DATABEHANDLERAVTALE

Denne databehandleravtalen («DPA») er partenes avtale med hensyn til behandling av personopplysninger og supplerer alle lisens-, abonnements-, tjeneste- eller andre skriftlige eller elektroniske avtaler (**«avtalene»**) mellom Trimble og kunden for kjøp av tjenester (inkludert Programvare som en tjeneste (SaaS), deres tilknyttede Trimble offline- eller mobilapplikasjoner og support, og definert som «tjenester» eller på annen måte i avtalen eller i det følgende) i løpet av hvilke Trimble mottar personopplysninger fra kunden.

Kunden inngår denne DPA-en (i) ved å signere eller på annen måte godta avtalen, (ii) ved å signere den på vegne av seg selv og som påkrevd i henhold til gjeldende personvernlover og -forskrifter, i navnet til og på vegne av autoriserte tilknyttede selskaper, hvis og i den grad Trimble behandler personopplysninger. I denne DPA-en, og med mindre noe annet er angitt, skal begrepet «kunde» innlemme kunden og autoriserte tilknyttede selskaper.

Ved levering av tjenestene til kunden i henhold til avtalen kan Trimble behandle personopplysninger på vegne av kunden, og partene er enige om å overholde følgende bestemmelser med hensyn til alle personopplysninger.

HVORDAN DU GJENNOMFØRER DENNE DPA-EN:

I. Denne DPA-en består av: hoveddelen av DPA-en og tillegg 1 til 3.
II. Den er forhåndssignert på vegne av Trimble. Standard avtalevilkår (som definert nedenfor) er innlemmet ved henvisning.
III. Hvis kunden ønsker å fylle ut denne DPA-en, må kunden:
    a. fylle ut informasjonen i signaturfeltet, og signer på side 6
    b. fylle ut informasjonen som dataeksportør på side 6
IV. Send den utfylte og signerte DPA-en til Trimble via e-post, og oppgi din organisasjons kundekontonummer (som angitt på den aktuelle Trimble-fakturaen), til privacy@trimble.com.

HVORDAN DENNE DPA-EN GJELDER:

- Hvis kundeenheten som aksepterer denne DPA-en er part i en avtale, er denne DPA-en et tillegg til og utgjør en del av den avtalen, og Trimble-enheten som er part i avtalen, er part i denne DPA-en.
- Hvis kundeenheten som signerer denne DPA-enheten, har sendt inn en ordre som er akseptert av Trimble eller noen av dets tilknyttede selskaper, men ikke selv er part i avtalen, er denne DPA-en et tillegg til den ordren (inkludert enhver fornyelsesordre), og Trimble-enheten som en slik ordre er lagt inn på, er part i denne DPA-en.
- Hvis kundeenheten som signerer DPA-en, har kjøpt Trimble-tjenester via en autorisert forhandler av Trimble, må kunden angi dette på side 6 og oppgi et kundenummer utstedt av Trimble eller forhandleren, eller, i mangel av dette, en bekreftelse fra forhandleren om at kunden abonnerer på en Trimble-tjeneste. I dette tilfellet skal denne DPA-en anses som en direkte avtale mellom kunden og Trimble.
- Hvis enheten eller personen som signerer denne DPA-en, verken er part i en ordre eller en avtale og ikke er en indirekte kunde gjennom en forhandler, er ikke denne DPA-en gyldig og heller ikke rettslig bindende. En slik enhet bør be om at dens tilknyttede enhet som er part i avtalen, undertegner denne DPA-en, eller skriftlig ber om å bli en del av avtalen.

Denne DPA-en erstatter ikke sammenlignbare eller ytterligere rettigheter knyttet til behandling av kundeopplysninger som finnes i avtalen (inkludert eventuelle eksisterende databehandlingstillegg til avtalen).

VILKÅR FOR DATABEHANDLING

1. DEFINISJONER

«Tilknyttet selskap» betyr enhver enhet som direkte eller indirekte kontrollerer, kontrolleres av eller er under felles kontroll med den subjektets enhet. Med «kontroll» menes i denne definisjonen direkte eller indirekte eierskap eller kontroll over mer enn 50 % av de utestående stemmeandelene i subjektets enhet.

