESTÄMMELSER

11.1 Mekanism för gränsöverskridande överföring. I de fall Trimble behandlar personuppgifter som härrör från och skyddas av lagar och förordningar om dataskydd i någon av de jurisdiktioner som anges i bilaga 3 i detta DPA (Mekanism för gränsöverskridande överföring), gäller de villkor som anges i bilaga 3 med avseende på tillämplig(a) jurisdiktion(er) utöver villkoren i detta DPA.

11.2 Mekanism för överföring av data över nationsgränser. I de fall kundens användning av tjänsterna kräver en vidareöverföringsmekanism för att lagligt överföra personuppgifter från en jurisdiktion (t.ex. Europeiska ekonomiska samarbetsområdet, Storbritannien, Schweiz, Turkiet eller en annan jurisdiktion som anges i bilaga 3 (Mekanism för gränsöverskridande överföring) till Trimble som ligger utanför den jurisdiktionen ("överföringsmekanism"), kommer villkoren som anges i bilaga 4 (Mekanism för gränsöverskridande överföring) i detta DPA att gälla.

12. ÖVRIGT

12.1 Konflikt. I händelse av konflikt eller inkonsekvens mellan följande dokument kommer de att gälla i följande rangordning: (1) de tillämpliga villkor som anges i bilaga 4 (Mekanism för gränsöverskridande överföring) i detta DPA; (2) villkoren i detta DPA som ligger utanför bilaga 4 (Villkor specifika för en viss jurisdiktion); och (3) Avtalet.

12.2 Uppdateringar. Trimble kan komma att uppdatera villkoren i detta avtal från tid till annan. Trimble måste dock meddela kunden skriftligen minst trettio (30) dagar i förväg när en uppdatering krävs till följd av (a) förändringar i lagar och förordningar om dataskydd; (b) sammanslagning, förvärv eller annan liknande transaktion; eller (c) offentliggörandet av nya produkter eller tjänster eller väsentliga ändringar av befintliga tjänster. De vid varje tid aktuella villkoren för detta DPA finns tillgängliga på trimble.com/privacy

Kundens juridiska namn: _____

Adress _____

Kundnummer hos Trimble: _____

☐ Kunden har köpt tjänsterna via Trimbles

auktoriserade återförsäljare eller affärspartner

Återförsäljarens namn _____

Adress _____

Kundnummer hos återförsäljaren _____

☐ För EU/EES/UK-faktura till kunder. Kunden önskar ingå EU:s standardavtalsklausuler direkt med Trimble Inc. Om denna ruta inte är markerad gäller den överföringsmekanism för överföringen till Trimble Inc. som beskrivs i avsnitt 2.2 i bilaga 4, eller andra överföringsmekanismer som upprättats mellan Trimbles närstående bolag i Europa och Trimble Inc.

Om föregående ruta är markerad: Kunden betraktar följande moduler som tillämpliga:

☐ Modul 1/Kontrakt 1

☐ Modul 2/Kontrakt 2

☐ Modul 3/Kontrakt 3

☐ Kunden väljer att ingå detta DPA-avtal

Parternas behöriga undertecknare har vederbörligen upprättat detta avtal:

KUND (signerar härmed detta DPA)

Namn: _____

Titel _____

Datum: _____

Trimble Inc.

Underskrift: _____
Namnförtydligande: Jennifer Allison
Titel: Senior Vice President och General Counsel
Datum: 15.7.2024

Trimble UK Limited

Underskrift: _____
Namnförtydligande: RHH Reeder
Titel: Director
Datum: 15.7.2024

Trimble Solutions Sandvika AS

Underskrift: _____
Namnförtydligande: RHH Reeder
Titel: Director
Datum: 15.7.2024

Lakefield eTechnologies Limited

Underskrift: _____
Namnförtydligande: RHH Reeder
Titel: Director
Datum: 15.7.2024

Trimble Finland Corporation

Underskrift: _____
Namnförtydligande: Jürgen Kesper
Titel: Director
Datum: 15.7.2024

Trimble MAPS Limited.

Underskrift: _____
Namnförtydligande: RHH Reeder
Titel: Director
Datum: 15.7.2024

Trimble Tyskland GmbH

Underskrift: _____
Namnförtydligande: Jürgen Kesper
Titel: Director
Datum: 15.7.2024

Trimble Europe BV

Underskrift: _____
Namnförtydligande: RHH Reeder
Titel: Director
Datum: 15.7.2024

Trimble France SAS

Underskrift: _____
Namnförtydligande: RHH Reeder
Titel: Director
Datum: 15.7.2024

Trimble Technologies Ireland Limited

Underskrift: _____
Namnförtydligande: RHH Reeder
Titel: Director
Datum: 15.7.2024

Trimble International BV

Underskrift: _____
Namnförtydligande: RHH Reeder
Titel: Director
Datum: 15.7.2024

Trimble Germany GmbH

Underskrift: _____
Namnförtydligande: RHH Reeder
Titel: Director
Datum: 15.7.2024

Trimble Forestry Europe Corporation

Underskrift: _____
Namnförtydligande: RHH Reeder
Titel: Director
Datum: 15.7.2024

Kontaktuppgifter till alla Trimble-enheter:

privacy@trimble.com

Adresser till Trimble-enheter	
Trimble Inc.	Trimble Europe B.V.
10368 Westmoor Drive Westminster, CO 80021, USA	Industrieweg 187a 5683CC Best, the Netherlands
Trimble UK Limited	Trimble France SAS
Trimble House, Gelderd Road, Gildersome, Leeds LS27 7JP UK	1 Quai Gabriel Péri 94340 Joinville-le-Pont, Frankrike
Trimble Solutions Sandvika AS	Trimble Technologies Ireland Limited
Leif Tronstads plass 4 1337 Sandvika, Norge	North Point Business Park, Unit 3D North Point House, New Mallow Rd, Cork, T23 AT2P, Irland
Lakefield eTechnologies Limited	Trimble International BV
North Point Business Park, Unit 3D North Point House, New Mallow Rd, Cork, T23 AT2P, Irland	Industrieweg 187a 5683CC Best, the Netherlands
Trimble Finland Corporation	Trimble Germany GmbH
Hatsinanpuisto 8, 02600 Esbo, Finland	Am Prime Parc 11, 65479 Raunheim
Trimble MAPS Limited.	Trimble Forestry Europe Corporation
53-64 Chancery Lane, Holborn, London England WC2A 1QS UK	Hatsinanpuisto 8, 02600 Esbo, Finland
Trimble Tyskland GmbH	
Am Prime Parc 11, 65479 Raunheim	

BILAGA 1 - BESKRIVNING AV BEHANDLING

1. KATEGORIER AV REGISTRERADE VARS PERSONUPPGIFTER ÖVERFÖRS

Kunden kan lämna personuppgifter till tjänsterna. Personuppgifternas omfattning bestäms och kontrolleras av kunden efter eget gottfinnande, och uppgifterna kan inkludera, men är inte begränsade till personuppgifter som rör följande kategorier av registrerade:

- Kundens arbetare, tjänstemän, chefer och leverantörer
- Kundens kunder (som är fysiska personer), ofta i egenskap av mottagare av leveranser, tjänster och produkter
- Anställda, representanter, rådgivare, frilansare hos kundens kunder, leverantörer och motparter i fråga om transaktioner som behandlas genom tjänsterna
- Kundens användare som av kunden fått behörighet att använda tjänsterna