«Autorisert tilknyttet selskap» betyr ethvert av kundens tilknyttede selskap(er) som (i) er underlagt en eller flere personvernlover og (ii) har tillatelse til å bruke tjenestene i henhold til avtalen mellom kunden og Trimble, men som ikke har signert sin egen ordre med Trimble og ikke er en «kunde» som definert i avtalen.

«CCPA» betyr California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., og dens gjennomførings-forskrifter.

«Behandlingsansvarlig» betyr den enheten som bestemmer formålene med og midlene for behandlingen av personopplysninger.

«Kunden» betyr enheten som har inngått avtalen, sammen med sine tilknyttede selskaper (så lenge de forblir tilknyttede selskaper) som har signert bestillingsskjemaer.

«Kundedata» betyr det som i avtalen er definert som «kundedata» eller «dine data».

«**Personvernlover og -forskrifter»** betyr alle lover og forskrifter, inkludert lover og forordninger i Den europeiske union, Det europeiske økonomiske samarbeidsområdet og deres medlemsstater, Sveits og Storbritannia, landene som er oppført i Tillegg 3 og alle andre land der kunden eller et av kundens tilknyttede selskaper har tilstedeværelse, alt som gjelder for behandling av personopplysninger i henhold til avtalen.

«Den registrerte» betyr den personen som personopplysningene gjelder.

«Europa» betyr Den europeiske union (EU), Det europeiske økonomiske samarbeidsområdet (EØS) og Sveits.

«GDPR» betyr Europaparlaments- og rådsforordning (EU) 2016/679.

«Personopplysninger» betyr all informasjon knyttet til (i) en identifisert eller identifiserbar person og (ii) en identifisert eller identifiserbar juridisk enhet (der slik informasjon er beskyttet på samme måte som personopplysninger eller personlig identifiserbar informasjon i henhold til gjeldende databeskyttelseslover og -forskrifter), forutsatt at slik informasjon er kundedata.

«Behandling» betyr enhver operasjon eller rekke av operasjoner som utføres på personopplysninger, enten automatisk eller ikke, for eksempel innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultasjon, bruk, utlevering ved overføring, spredning eller annen form for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sperring, sletting eller tilintetgjøring.

«**Databehandler**» betyr den enheten som behandler personopplysninger på instruks og på vegne av behandlingsansvarlig, inkludert, der det er aktuelt, enhver «tjenesteleverandør» slik dette begrepet er definert i CCPA.

«Offentlig myndighet» betyr en offentlig etat eller rettshåndhevende myndighet, inkludert rettsmyndigheter.

«EUs standard avtalevilkår» betyr en avtale inngått av og mellom enten (i) et Trimble-tilknyttet selskap og Trimble Inc. eller (ii) kunden og Trimble Inc. i henhold til innføringsbeslutning (EU) 2021/914.

«Underdatabehandler» betyr enhver databehandler engasjert av Trimble eller et medlem av Trimble-konsernet.

«Trimble» betyr Trimble-enheten som er part i denne DPA-en, som spesifisert i avsnittet «HVORDAN GJELDER DENNE DPA-en» ovenfor. Trimble-enheter som opptrer som behandlere, er: Trimble Inc, et selskap registrert i Delaware, Trimble Europe B.V., et selskap registrert i Nederland, Trimble International B.V., et selskap registrert i Nederland, Trimble UK Ltd, et selskap registrert i England og Wales, Trimble Maps, Ltd, et selskap registrert i England og Wales, Trimble Technologies Ireland Ltd, et selskap registrert i Nederland, Trimble UK Ltd, et selskap registrert i England og Wales, Trimble Maps, Ltd, et selskap registrert i England og Wales, Trimble Technologies Ireland Ltd, et selskap registrert i Irland, Trimble France SAS, et selskap registrert i Frankrike, Trimble Solutions Sandvika AS, et selskap stiftet i Norge, Trimble Finland Corporation, et selskap stiftet i Finland, Trimble Forestry Europe Corporation, et selskap stiftet i Finland, Lakefield eTechnologies Ltd, et selskap stiftet i Irland, Trimble GmbH, et selskap stiftet i Tyskland, eller Trimble Germany GmbH, et selskap stiftet i Tyskland, alt etter hva som er aktuelt.

«Trimble Group» betyr Trimble og dets tilknyttede selskaper som er involvert i behandlingen av personopplysninger.