2. KATEGORIER AV PERSONUPPGIFTER SOM ÖVERFÖRS

Kunden kan lämna personuppgifter till tjänsterna. Personuppgifternas omfattning bestäms och kontrolleras av kunden efter eget gottfinnande, och uppgifterna kan inkludera, men är inte begränsade till följande kategorier av personuppgifter:

- Kontakt- och masterdata (för- och efternamn, titel, befattning)
- Kontaktuppgifter (företag, e-postadress, telefon, fysisk företagsadress)
- ID-uppgifter såsom pass, körkort, IP-adresser, unika identifierare (UUID)
- Yrkes- och utbildningsdata (kvalifikationer, erfarenheter, färdigheter)
- Jobbrelaterade data (utförda tjänster, bidrag i projekt, tilldelade jobb och arbetsuppgifter, prestationsrelaterade data, tjänstetimmor, utgifter)
- Lokaliseringsdata
- Avtalsrelaterade data (fakturerings, betalning, transaktionshistorik)
- Historik över interaktioner

3. KÄNSLIGA UPPGIFTER SOM ÖVERFÖRS (OM TILLÄMPLIGT)

Känsliga uppgifter som överförs (i tillämpliga fall) och tillämpade begränsningar eller skyddsåtgärder där full hänsyn tas till uppgifternas karaktär och de medföljande riskerna, till exempel strikt ändamålsbegränsning, åtkomstbegränsningar (däribland åtkomst endast för personal som har specialutbildning), registrering av åtkomst till uppgifterna, begränsningar av vidare överföringar eller ytterligare säkerhetsåtgärder.

Uppgiftsutföraren kan komma att föra in särskilda kategorier av uppgifter i tjänsterna. I vilken utsträckning detta sker bestäms och kontrolleras av uppgiftsutföraren efter eget gottfinnande. För tydlighets skull avser detta personuppgifter med information som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska eller biometrisk data för unik identifiering av en fysisk person, uppgifter om hälsa eller en persons sexualliv eller sexuella läggning.

De tillämpliga säkerhetsåtgärderna beskrivs i avsnitt 11 i bilaga 2 nedan.

4. ÖVERFÖRINGARNAS FREKVENS

Hur ofta överföringen sker (t.ex. ifall uppgifterna överförs som en engångshändelse eller kontinuerligt):

Kontinuerlig basis beroende på kundens användning av tjänsterna.

5. BEHANDLINGENS KARAKTÄR

Behandlingens karaktär är utförandet av tjänsterna enligt Avtalet.

6. SYFTET MED BEHANDLINGEN, DATAÖVERFÖRINGEN OCH VIDARE BEHANDLING

Trimble kommer att behandla personuppgifter om det är nödvändigt för att utföra tjänsterna enligt Avtalet, enligt vad som anges i dokumentationen, och i enlighet med kundens instruktioner vid dennes användning av tjänsterna. Trimble kommer vidare att anonymisera personuppgifter för att kunna utföra dataanalys och utveckling av tjänster.

7. BEHANDLINGENS VARAKTIGHET

Den period under vilken personuppgifterna kommer att behållas, eller, om det inte är möjligt, de kriterier som används för att fastställa denna period:

Trimble kommer att behandla personuppgifter enligt vad som anges i Avtalet, om inte annat överenskommits, till exempel i avsnitt 9 i DPA-avtalet.

8. ÖVERFÖRINGAR TILL UNDERENTREPRENÖR

Vid överföringar till personuppgiftsbiträden/underentreprenörer, ange även föremålet för behandlingen liksom dess karaktär och varaktighet.

Underentreprenören kommer att behandla personuppgifter om det är nödvändigt för att utföra tjänsterna enligt Avtalet. Som följer av avsnitt 9 i detta DPA kommer underentreprenören att behandla personuppgifter under avtalets löptid, om inte annat skriftligen överenskommits.

De underentreprenörer som anlitas för att tillhandahålla tjänsterna och vilket land de har sin verksamhet i framgår under fliken "Ytterligare material" på trimble.com/privacy.

BILAGA 2 - Tekniska och organisatoriska säkerhetsåtgärder

I tillämpliga fall kommer denna bilaga 2 även att fungera som Bilaga II till EU:s standardavtalsklausuler.

Teknisk och organisatorisk säkerhetsåtgärd

1. Åtgärder för pseudonymisering och kryptering av personuppgifter

Om möjligt krypterar Trimble data som överförs mellan kunder och Trimbles program via offentliga nätverk. Vid kryptering används TLS 1.2 eller senare. Kunddata som lagras på system som handhas av Trimble (för AICPA-certifierade produkter - se punkt 7 nedan för mer information) krypteras med AES 256 eller starkare metod.

2. Åtgärder för att säkerställa fortlöpande konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlande system och tjänster

Trimble har särskild personal för cybersäkerhet som ansvarar för att övervaka säkerhet och integritet. Trimble har utöver ett dataskyddsbud också utsett ansvariga för cybersäkerhet och integritet, samt ett råd av tekniska chefer, "Engineering Leadership Council" som träffas kvartalsvis för att diskutera sekretess- och säkerhetsrisker som hanteras inom sektorns produktportföljer. Dessutom följs risker med produkten upp i en intern portal där efterlevnaden övervakas månatligen.

3. Åtgärder för att säkerställa möjligheten att återställa tillgängligheten och tillgången till personuppgifter inom rimlig tid i händelse av en fysisk eller teknisk incident

För att upprätthålla tillgängligheten till Trimbles SaaS-produkter (Software as a Service, molntjänster som tillhandahåller programvara över internet) förlitar sig Trimble på branschledande molntjänstleverantörer (Amazon Web Services (AWS) och Microsoft Azure) för automatisk skalning, geografiskt åtskilda datacenter, omfattande program- och infrastrukturövervakning och supportmekanismer som är tillgängliga dygnet runt.

Trimble upprätthåller säkerhetskopior av lagrade data, inklusive kunddata, som stöder de primära funktionerna i Trimble-programmen. Där så är möjligt lagras säkerhetskopiorna på en plats som är geografiskt skild från den primära datalagringsplatsen.

Utöver de åtgärder som vidtas av våra tjänstleverantörer, upprätthåller Trimble en funktion för hantering av säkerhetsincidenter, som inkluderar en dokumenterad policy för incidenthantering och en plan för att triagera (bedöma, kategorisera och prioritera) säkerhetshändelser och incidenter som involverar kunddata. Detta definierar motåtgärder vid säkerhetsincidenter såsom inneslutning, utrotning, återställande och kommunikationsaktiviteter, samt roller och ansvar för Trimbles personal och ett krav på att i efterhand gå igenom incidenten med Trimbles ledning.