2. BEHANDLING AV PERSONOPPLYSNINGER

2.1 Partenes roller. Partene erkjenner og er enige om at med hensyn til behandling av personopplysninger er kunden behandlingsansvarlig, Trimble er databehandler, og at Trimble eller medlemmer av Trimble-konsernet vil engasjere underdatabehandlere i henhold til kravene som er angitt i punkt 5 nedenfor, forutsatt at Trimble er behandlingsansvarlig for behandling av kundens kontodata.

2.2 Kundens behandling av personopplysninger. Kunden skal, i sin bruk av tjenestene, behandle personopplysninger i samsvar med kravene i personvernlover og -forskrifter. For å unngå enhver tvil skal kundens instruksjoner for behandling av personopplysninger være i samsvar med personvernlover og -forskrifter. Kunden er eneansvarlig for nøyaktigheten, kvaliteten og lovligheten av personopplysningene og måten kunden har innhentet personopplysningene på. Trimble skal umiddelbart informere kunden dersom en instruks etter Trimbles oppfatning er i strid med personvernlover og -forskrifter eller andre lovfestede bestemmelser.

2.3 Trimbles behandling av personopplysninger. Trimble skal kun behandle personopplysninger på vegne av og i samsvar med kundens instruksjoner, deriblant med hensyn til overføring av personopplysninger til et tredjeland eller en internasjonal organisasjon. Kunden instruerer Trimble om å behandle personopplysninger for følgende formål: (i) Behandling i samsvar med avtalen og gjeldende ordrer; (ii) Behandling initiert av brukere i deres bruk av tjenestene; (iii) Behandling for å overholde andre rimelige instruksjoner gitt av kunden der slike instruksjoner er i samsvar med vilkårene i avtalen; og (iv) Behandling med det formål å anonymisere i samsvar med bestemmelsene om databruk i avtalen (og inkludert i Tillegg 1).

TRIMBLE FUNGERER IKKE DATABEHANDLERFOR FØLGENDE PERSONOPPLYSNINGER: Brukerens påloggings- og kontaktopplysninger, data om programvarebruk og data som genereres av sikkerhetstiltak (**«Kundekontodata»**).

2.4 Omfang og formål; kategorier av personopplysninger og registrerte. Formålet med Trimbles behandling av personopplysninger er utførelsen av tjenestene i henhold til avtalen. Hvilke typer personopplysninger og kategorier av registrerte som behandles i henhold til denne DPA-en, er nærmere spesifisert i Tillegg 1 (Beskrivelse av behandlingen) til denne DPA-en.

3. DE REGISTRERTES RETTIGHETER

3.1 De registrertes rettigheter. Med tanke på behandlingens art bistår Trimble kunden ved å sørge for passende tekniske og organisatoriske tiltak, så langt dette er mulig, for å oppfylle kundens forpliktelse til å svare på forespørsler fra registrerte om å utøve sine rettigheter i henhold til personvernlover og -forskrifter. I den grad kunden, i sin bruk av tjenestene, ikke har mulighet til å utøve disse rettighetene selv, skal Trimble etterkomme enhver kommersielt rimelig anmodning fra kunden om å legge til rette for slike handlinger i den grad Trimble har lovlig adgang til å gjøre det. I den grad det er lovlig tillatt, skal kunden være ansvarlig for alle kostnader som oppstår som følge av Trimbles tilveiebringelse av slik assistanse.

3.2 Direkte forespørsler fra den registrerte. Trimble skal, i den grad det er lovlig tillatt, umiddelbart varsle kunden dersom Trimble mottar en forespørsel fra en registrert om å utøve sine rettigheter som registrert i henhold til avsnitt 3.1. Trimble skal ikke svare på slike forespørsler fra registrerte uten kundens forhåndssamtykke i tekstform, bortsett fra å bekrefte at forespørselen gjelder kunden, noe kunden herved samtykker til.

4. TRIMBLE OG KUNDENS PERSONELL

4.1 Generelt. Trimble og kunden skal treffe tiltak for å sikre at enhver fysisk person som handler under deres respektive myndighet og som har tilgang til kundedata, ikke behandlerkundedata unntatt etter instruks fra kunden, med mindre han eller hun er pålagt å gjøre det i henhold til personvernlover og -forskrifter.

4.2 Konfidensialitet. Trimble skal sørge for at personalet som er involvert i behandlingen av personopplysninger, er informert om personopplysningenes konfidensielle art, har fått passende opplæring i sitt ansvarsområde og har inngått skriftlige avtaler om taushetsplikt.

4.3 Pålitelighet. Trimble skal ta kommersielt rimelige skritt for å sikre påliteligheten til alt Trimble-personell som er engasjert i behandlingen av personopplysninger.

4.4 Begrensning av tilgang. Trimble skal sørge for at personalets tilgang til personopplysninger er begrenset til det personalet som utfører tjenester i henhold til avtalen.

5. UNDERDATABEHANDLERE

5.1 Utnevnelse av underdatabehandlere. Kunden erkjenner og samtykker i at (i) Trimbles tilknyttede selskaper kan benyttes som underdatabehandlere, og (ii) Trimble og Trimbles tilknyttede selskaper kan engasjere tredjeparts underdatabehandlere i forbindelse med tilveiebringelse av tjenestene. I slike tilfeller skal Trimble og Trimbles tilknyttede selskap pålegge enhver underdatabehandler i det vesentlige tilsvarende krav til vern av personopplysninger som er fastsatt i denne DPA-en i form av en kontrakt eller annen rettsakt. Kontrakten eller annen rettsakt skal inneholde tilstrekkelige garantier for at enhver underdatabehandler iverksetter egnede tekniske og organisatoriske tiltak på en slik måte at behandlingen oppfyller kravene i personvernlovene og -forskriftene.

5.2 Liste over nåværende underdatabehandlere og melding om nye underdatabehandlere. Den gjeldende listen over underdatabehandlere som er engasjert i behandling av personopplysninger for utførelsen av hver gjeldende tjeneste, inkludert en beskrivelse av deres behandlingsaktiviteter og lokaliseringsland, er oppført under https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center under «Tilleggsressurser» («Lister overunder-databehandlere»"). Kunden samtykker herved til disse underdatabehandlerne, deres lokasjoner og behandlingsaktiviteter når det gjelder deres personopplysninger, og instruerer Trimble i henhold til dette. Trimble skal informere om endringer av underdatabehandlere i sine

utgivelsesnotater, kundeoppdateringer eller lignende kommunikasjon, som skal anses som varsel i henhold til avsnitt [9.2 i EUs standard avtalevilkår].

5.3 Innsigelsesrett for nye underdatabehandlere. For å utøve sin rett til å protestere mot Trimbles bruk av en ny underdatabehandler skal kunden varsle Trimble omgående i tekstform sendt til privacy@trimble.com innen tretti (30) virkedager etter mottak av Trimbles varsel i samsvar med mekanismen som er beskrevet i avsnitt 5.2. Dersom kunden protesterer mot en ny underdatabehandler, og denne protesten ikke er urimelig, vil Trimble gjøre rimelige anstrengelser for å gjøre tilgjengelig for kunden en endring i tjenestene eller anbefale en kommersielt rimelig endring i kundens konfigurasjon eller bruk av tjenestene for å unngå at den nye underdatabehandleren, som det er protestert mot, behandler personopplysninger, uten å påføre kunden urimelige byrde. Hvis Trimble ikke er i stand til å gjøre en slik endring tilgjengelig innen en rimelig tidsperiode, som ikke skal overstige seksti (60) dager, kan kunden si opp gjeldende ordre(r) og avtaler med hensyn til kun de tjenestene som ikke kan leveres av Trimble uten bruk av den nye underdatabehandleren som det er gjort innsigelse mot, ved å gi Trimble skriftlig varsel. Trimble skal refundere kunden eventuelle forhåndsbetalte gebyrer som dekker resten av løpetiden for slike ordre(r) etter den effektive oppsigelsesdatoen med hensyn til slike oppsagte tjenester.

5.4 Ansvar. Trimble skal være ansvarlig for handlinger og unnlatelser fra sine underdatabehandlere i samme grad som Trimble ville være ansvarlig hvis de utførte tjenestene til hver underdatabehandler direkte i henhold til vilkårene i denne DPA-en, med mindre noe annet er fastsatt i avtalen.