4. Processer för regelbunden testning, bedömning och utvärdering av effektiviteten hos tekniska och organisatoriska åtgärder för att säkerställa en säker behandling

Trimble använder oberoende tredjepartsföretag för att utföra periodiska penetrationstester, inklusive Sarbanes-Oxley, PCI, SOC 1, typ II, SOC 2 typ II, ISO27001 eller NIST 800-171 eller motsvarande revisioner på årsbasis där så krävs för att uppfylla kraven i lagstiftningen. Dessutom genomför Trimble regelbundna interna sårbarhetstester och penetrationstester på tillämpliga produkter och plattformar i samband med Trimbles policykrav och program för cybersäkerhet. Trimble kan utföra bedömningar av nya leverantörer eller partners om affärsrisken motiverar granskning. Trimble uppmuntrar tredje part att rapportera eventuella cybersäkerhetsproblem, incidenter och sårbarheter som är förknippade med våra produkter, tjänster eller webbplatser.

5. Åtgärder för identifiering och godkännande av användare

För produkter som utnyttjar Trimble ID (TID, Trimble Identity) för autentisering behandlar Trimble lösenordet på ett säkert sätt. Dessutom kan vissa Trimble-produkter ha stöd för integrering av en enda inloggning (single sign-on, SSO) med en leverantör av kundidentiteter som använder SAML (Security Assertion Markup Language) och MFA (Multifactor Authentication).

6. Åtgärder för skydd av uppgifter under överföring

Som framgår av punkt 1 krypterar Trimble kunddata som överförs via offentliga nätverk mellan kunden och Trimble-programmet med hjälp av aktuella krypteringschiffer när så är möjligt.

7. Åtgärder för skydd av uppgifter under lagring

Som framgår av punkt 1 krypteras kunddata som lagras på system som handhas av Trimble med AES 256 eller starkare för alla Trimble-produkter; för närvarande AICPA SOC 1, typ II, SOC 2, typ II eller NIST 800-171-certifierade. Se punkt 11 för mer detaljerad information.

8. Åtgärder för att säkerställa fysisk säkerhet på platser där personuppgifter behandlas

Trimbles SaaS-produkter, program och tjänster har ofta kunddata som lagras i datacenter som tillhandahålls av Amazon Web Services (AWS), Microsoft Azure eller Google Cloud Platform (GCP). Därav följer att Trimble förlitar sig på den fysiska, miljömässiga och infrastrukturmässiga styrningen av dessa plattformar. Trimble granskar regelbundet certifieringar och tredjepartsintyg som tillhandahålls av dessa leverantörer och som bedömer hur effektivt deras datacenter styrs.

9. Åtgärder för att säkerställa loggning av händelser

Trimble upprätthåller många loggar för cybersäkerhetsverktyg och loggar för säkerhetsgranskning av program och infrastruktur. Säkerhetsloggarna analyseras med hjälp av SIEM-teknik i kombination med händelsekorrelation för att upptäcka onormal aktivitet.

10. Åtgärder för att säkerställa systemkonfiguration, inklusive standardkonfiguration

Trimble utnyttjar gemensamma branschstandarder för att stärka cybersäkerheten genom säker konfiguration och flernivåförsvar. Trimble utför säkerhetskorrigeringar av sina system i enlighet med Trimble Secure Development Lifecycle Policy (TSDLCP).

11. Åtgärder för styrning och förvaltning av intern IT och IT-säkerhet

För Trimble-produkter som är certifierade enligt SOC 1, typ II, SOC 2, typ II eller NIST 800-171 tillämpas för personal som har tillgång till kunddata rollbaserade principer och principer för minsta möjliga behörighet för att kontrollera åtkomst. Personalen får inte större åtkomst till kunddata än vad som är absolut nödvändigt för att de ska kunna utföra sina arbetsuppgifter på ett säkert sätt. Fjärråtkomst till Trimbles system kräver krypterad kommunikation via säkra protokoll och användning av flerfaktorsautentisering. Trimble har upprättat och kommer att upprätthålla rutiner för lösenordshantering för denna personalgrupp, utformade för att säkerställa att lösenord är unika för varje individ och ej åtkomliga för obehöriga personer. Rutinerna har en lägstanivå som inkluderar att:

- kryptografiskt skydda lösenord när de lagras i datorsystem eller i befinner sig transit över ett offentligt nätverk;
- ändra standardlösenord från leverantörer; och
- utbildning i bra lösenordsrutiner, såsom att använda lösenfraser
- personalens tillgång till produktionsinfrastruktur kräver multifaktoraautentisering (MFA).

I enlighet med kraven för ISO 27001-certifikat och för att säkerställa korrekt och effektiv användning av kryptografi för att skydda sekretessen och integriteten för data som ägs eller hanteras av Trimble-avdelningar, måste data som klassificeras som konfidentiella eller begränsade krypteras genom användning av giltiga krypteringsprocesser för data i vila och i rörelse enligt krav i förordning och/eller riskbedömning. Detta inkluderar men är inte begränsat till känslig information som lagras på mobila enheter, flyttbara enheter och bärbara datorer. Trimble-avdelningar kommer endast att använda icke-modifierade, kommersiella krypteringsprogram för att kryptera data i vila och/eller under transport.

Trimbles personal omfattas av sekretessförpliktelser och olika policyer, till exempel policyer för godtagbar användning (av informationssystem), dataklassificering, säker förstörelse och MFA. Trimble kräver att personalen genomgår utbildning i informationssäkerhetsmedvetenhet, både när de börjar sin anställning och därefter årligen. Trimble kräver också att dess personal genomgår integritetsutbildning årligen (inklusive för att följa GDPR).

För tillämpliga produkter har Trimble implementerat säkerhet och integritet genom designprinciper, inklusive men inte begränsat till modellering av hot och produktapplikationspenetrationstester.

12. Åtgärder för certifiering/försäkran av processer och produkter

Trimble kommer att upprätthålla SOC 2-, Typ II-, ISO 27001- eller NIST 800-171-certifieringar och genomgå regelbundna externa övervaknings- och omcertifieringsrevisioner för att säkerställa att dess ledningssystem för informationssäkerhet (ISMS) uppfyller kraven i denna standard för tillämpliga produkter.

Trimble kommer att upprätthålla informationssäkerhetspolicyer som uppfyller kraven i ISO 27001-standarden, ett internt revisionsprogram som utvärderar Trimbles ISMS och informationssäkerhetskontroller, och en ledningskommitté som ansvarar för tillsynen av Trimbles ledningssystem för informationssäkerhet (ISMS).

13. Åtgärder för att säkerställa dataminimering

Trimble kan tillåta besökare att använda vissa funktioner i vissa produkter anonymt och minimerar de uppgifter som avkrävs från kunder till vad som är nödvändigt för att tillhandahålla den tjänst som begärs enligt lokala lagar och förordningar.

14. Åtgärder för att säkerställa datakvalitet

Trimble säkerställer kvaliteten på sina data genom olika verifieringsmekanismer som är unika för tillämpliga Trimble-produkter. Trimble kan också tillåta produktanvändare att uppdatera informationen på sina konton själva eller genom förfrågningar till sina kundsupportfunktioner.

15. Åtgärder för att säkerställa begränsad lagring av uppgifter

Trimble kan implementera kundens datalagringspolicy och ange lagringsperioder för olika typer av data.

16. Åtgärder för att möjliggöra dataportabilitet och säkerställa radering

Tillämpliga Trimble-produkter har en process för att raderat kunddata inom 30 dagar efter mottagande av en skriftlig förfrågan från kund, och kan erbjuda möjligheten att hämta kunddata för att tillhandahålla till alternativa tjänsteleverantörer enligt GDPR.