6. SIKKERHET, REVISJONER OG ASSISTANSE

6.1 Sikkerhet i behandlingen. Trimble skal opprettholde administrative, fysiske og tekniske sikkerhetstiltak for å beskytte sikkerheten, konfidensialiteten og integriteten til kundens opplysninger, inkludert personopplysninger, som angitt i Tillegg 1. Trimble overvåker regelmessig at disse sikkerhetstiltakene overholdes. Trimble skal ikke vesentlig redusere den generelle sikkerheten til tjenestene i løpet av avtalens løpetid.

6.2 Revisjoner. Trimble utfører fra tid til annen revisjoner og inspeksjoner (inkludert, der det er rimelig, revisjoner utført av eksterne revisorer) for å sikre overholdelse av personvernlovgivning og denne DPA-en, samt, der det er rimelig, bransjestandarder som ISO 27001. Trimble skal på forespørsel gjøre tilgjengelig for kunden all informasjon som er nødvendig (inkludert slike revisjonsrapporter) for å påvise overholdelse av sine forpliktelser i henhold til gjeldende personvernlovgivning og denne DPA-en. Avhengig av hvilken informasjon som etterspørres, kan Trimble kreve at kunden undertegner en taushetserklæring.

6.3 Bistand til kunden. Trimble skal bistå kunden med å sikre overholdelse av forpliktelsene vedrørende sikkerhet ved behandling, varsling og kommunikasjon av brudd på personopplysningssikkerheten, konsekvensutredninger for personvern og forutgående konsultasjoner med tilsynsmyndighetene i henhold til personvernlovene og -forskriftene.

6.4 Håndtering og varsling av sikkerhetsbrudd. I tilfelle brudd på personopplysningssikkerheten i henhold til personvernlovene og -forskriftene, opprettholder Trimble retningslinjer og prosedyrer for håndtering av sikkerhetshendelser og skal, i den grad loven tillater det, varsle kunden om slike brudd uten unødig forsinkelse.

7. RETUR OG SLETTING AV KUNDEOPPLYSNINGER

Trimble skal, etter endt tilveiebringelse av tjenester etter kundens valg, returnere kundeopplysninger til kunden og/eller slette opplysningene i samsvar med prosedyrene og tidsrammene som er spesifisert i avtalen eller tjenestebeskrivelsen, med mindre lovgivning som er pålagt kunden, krever lagring av kundeopplysninger.

8. INNSYNSBEGJÆRINGER FRA MYNDIGHETENE

8.1 Med mindre det er forbudt i henhold til gjeldende rett, skal Trimble informere kunden i generelle vendinger om forespørsler, pålegg eller lignende krav fra en domstol, kompetent myndighet, rettshåndhevende myndighet eller annet myndighetsorgan («Forespørsel om rettshåndhevelse») knyttet til behandling av personopplysninger i henhold til disse bestemmelsene.

8.2 Trimble vil protestere mot og utfordre enhver forespørsel fra rettshåndhevende organer ved å ta i bruk rettsmidler i den grad de er rimelige gitt omstendighetene. Hvis Trimble blir tvunget til å utlevere personopplysninger som er overført i henhold til disse bestemmelsene på grunn av en forespørsel fra et rettshåndhevende organ, vil Trimble, med mindre det er forbudt i henhold til gjeldende rett, gi kunden rimelig varsel for å gi kunden mulighet til å søke om en beskyttelsesordre eller andre passende rettsmidler, med mindre Trimble er rettslig forhindret fra å gjøre dette.

8.3 Dersom Trimble gjør personopplysninger tilgjengelige for underdatabehandlere, vil Trimble velge underdatabehandlere i et land utenfor EØS-området som ikke er gjenstand for en konklusjon om tilstrekkelig beskyttelsesnivå fra EU-kommisjonen, kun etter en due diligence som innebærer (i) en gjennomgang av eventuelle

åpenhetsrapporter som er gjort tilgjengelig av underdatabehandleren, (ii) og gjennomføring av en vurdering av overføringsrisiko.