17. Kontroll och hantering av tredje part (underentreprenör)

Trimble anlitar endast underentreprenörer som behandlar personuppgifter för Trimbles räkning, som en del av tillämpliga prenumerationstjänster, i enlighet med lagar och förordningar om dataskydd. Innan en underentreprenör anlitas och personuppgifter överförs verifierar Trimble också de tekniska och organisatoriska åtgärder som underentreprenören vidtagit för att säkerställa en säkerhetsnivå som är rimlig med beaktande av de risker som är förknippade med att behandla dess kunders data. Trimble vidtar också rimliga åtgärder för att säkerställa säkerheten vid överföring av kunddata till underentreprenörer (tredje part). Som ett minimum innefattar sådana åtgärder: identifiering av vilka hot som finns mot kundens och de registrerades rättigheter baserat på behandlingens karaktär, omfattning och ändamål; granskning av vilken styrning av säkerhet och dataskydd som implementerats av underentreprenören för att skydda kundens data (inklusive SOC 2 typ II-granskningsrapporter och/eller ISO 27001-certifikat, om tillämpligt); införande av kontraktsvillkor som skyddar personuppgifter i samma eller liknande utsträckning som Trimble är ålagda att erbjuda sina kunder (inklusive giltiga mekanismer för gränsöverskridande data, hantering av underentreprenörer och program för efterlevnad); ställa krav på underentreprenören att endast behandla kunddata på uppdrag av Trimble och dess kunder och begränsning av behandlingen av kunddata till sådan behandling som sker enligt instruktioner från Trimble.

BILAGA 3 – Gränsöverskridande överföringsmekanism

1. Europeiska ekonomiska samarbetsområdet (EES):

1.1 Definitionen av "lagar och förordningar om dataskydd" omfattar den allmänna dataskyddsförordningen (EU 2016/679) ("**GDPR**").

1.2 När Trimble anlitar en underentreprenör enligt avsnitt 5.1 (Anlitande av underentreprenörer) i detta DPA kommer Trimble att:

(a) kräva att anlitad underentreprenör skyddar kunddata enligt den standard som krävs enligt lagar och förordningar om dataskydd och ålägger underentreprenören samma skyldigheter inom dataskydd som refereras till i artikel 28(3)

i GDPR, särskilt när det gäller att tillhandahålla tillräckliga garantier för implementerandet av lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen kommer att uppfylla kraven i GDPR, och

(b) kräva att en anlitad underentreprenör (i) skriftligen samtycker till att endast behandla personuppgifter i länder som Europeiska unionen har förklarat har en "adekvat" skyddsnivå eller (ii) endast behandla personuppgifter på grundval av EU:s standardavtalsklausuler eller i enlighet med bindande företagsregler som godkänts av kompetenta dataskyddsmyndigheter i Europeiska unionen.

1.3 Utan hinder av något annat i detta DPA eller i Avtalet (inklusive, men inte begränsat till, endera partens ersättningsskyldigheter), kommer ingen av parterna att vara ansvarig för eventuella GDPR-böter som utfärdats eller tagits ut enligt artikel 83 i GDPR mot den andra parten av en tillsynsmyndighet eller ett statligt organ i samband med sådan annan parts överträdelse av GDPR.

1.4 Kunden är införstådd med att Trimble, såsom personuppgiftsansvarig, i enlighet med lagar och förordningar om dataskydd, kan vara tvungen att meddela en tillsynsmyndighet om säkerhetsincidenter som involverar kunders användaruppgifter. Om en tillsynsmyndighet kräver att Trimble meddelar berörda registrerade med vilka Trimble inte har någon direkt relation (t.ex. kundens slutanvändare), kommer Trimble att meddela kunden om detta krav. Kunden kommer att bistå Trimble i rimlig omfattning med att meddela berörda registrerade.

2. Storbritannien (UK):

2.1 Referenser i detta DPA till "GDPR" kommer att betraktas som refererande till motsvarande lagar och förordningar i Storbritannien, inklusive, men inte begränsat till, UK GDPR och Data Protection Act 2018.

2.2 När Trimble anlitar en underentreprenör enligt avsnitt 5.1 (Anlitande av underentreprenörer) i detta DPA kommer Trimble att:

(a) kräva att anlitad underentreprenör skyddar kunddata enligt den standard som krävs enligt lagar och förordningar om dataskydd, såsom att inkludera samma dataskyddsskyldigheter som avses i artikel 28(3) i UK GDPR, särskilt genom att tillhandahålla tillräckliga garantier för genomförandet av lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen kommer att uppfylla kraven i UK GDPR, och

(b) kräva att en utsedd underentreprenör (i) skriftligen samtycker till att endast behandla personuppgifter i ett land som Storbritannien har förklarat har en "adekvat" skyddsnivå eller (ii) endast behandlar personuppgifter på ett sätt som motsvarar UK International Data Transfer Agreement eller EU:s standardavtalsklausuler med tillägg av UK International Data Transfer Addendum eller i enlighet med bindande företagsregler som godkänts av behöriga dataskyddsmyndigheter i Storbritannien.

2.3 Utan hinder av något annat i detta DPA eller i avtalet (inklusive, men inte begränsat till, endera partens ersättningsskyldigheter), kommer ingen av parterna att vara ansvarig för eventuella UK GDPR-böter som utfärdats eller tagits ut enligt artikel 83 i UK GDPR mot den andra parten av en tillsynsmyndighet eller ett statligt organ i samband med sådan annan parts överträdelse av UK GDPR.

2.4 Kunden är införstådd med att Trimble, såsom personuppgiftsansvarig, i enlighet med lagar och förordningar om dataskydd, kan vara tvungen att meddela en tillsynsmyndighet om säkerhetsincidenter som involverar kunders användaruppgifter. Om en tillsynsmyndighet kräver att Trimble meddelar berörda registrerade med vilka Trimble inte har någon direkt relation (t.ex. kundens slutanvändare), kommer Trimble att meddela kunden om detta krav. Kunden kommer att bistå Trimble i rimlig omfattning med att meddela berörda registrerade.

3. Schweiz:

3.1 Definitionen av "lagar och förordningar om dataskydd" inkluderar den schweiziska federala lagen om dataskydd, ("**FADP**").

3.2 När Trimble anlitar en underentreprenör enligt avsnitt 5.1 (Anlitande av underentreprenörer) i detta DPA kommer Trimble att:

(a) kräva att anlitad underentreprenör skyddar kunddata enligt den standard som krävs enligt lagar och förordningar om dataskydd, särskilt genom att tillhandahålla tillräckliga garantier för implementerandet av lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen kommer att uppfylla kraven i FADP, och

(b) kräva att en anlitad underentreprenör (i) skriftligen samtycker till att endast behandla personuppgifter i länder som Schweiz har förklarat har en "adekvat" skyddsnivå eller (ii) endast behandlar personuppgifter på ett sätt som motsvarar EU:s standardavtalsklausuler inklusive de ändringar som uppges i avsnitt 3.3 eller i enlighet med bindande företagsregler som godkänts av behöriga dataskyddsmyndigheter i Europeiska unionen eller Schweiz.

3.3 I den utsträckning som överföringar av personuppgifter från Schweiz omfattas av EU:s standardavtalsklausuler i enlighet med avsnitt 2.3 i bilaga 3 (EU:s standardavtalsklausuler), är parterna överens om att göra alla ändringar i EU:s standardavtalsklausuler som anses nödvändiga av den schweiziska federala dataskyddskommissionären, Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB). Dessa är, vid tidpunkten för slutförandet av detta DPA, specifikt:

(a) hänvisningar till "EU-medlemsstat" och "medlemsstat" ska tolkas så att de omfattar Schweiz, och

(b) i den mån överföringen eller vidareöverföringen omfattas av FADP:

(i) hänvisningar till "Förordning (EU) 2016/679" ska tolkas som hänvisningar till FADP:

(ii) den "behöriga tillsynsmyndigheten" i Bilaga I, del C kommer att vara den schweiziska federala dataskyddskommissionären, Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB).

(iii) i Paragraf 17 (Alternativ 1) regleras EU:s standardavtalsklausuler av lagstiftningen i Schweiz; och

(iv) i Paragraf 18 (b) i EU:s standardavtalsklausuler kommer tvister att lösas vid domstolarna i Schweiz.

(v) Paragraf 18(c) i EU:s standardavtalsklausuler gäller, samtidigt som en registrerad också kan väcka talan mot uppgiftsutföraren och/eller uppgiftsinföraren vid domstolarna i Schweiz där den registrerade har sin hemvist.

4. Amerikas förenta stater:

4.1 "**US State Privacy Laws**" avser alla statliga lagar som rör skydd och behandling av personuppgifter som gäller i USA, vilket kan inkludera, men inte är begränsat till, California Consumer Privacy Act, ändrad genom California Privacy Rights Act ("**CCPA**"), Virginia Consumer data Protection Act, Colorado Privacy Act, Connecticut data Privacy Act och Utah Consumer Privacy Act.

4.2 Definitionen av "lagar och förordningar om dataskydd" omfattar US State Privacy Laws.

4.3 Följande villkor gäller när Trimble behandlar personuppgifter som omfattas av CCPA:

(a) termen "**personuppgifter**" ("personal information"), som används i detta avsnitt 4.3 kommer att ha den betydelse som anges i CCPA;

(b) Trimble är en tjänsteleverantör vid behandling av kunddata. Trimble kommer att behandla personuppgifter som finns i kunddata endast för de affärsändamål som anges i Avtalet, inklusive syftet med behandlingen och behandlingsaktiviteter som anges i detta DPA ("**Ändamål**"). Som tjänsteleverantör kommer Trimble inte att sälja eller dela kunddata, och inte heller behålla, använda eller lämna ut kunddata (i) för något annat ändamål än Syftet, inklusive att behålla, använda eller avslöja kunddata för ett annat kommersiellt syfte än Syftet, eller som på annat sätt tillåts av CCPA; eller (ii) utanför det direkta affärsförhållandet mellan kunden och Trimble;

(c) Trimble kommer att (i) uppfylla de skyldigheter som gäller för företaget som tjänsteleverantör enligt CCPA och (ii) tillhandahålla personuppgifter med samma nivå av integritetsskydd som krävs enligt CCPA. Kunden är ansvarig för att säkerställa att den har uppfyllt och kommer att fortsätta att uppfylla kraven i CCPA vid sin användning av tjänsterna och sin egen behandling av personuppgifter;

(d) Kunden har rätt att vidta rimliga och lämpliga åtgärder för att säkerställa att Trimble använder personuppgifter på ett sätt som överensstämmer med kundens skyldigheter enligt CCPA;

(e) Trimble kommer att meddela kunden om Trimble kommer fram till att det inte längre kan uppfylla sina skyldigheter som tjänsteleverantör enligt CCPA;

(f) Efter ett sådant meddelande har kunden rätt att vidta rimliga och lämpliga åtgärder i enlighet med Avtalet för att stoppa och åtgärda obehörig användning av personuppgifter;

(g) Trimble kommer att tillhandahålla assistans i rimlig omfattning och inom rimlig tid för att hjälpa kunden att uppfylla sina skyldigheter med avseende på konsumentförfrågningar enligt vad som anges i Avtalet;

(h) för varje underentreprenör som anlitas av Trimble för att behandla personuppgifter som omfattas av CCPA, kommer Trimble att se till att Trimbles avtal med sådan underentreprenör överensstämmer med CCPA, inklusive, men inte begränsat till, kontraktskraven för tjänsteleverantörer och uppdragstagare;

(i) Trimble kommer inte att kombinera kunddata som Trimble tar emot från, eller på uppdrag av, kunden med personuppgifter som Trimble tar emot från, eller på uppdrag av, någon annan person eller personer, eller samlar in genom egen interaktion med konsumenten, såvida inte ett sådant kombinerande av data krävs för att utföra något affärsändamål som tillåts av CCPA, inklusive eventuella förordningar därtill, eller av föreskrifter som antagits av California Privacy Protection Agency; och

(j) Trimble intygar att det förstår och kommer att uppfylla sina skyldigheter enligt CCPA.

4.4 Trimble bekräftar att det inte tar emot kunddata som ersättning för tjänster som tillhandahålls kunden.

5. Australien:

5.1 Definitionen av "Lagar och förordningar om dataskydd" omfattar Australian Privacy Principles och Australian Privacy Act (1988).

5.2 Definitionen av "Personuppgifter" omfattar eng. "Personal Information" såsom det definieras i lagar och förordningar om dataskydd.

5.3 Definitionen av "Känsliga uppgifter" omfattar eng. "Sensitive Information" såsom det definieras i lagar och förordningar om dataskydd.

6. Brasilien:

6.1 Definitionen av "Lagar och förordningar om dataskydd" omfattar Lei Geral de Proteção de Dados (General personal data Protection Act).

6.2 Definitionen av "Säkerhetsincident" omfattar säkerhetsincident som kan leda till relevant risk eller skada för registrerade.

6.3 Definitionen av "Personuppgiftsbiträde" omfattar eng. "operator" såsom det definieras i lagar och förordningar om dataskydd.

7. Kanada:

7.1 Definitionen av "Lagar och förordningar om dataskydd" omfattar Federal Personal Information Protection and Electronic Documents Act.

7.2 Trimbles underentreprenörer, enligt Avsnitt 5 (Underentreprenörer) i detta DPA, är tredjeparter enligt lagar och förordningar om dataskydd, med vilka Trimble har ingått ett skriftligt kontrakt som innehåller villkor som väsentligen liknar detta DPA. Trimble har genomfört lämplig due diligence-granskning av sina underentreprenörer.

7.3 Trimble kommer att implementera tekniska och organisatoriska åtgärder enligt Avsnitt 11 i bilaga 2 (Säkerhet) i detta DPA.

8. Israel:

8.1 Definitionen av "Lagar och förordningar om dataskydd" omfattar Protection of Privacy Law.

8.2 Definitionen av "Personuppgiftsansvarig" omfattar eng. "Database Owner" såsom det definieras i lagar och förordningar om dataskydd.

8.3 Definitionen av "Personuppgiftsbiträde" omfattar eng. "Holder" såsom det definieras i lagar och förordningar om dataskydd.