9. AUTORISERTE DATTERSELSKAPER

9.1 Kontraktsmessig forhold. Kunden inngår DPA-enpå vegne av seg selv og, etter omstendighetene, i navnet til og på vegne av autoriserte tilknyttede selskaper, og etablerer dermed en separat DPA mellom Trimble og hvert slikt autorisert tilknyttet selskap. Alle autoriserte tilknyttede selskaper er bundet av forpliktelsene i henhold til denne DPA-en. For å unngå enhver tvil er og blir ikke et autorisert tilknyttet selskap en part av avtalen, men er kun en part i DPA-en. All tilgang til og bruk av tjenestene av autoriserte tilknyttede selskaper må være i samsvar med vilkårene i avtalen, og enhver overtredelse på vilkårene i avtalen fra et autorisert tilknyttet selskap skal anses som et brudd fra kundens side..

9.2 Kommunikasjon. Kunden som er avtalepart i avtalen, skal fortsatt være ansvarlig for å koordinere all kommunikasjon med Trimble i henhold til denne DPA-en, og skal ha rett til å foreta og motta all kommunikasjon i forbindelse med denne DPA-en på vegne av sine autoriserte tilknyttede selskaper.

9.3 Rettigheter for autoriserte tilknyttede selskaper. Når et autorisert tilknyttet selskap blir part i DPA-en med Trimble, skal det i den grad det kreves i henhold til gjeldende personvernlover og -forskrifter ha rett til å utøve rettighetene og søke rettsmidler i henhold til denne DPA-en. Hvis personvernlover og -forskrifter krever at det autoriserte tilknyttede selskapet skal utøve en rettighet eller søke rettsmidler i henhold til denne DPA-en som behandlingsansvarlig, gir det autoriserte tilknyttede selskapet herved kunden fullmakt til å utøve en slik rettighet i stedet for det autoriserte tilknyttede selskapet. Videre skal kunden som er avtalepart i avtalen, utøve alle slike rettigheter i henhold til denne DPA-en ikke separat for hvert autoriserte tilknyttede selskap, men samlet for alle sine autoriserte tilknyttede selskaper sammen.

10. BEGRENSNING AV ANSVAR

Hver parts og dens tilknyttede selskapers ansvar som oppstår som følge av eller i forbindelse med denne DPA-en og alle DPA-er mellom autoriserte tilknyttede selskaper og Trimble, enten det er i henhold til kontrakt, erstatningsrettslig eller annen ansvarsteori, er underlagt avsnittet «Begrensning av ansvar» i avtalen, og enhver henvisning i et slikt avsnitt til ansvaret til en part betyr det samlede ansvaret til den parten og dens tilknyttede selskaper i henhold til avtalen og alle DPA-er samlet. For å unngå tvil skal Trimbles og dets tilknyttede selskapers totale ansvar for alle krav fra kunden og kundens autoriserte tilknyttede selskaper som oppstår som følge av eller i forbindelse med avtalen og hver DPA gjelde samlet for alle krav i henhold til både avtalen og alle DPA-er som er etablert i henhold til en slik avtale, inkludert av ethvert autorisert tilknyttet selskap, og skal særlig ikke forstås som å gjelde individuelt og separat for hvert autorisert tilknyttet selskap som er en kontraktspart i en slik DPA-avtale. For å unngå ytterligere tvil betyr alle henvisninger til DPA-en i denne DPA-en denne DPA-en, inkludert dens tillegg og vedlegg.

Hvis kunden har abonnert på eller kjøpt tjenestene gjennom en forhandler eller annen forretningspartner av Trimble, skal Trimbles og dets tilknyttede selskapers ansvar som følge av eller relatert til denne DPA-en og alle DPA-er mellom autoriserte tilknyttede selskaper og Trimble, enten i kontrakt, erstatningsrettslig eller under noen annen ansvarsteori, være begrenset, i den grad det er lovlig tillatt, til det høyeste av beløpene Trimble har mottatt for disse tjenestene eller EUR 50 000.

11. INTERNASJONALE BESTEMMELSER

11.1 Overføringsmekanismer på tvers av landegrenser. I den grad Trimble behandler personopplysninger som stammer fra og er beskyttet av personvernlover og -forskrifter i en av jurisdiksjonene som er oppført i Tillegg 3 (Overføringsmekanismer på tvers av landegrenser) i denne DPA-en, gjelder vilkårene som er spesifisert i Tillegg 3 med hensyn til gjeldende jurisdiksjon(er) i tillegg til vilkårene i denne DPA-en.