8.4 Trimble kommer att kräva att all personal som är behörig att behandla kunddata följer principen om tystnadsplikt och har fått information om lagar och förordningar om dataskydd. Sådan personal undertecknar sekretessavtal med Trimble i enlighet med Avsnitt 6 (Sekretess) i detta DPA.

8.5 Trimble måste vidta tillräckliga åtgärder för att säkerställa de registrerades integritet genom att genomföra och upprätthålla de säkerhetsåtgärder som anges i Avsnitt 11 i bilaga 2 (Säkerhet) i detta DPA och följa villkoren i Avtalet.

8.6 Trimble måste se till att personuppgifterna inte överförs till någon underentreprenör såvida inte denna underentreprenör har ingått ett avtal med Trimble i enlighet med avsnitt 5.1 (Anlitande av underentreprenörer) i detta DPA.

9. Japan:

9.1 Definitionen av "Lagar och förordningar om dataskydd" omfattar Act on the Protection of Personal Information ("APPI").

9.2 Definitionen av "personuppgifter" inkluderar information om en specifik individ enligt avsnitt 2(1) i APPI, som kunden anförtror Trimble under den tid som Trimble tillhandahåller tjänsterna till kunden.

9.3 Trimble samtycker till att upprätthålla ett integritetsprogram som överensstämmer med de standarder som föreskrivs i reglerna som ställts upp av Japans Personal Information Protection Commission gällande behandling av personuppgifter i enlighet med bestämmelserna i kapitel 4 i APPI. Därav följer att:

(a) Trimble kommer att (i) att behandla personuppgifter som är nödvändiga för att tillhandahålla tjänsterna till kunden i enlighet med Avtalet på det sätt som beskrivs i bilaga 1 (Beskrivning av behandlingen) i detta DPA ("Syftet med behandlingen") och (ii) inte behandla personuppgifter för något annat ändamål än Syftet med behandlingen utan kundens samtycke;

(b) Trimble kommer att implementera och upprätthålla åtgärder som är lämpliga och nödvändiga för att förhindra obehörigt röjande och förlust av personuppgifter och för säker hantering av personuppgifter i enlighet med APPI enligt bilaga 2 (Tekniska och organisatoriska säkerhetsåtgärder) till detta DPA;

(c) Trimble kommer att meddela kunden om (i) Trimble underlåtit att följa avsnitt 9.3(a) i denna bilaga 3 eller (ii) Trimble upptäckt en säkerhetsincident som påverkar kunddata, i båda fallen i enlighet med avsnitt 6.4 i detta DPA. Trimble kommer att ge kunden rimlig assistans i händelse av att kunden är skyldig att meddela en tillsynsmyndighet eller någon registrerad person som påverkas av en säkerhetsincident;

(d) Trimble kommer att se till att alla dess anställda som har tillgång till personuppgifter (i) har ingått en överenskommelse med arbetsgivaren om att hålla sådana personuppgifter konfidentiella och (ii) och som bryter mot sekretessen kommer att bli föremål för disciplinära åtgärder och eventuell uppsägning; (iii) utföra lämplig personalövervakning och utbildning för att säkerställa en säker hantering av personuppgifter; och (iv) begränsa antalet anställda med behörighet, inklusive bland Trimbles anställda, som har tillgång till uppgifter kontrollera sådan åtkomst så att den bara är tillåten under den tid som krävs för Syftet med behandlingen.

(e) Trimble kommer inte att lämna ut personuppgifter till någon tredje part, förutom om kunden har gett Trimble tillåtelse att göra det i Avtalet. När Trimble anlitar underentreprenörer kommer Trimble att följa kraven i avsnitt 9 (Underentreprenörer) i detta DPA för att säkerställa att rutiner finns på plats för att upprätthålla sekretessen och säkerheten för personuppgifter;

(f) Trimble kommer att föra register över den hantering av personuppgifter som anförtrots Trimble av kunden, och som utförs för kundens räkning;

(g) Kunden kan bedöma Trimbles efterlevnad av dess skyldigheter enligt lagar och förordningar om dataskydd och enligt vad som anges i avsnitt 6 i detta DPA.

(h) Trimble kommer att samarbeta med kunden i rimlig omfattning och efter skriftlig begäran, om kunden rapporterar till japanska Personal Information Protection Commission eller andra tillsynsmyndigheter; och

(i) Trimbles primära anläggningar där data behandlas är belägna i USA och, beroende på kundens användning av tjänsterna, kan behandling också ske från de platser som anges på <https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center> under "Ytterligare resurser"

("Listor över underentreprenörer"). Trimble kommer att meddela kunden om eventuella ändringar och ger kunden möjlighet att komma med invändningar i enlighet med avsnitt 9 i detta avtal. Om Trimble behandlar personuppgifter i något annat land än Japan kommer Trimble att säkerställa efterlevnaden av sitt integritetsprogram såsom det beskrivs i detta DPA.

9.4 Följande villkor gäller för samtycke från den registrerade:

(a) Kunden anförtror Trimble personuppgifter för Syftet med behandlingen. Kunden samtycker till att Trimble inte är en "tredje part" såsom termen används i APPI-bestämmelserna som begränsar tillhandahållandet av personuppgifter till tredje part. Därigenom gäller inte kravet på att inhämta samtycke från den registrerade i förväg;

(b) om samtycke från den registrerade krävs enligt artikel 4 i Telecommunications Business Act, kommer kunden att uppfylla alla krav på samtycke som är specifika för dess användning av tjänsterna.

10. Mexiko:

10.1 definitionen av "lagar och förordningar om dataskydd" omfattar Federal Law for the Protection of Personal Data Held by Private Parties och dess förordningar.

10.2 När Trimble agerar som personuppgiftsbiträde kommer Trimble att:

(a) behandla personuppgifter i enlighet med kundens instruktioner såsom anges i avsnitt 5 i detta DPA;

(b) behandla personuppgifter endast i den utsträckning det är nödvändigt för att tillhandahålla tjänsterna;

(c) genomföra säkerhetsåtgärder i enlighet med lagar och förordningar om dataskydd och bilaga 2 (Tekniska och organisatoriska åtgärder) i detta DPA;

(d) hålla de personuppgifter som behandlas konfidentiella i enlighet med Avtalet;

(e) radera alla personuppgifter vid uppsägning av Avtalet i enlighet med avsnitt 10 (Återlämnande och radering av kunduppgifter) i detta DPA; och

(f) endast överföra personuppgifter till underentreprenörer i enlighet med avsnitt 9 (Underentreprenörer) i detta DPA.

11. Singapore:

11.1 Definitionen av "lagar och förordningar om dataskydd" omfattar Personal Data Protection Act 2012 ("**PDPA**").

11.2 Trimble kommer att behandla personuppgifter med en skyddsstandard som överensstämmer med PDPA genom att implementera lämpliga tekniska och organisatoriska åtgärder såsom anges i bilaga 2 (Tekniska och organisatoriska åtgärder) i detta DPA, och följa villkoren i Avtalet.

12. Turkiet

12.1 Definitionen av "lagar och förordningar om dataskydd" omfattar (i) Law on the Protection of Personal Data (PDPL), Lag nummer 6698, från den 24 mars 2016, med ändringar genom Law on the Construction of Amendments to the Code of Criminal Procedure och andra lagar, Lag nummer 7499, från den 2 mars 2024 och (ii) Regulation on Principles regarding Procedures and Rules for Transferring Personal Data Abroad från Personal Data Protection Authority så som den publicerats i Official Gazette den 10 juli Nummer 32598.