11.2 Mekanismer for dataoverføring på tvers av landegrensene. I den grad kundens bruk av tjenestene krever en videreoverføringsmekanisme for lovlig overføring av personopplysninger fra en jurisdiksjon (dvs. Det europeiske økonomiske samarbeidsområdet, Storbritannia, Sveits, Tyrkia eller en annen jurisdiksjon som er oppført i Tillegg 3 (Overføringsmekanismer på tvers av landegrenser) til Trimble utenfor den jurisdiksjonen («Overføringsmekanisme»), vil vilkårene i Tillegg 4 (Overføringsmekanismer på tvers av landegrenser) i denne DPA-en gjelde.

12. DIVERSE

12.1 Konflikt. I tilfelle motstrid eller uoverensstemmelse mellom de følgende dokumentene, skal rekkefølgen som gjelder være følgende: (1) de gjeldende vilkårene som er angitt i Tillegg 4 (Overføringsmekanismer på tvers av landegrenser) i denne DPA-en; (2) vilkårene i denne DPA-en utenfor Tillegg 4 (Overføringsmekanismer på tvers av landegrenser); og (3) avtalen.

12.2 Oppdateringer. Trimble kan oppdatere vilkårene i denne DPA-en fra tid til annen, forutsatt at Trimble gir minst tretti (30) dagers skriftlig forhåndsvarsel til kunden når en oppdatering er nødvendig som følge av (a) endringer i personvernlover og -forskrifter; (b) en fusjon, et oppkjøp eller en annen lignende transaksjon; eller (c) lansering av nye produkter eller tjenester eller vesentlige endringer i noen av de eksisterende tjenestene. De gjeldende vilkårene i denne DPA-en er tilgjengelig på trimble.com/privacy

Kundens juridiske navn:_____

Adresse

Kundenummer hos Trimble:_____

☐ Kunden har kjøpt tjenestene gjennom Trimbles autoriserte forhandler eller forretningspartner

Forhandlerens navn

Adresse _____

Forhandlerens kundenummer

☐ For EU/EØS/UK-faktura til kunder. Kunden ønsker å inngå EUs standard avtalevilkår direkte med Trimble Inc.Hvis denne boksen ikke er krysset av, er overføringsmekanismen for overføringen til Trimble Inc. den som er beskrevet i punkt 2.2 i Tillegg 4 eller andre overføringsmekanismer som er etablert mellom Trimble-datterselskapet i Europa og Trimble Inc.

Hvis den forrige boksen er merket av: Kunden anser følgende moduler som aktuelle:

☐ Modul 1/Kontrakt 1 ☐ Modul 2/Kontrakt 2 ☐ Modul 3/Kontrakt 3

☐ Kunden velger å gjennomføre denne DPA-en
Partene har undertegnet denne avtalen på behørig måte:

KUNDEN (undertegner herved denne DPA-en)

Navn:

Tittel

Dato:

Trimble Inc.

Signatur:_____
Navn (blokkbokstaver): Jennifer Allison
Tittel: Senior Vice President and General Counsel
Dato: 15.7.2024

Trimble Europe BV

Signatur:_____
Navn (blokkbokstaver): RHH Reeder
Tittel: Director
Dato: 15.7.2024

Trimble UK Limited

Signatur:_____
Navn (blokkbokstaver): RHH Reeder
Tittel: Director
Dato: 15.7.2024

Trimble France SAS

Signatur:_____
Navn (blokkbokstaver): RHH Reeder
Tittel: Director
Dato: 15.7.2024

Trimble Solutions Sandvika AS

Signatur:_____
Navn (blokkbokstaver): RHH Reeder
Tittel: Director
Dato: 15.7.2024

Trimble Technologies Ireland Limited

Signatur:_____
Navn (blokkbokstaver): RHH Reeder
Tittel: Director
Dato: 15.7.2024

Lakefield eTechnologies Limited

Trimble International BV

Signatur:_____
Navn (blokkbokstaver): RHH Reeder
Tittel: Director
Dato: 15.7.2024

Trimble Finland Corporation

Signatur:_____
Navn (blokkbokstaver): RHH Reeder
Tittel: Director
Dato: 15.7.2024

Trimble Germany GmbH

Signatur:_____
Navn (blokkbokstaver): Jürgen Kesper
Tittel: Director
Dato: 15.7.2024

Trimble MAPS Limited.