12.2 Kunden är införstådd med att Trimble, såsom personuppgiftsansvarig, i enlighet med lagar och förordningar om dataskydd, kan vara tvungen att meddela en tillsynsmyndighet om säkerhetsincidenter som involverar kunder användningsdata. Om en tillsynsmyndighet kräver att Trimble meddelar berörda registrerade med vilka Trimble inte har någon direkt relation (t.ex. kundens slutanvändare), kommer Trimble att meddela kunden om detta krav. Kunden kommer att bistå Trimble i rimlig omfattning med att meddela berörda registrerade.

BILAGA 4 - MEKANISM FÖR GRÄNSÖVERSKRIDANDE ÖVERFÖRING (Gäller data som överförs från EU, EES, Storbritannien och Schweiz)

1. Definitioner

- **Med "EU:s standardavtalsklausuler"** avses de standardavtalsklausuler som godkänts av Europeiska kommissionen genom beslut 2021/914.
- **"UK International data Transfer Agreement (IDTA)"** avser det internationella tillägget ("Addendum") till EU-kommissionens standardavtalsklausuler som utfärdats av den brittiska informationskommissionären, version B1.0, och som trädde i kraft den 21 mars 2022.
- **"Ramverket för dataskydd"** avser det självcertifieringsprogram i ramverket för dataskydd mellan EU och USA och/eller mellan Schweiz och USA som drivs av det amerikanska handelsdepartementet, US Department of Commerce.
- **"Dataskyddsprinciper"** avser principerna i Ramverket för dataskydd (kompletterade med de kompletterande principerna).
- **"Turkiska standardavtalsklausuler"** avser det standardavtal som ska användas vid överföring av personuppgifter utomlands 1–4 såsom det godkänts genom beslut 2024/959 från den 4 juni 2024 av den turkiska dataskyddsmyndigheten.

2. Mekanismer för gränsöverskridande överföring av data

2.1 Rangordning. Om tjänsterna omfattas av mer än en överföringsmekanism kommer överföringen av personuppgifter i tillämpliga fall att omfattas av en enda överföringsmekanism, enligt följande prioritetsordning: (a) Ramverket för dataskydd som refereras till i avsnitt 2.2 (Ramverk för dataskydd) i denna bilaga; (b) EU:s standardavtalsklausuler som refereras till i avsnitt 2.3 (EU:s standardavtalsklausuler) i denna bilaga; (c) Storbritanniens tillägg "International Data Transfer Addendum", som refereras till i avsnitt 2.4 (UK International Data Transfer Addendum) i denna bilaga; och – om varken (a), (b) eller (c) är tillämpliga – (f) övriga tillämpliga dataöverföringsmekanismer som är tillåtna enligt lagar och förordningar om dataskydd.

2.2 Ramverk för dataskydd. I den mån Trimble Inc. via tjänsterna behandlar personuppgifter som härrör från EES eller Schweiz, är Trimble Inc. självcertifierade enligt Ramverket för dataskydd och följer dataskyddsprinciperna vid behandling av sådana personuppgifter. I den mån kunden är (a) belägen i USA och också självcertifierad enligt Ramverket för dataskydd eller (b) har sitt säte i EES eller Schweiz, samtycker Trimble vidare till (i) att tillhandahålla minst samma skyddsnivå för alla personuppgifter som krävs enligt dataskyddsprinciperna; (ii) att meddela kunden skriftligen, utan onödigt dröjsmål, i det fall dess självcertifiering enligt Ramverket för dataskydd återkallas, upphör, dras in eller på annat sätt blir ogiltigförklarad (i vilket fall en alternativ överföringsmekanism kommer att tillämpas i enlighet med den rangordning som anges i avsnitt 2.1 (Rangordning) i denna bilaga 4); och (iii) att efter skriftlig begäran om detta samarbeta med kunden för att vidta rimliga och ändamålsenliga åtgärder för att stoppa och avhjälpa konsekvenserna av all obehörig behandling av personuppgifter.

2.3 EU:s standardavtalsklausuler. EU:s standardavtalsklausuler gäller för personuppgifter som, via tjänsterna, överförs från EES, Schweiz eller Storbritannien, antingen direkt eller genom vidareöverföring, till ett land eller en mottagare utanför EES, Schweiz eller Storbritannien som av relevant behörig myndighet inte anses tillhandahålla en tillfredsställande nivå av skydd för personuppgifter. För dataöverföringar som omfattas av EU:s standardavtalsklausuler anses EU:s standardavtalsklausuler vara ingångna och införlivade i detta DPA genom denna referens, och fylls i enligt följande:

(a) Modul Ett (Personuppgiftsansvarig till Personuppgiftsansvarig) i EU:s standardavtalsklausuler gäller när (i) Trimble behandlar data gällande kundens konto och (ii) kunden är personuppgiftsansvarig för kundens användardata och Trimble behandlar kundens användardata.

(b) Modul Två (Personuppgiftsansvarig till Personuppgiftsbiträde) i EU:s standardavtalsklausuler gäller när kunden är personuppgiftsansvarig för personuppgifterna och Trimble behandlar personuppgifter för kundens räkning; och

(c) Modul Tre (Personuppgiftsbiträde till Personuppgiftsbiträde) i EU:s standardavtalsklausuler gäller när kunden är personuppgiftsbiträde och Trimble behandlare i form av underentreprenör för kundens räkning.

(d) För varje modul, där så är tillämpligt:

(i) i Klausul 7 i EU:s standardavtalsklausuler ska den valfria dockningsklausulen inte gälla;

(ii) i klausul 9 i EU:s standardavtalsklausuler kommer Alternativ 2 att gälla och tidsfristen för föregående skriftligt meddelande om ändringar av underentreprenörer kommer att vara den som anges i avsnitt 5.2 (Förteckning över aktuella underentreprenörer och meddelande om nya underentreprenörer) i detta DPA;

(iii) i klausul 11 i EU:s standardavtalsklausuler kommer det valfria språket inte att gälla;

(iv) identifiera den eller de behöriga tillsynsmyndigheterna i enlighet med Klausul 13;

(v) i klausul 17 (alternativ 1) kommer EU:s standardavtalsklausuler att regleras av nederländsk lag;

(vi) i klausul 18 (b) i EU:s standardavtalsklausuler kommer tvister att lösas vid domstolarna i Amsterdam, Nederländerna;

(vii) i bilaga 1 del A i EU:s standardavtalsklausuler:

Uppgiftsutförare: Kund (om rutan på sidan 6 är markerad).

Kontaktuppgifter: E-postadressen (e-postadresserna) som angetts av kunden i kundens konto, som föredragen adress för meddelanden.

Rollen som uppgiftsutförare: Uppgiftsutförarens roll beskrivs på sidan 6.

Underskrift och datum: Genom att ingå Avtalet anses uppgiftsutföraren ha undertecknat de EU-standardavtalsklausuler som införlivas här, inklusive deras bilagor, från och med datumet för Avtalets ikraftträdande.

Uppgiftsinförare: Trimble Inc.

Kontaktuppgifter: Trimble Privacy Team - privacy@Trimble.com

Uppgiftsinförarens roll: Uppgiftsinförarens roll anges på sidan 6.

Underskrift och datum: Genom att ingå Avtalet anses uppgiftsinföraren ha undertecknat de EU-standardavtalsklausuler, som införlivas här, inklusive deras bilagor, från och med datumet för Avtalets ikraftträdande.

(viii) i Bilaga I, del B i EU:s standardavtalsklausuler:

De olika kategorierna av registrerade anges i avsnitt 1 i bilaga 1 (Beskrivning av behandling) i detta DPA.

Vilka känsliga uppgifter som överförs anges i avsnitt 3 i bilaga 1 (Beskrivning av behandling) i detta DPA.

Frekvensen för överföringarna är kontinuerligt under avtalets löptid.

Behandlingens karaktär anges i avsnitt 5 i bilaga 1 (Beskrivning av behandling) i detta DPA.

Syftet med behandlingen anges i avsnitt 6 i bilaga 1 (Beskrivning av behandling) av detta DPA.

Den period under vilken personuppgifterna kommer att behållas anges i avsnitt 7 i bilaga 1 (Beskrivning av behandling) i detta DPA.

Vid överföringar till underentreprenörer anges föremålet för behandlingen, samt dess karaktär och varaktighet på <https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center> under "Ytterligare resurser" ("Listor över underentreprenörer").

(ix) i Bilaga I, del C i EU:s standardavtalsklausuler: I tillämpliga fall ska den nederländska dataskyddsmyndigheten vara den ledande tillsynsmyndigheten. I annat fall, om en Trimble-enhet med säte i EU är uppgiftsutförare är det den behöriga tillsynsmyndigheten i den medlemsstat där Trimble-enheten har sitt säte, som är behörig

tillsynsmyndighet. Om kunden är uppgiftsutföraren är det den behöriga tillsynsmyndigheten i den medlemsstat där kunden har sitt säte som är behörig tillsynsmyndighet.

(x) Bilaga 2 (Tekniska och organisatoriska säkerhetsåtgärder) i detta DPA fungerar som Bilaga II i EU:s standardavtalsklausuler.

2.4 Storbritanniens tillägg ("Extension") till Ramverket för dataskydd och Storbritanniens International Data Transfer Addendum. Kunden och Trimble samtycker till att det brittiska tillägget ("Extension") till Ramverket för dataskydd ska gälla, och i avsaknad av sådant kommer EU:s standardavtalsklausuler tillsammans med det brittiska tillägget, International Data Transfer Addendum till dessa, i sin senaste version, att gälla för personuppgifter som överförs från Storbritannien via tjänsterna, antingen direkt eller genom vidareöverföring, till något land eller någon mottagare utanför Storbritannien som av relevant behörig myndighet i Storbritannien inte anses tillhandahålla en tillfredsställande nivå av skydd för personuppgifter. Vid överföring från Storbritannien av data som omfattas av EU:s standardavtalsklausuler och Storbritanniens Addendum, kommer EU:s standardavtalsklausuler att anses vara ingångna och införlivade i detta avtal såsom beskrivs i avsnitt 2.3 i detta avsnitt 4 och Storbritanniens Addendum kommer att anses vara ingånget i och införlivat i detta DPA genom denna referens och fylls i enligt följande:

(a) i Tabell 1 i Storbritanniens Addendum anges kundens och Trimbles uppgifter och viktiga kontaktuppgifter i avsnitt 2.3 (e)(vii) i denna bilaga 3;

(b) i Tabell 2 i Storbritanniens Addendum anges information om versionen av EU:s standardavtalsklausuler, och utvalda klausuler, som det brittiska Addendum utgör tillägg till, i avsnitt 2.3 (EU:s standardavtalsklausuler) i denna bilaga 4;

(c) i Tabell 3 i Storbritanniens Addendum gäller följande:

(i) Förteckningen över parter återfinns i avsnitt 2.3(e)(vii) i denna bilaga 3.

(ii) Beskrivningen av överföringen finns i avsnitt 1 (Behandlingens karaktär och ändamål) i bilaga 1 (Beskrivning av behandling).

(iii) Annex II finns i bilaga 2 (Tekniska och organisatoriska säkerhetsåtgärder) i detta DPA.

(iv) förteckningen över underentreprenörer finns på <https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center> under "Ytterligare resurser" ("Listor över underentreprenörer")

(d) Enligt Tabell 4 i Storbritanniens Addendum kan både uppgiftsinföraren och uppgiftsutföraren säga upp det brittiska IDTA-avtalet i enlighet med villkoren i Storbritanniens Addendum.

2.5 Turkiska standardavtalsklausuler. De turkiska standardavtalsklausulerna gäller för personuppgifter som, via tjänsterna, överförs från EES, Schweiz eller Storbritannien, antingen direkt eller genom vidareöverföring, till ett land eller en mottagare utanför Turkiet som av relevant behörig myndighet inte anses tillhandahålla en tillfredsställande nivå av skydd för personuppgifter. För dataöverföringar som omfattas av de turkiska standardavtalsklausulerna anses de turkiska standardavtalsklausulerna vara ingångna och införlivade i detta DPA genom denna referens och fylls i enligt följande:

För varje modul, i tillämpliga fall:

(i) i Artikel 8 i Contract 2 och Contract 3 i de turkiska standardavtalsklausulerna kommer alternativ 2 att tillämpas och tidsfristen för föregående skriftligt meddelande om ändringar av underentreprenörer kommer att vara den som anges i avsnitt 5.2 (Förteckning över aktuella underentreprenörer och meddelande om nya underentreprenörer) i detta DPA;

(ii) parterna är överens om att kunden ska meddela den behöriga turkiska dataskyddsmyndigheten inom fem (5) arbetsdagar för att informera om införandet av de turkiska standardavtalsklausulerna.

(iii) Uppgiftsinförare ska vara: Trimble med adresser, namn och efternamn, titel och kontaktinformation för Trimble och undertecknare enligt vad som anges i DPA.

(iv) Underskrift och datum: Genom att ingå Avtalet anses Trimble och uppgiftsutföraren ha undertecknat de turkiska standardavtalsklausuler som införlivas här, inklusive deras bilagor, från och med datumet för avtalets ikraftträdande.

(v) Uppgifterna i appendix I till de turkiska standardavtalsklausulerna anges i bilaga 1:

(vi) Bilaga 2 (Tekniska och organisatoriska säkerhetsåtgärder) i detta DPA fungerar som appendix II i de turkiska standardavtalsklausulerna.

(vii) förteckningen över underentreprenörer finns på <https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center> under "Ytterligare resurser" ("Listor över underentreprenörer").

2.6 Konflikt. I den mån det finns någon konflikt eller inkonsekvens mellan EU:s standardavtalsklausuler, Storbritanniens IDTA eller de turkiska standardavtalsklausulerna, och andra villkor i detta DPA, inklusive bilaga 4 (Gränsöverskridande överföringsmekanism), kommer Avtalet, bestämmelserna i EU:s standardavtalsklausuler, Storbritanniens Addendum och turkiska standardavtalsklausuler, såsom tillämpligt, att gälla.