Signatur:_____
Navn (blokkbokstaver): RHH Reeder
Tittel: Director
Dato: 15.7.2024

Trimble Forestry Europe Corporation

Signatur:_____
Navn (blokkbokstaver): RHH Reeder
Tittel: Director
Dato:15.7.2024

Trimble GmbH

Signatur:_____
Navn (blokkbokstaver): Jürgen Kesper
Tittel: Director
Dato: 15.7.2024

Kontaktinformasjon for alle Trimble-enheter:

privacy@trimble.com

Adresser til Trimbles enheter	
Trimble Inc.	**Trimble Europe B.V.**
10368 Westmoor Drive Westminster, CO 80021, USA	Industrieweg 187a 5683CC Best, Nederland
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, Nederland
Trimble Finland Corporation	**Trimble Germany GmbH**
Hatsinanpuisto 8, 02600 Espoo, Finland	Am Prime Parc 11, 65479 Raunheim
Trimble MAPS Limited.	**Trimble Forestry Europe Corporation**
53-64 Chancery Lane, Holborn, London	Hatsinanpuisto 8, 02600 Espoo, Finland

England WC2A 1QS UK	
Trimble GmbH	
Am Prime Parc 11, 65479 Raunheim	

TILLEGG 1 – BESKRIVELSE AV BEHANDLINGEN

1. KATEGORIER AV REGISTRERTE HVIS PERSONOPPLYSNINGER OVERFØRES

Kunden kan sende inn personopplysninger til tjenestene, hvis omfang bestemmes og kontrolleres av kunden etter eget skjønn, og som kan omfatte, men ikke er begrenset til, personopplysninger knyttet til følgende kategorier av registrerte personer:

- Ansatte, ledere, styremedlemmer og underleverandører hos kunden.
- Kundens kunder (som er fysiske personer), ofte i egenskap av mottakere av forsendelser, tjenester og produkter.
- Ansatte, agenter, rådgivere, frilansere hos kundens kunder, leverandører og motparter i transaksjoner som behandles gjennom tjenestene.
- Kundens brukere som er autorisert av kunden til å bruke tjenestene.

2. KATEGORIER AV PERSONOPPLYSNINGER SOM OVERFØRES

Kunden kan sende inn personopplysninger til tjenestene, hvis omfang bestemmes og kontrolleres av kunden etter eget skjønn, og som kan omfatte, men ikke er begrenset til, følgende kategorier av personopplysninger:
- kontakt- og stamdata (for- og etternavn, tittel, stilling)
- kontaktinformasjon (firma, e-post, telefon, fysisk forretningsadresse)
- ID-opplysninger som pass, førerkort, IP-adresser, unike identifikatorer (UUID)
- yrkes- og utdanningsopplysninger (kvalifikasjoner, erfaringer, ferdigheter)
- jobbrelaterte opplysninger (utførte tjenester, prosjektbidrag, tildelte jobber og oppgaver, prestasjonsrelaterte data, tjenestetid, utgifter)
- lokaliseringsopplysninger
- kontraktsrelaterte opplysninger (fakturering, betaling, transaksjonshistorikk)
- Interaksjonshistorikk

3. SENSITIVE OPPLYSNINGER SOM OVERFØRES (HVIS DET ER AKTUELT)

Sensitive opplysninger som overføres (hvis det er aktuelt) og anvendte begrensninger eller sikkerhetstiltak som fullt ut tar hensyn til opplysningenes art og de involverte risikoene, som for eksempel streng formålsbegrensning, tilgangsbegrensninger (inkludert tilgang kun for ansatte som har fått spesialisert opplæring), registrering av tilgang til opplysningene, begrensninger for videre overføring eller ytterligere sikkerhetstiltak:
Dataeksportøren kan sende inn særlige kategorier av opplysninger til tjenestene, hvis omfang bestemmes og kontrolleres av dataeksportøren etter eget skjønn, og som for klarhetens skyld er personopplysninger med informasjon som avslører rasemessig eller etnisk opprinnelse, politiske meninger, religiøs eller filosofisk overbevisning eller fagforeningsmedlemskap, og behandling av genetiske opplysninger, biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.
De aktuelle sikkerhetstiltakene er beskrevet i avsnitt 11 i Tillegg 2 nedenfor.

4. HYPPIGHETEN AV OVERFØRINGEN

Hyppigheten av overføringen (f.eks. om opplysningene overføres på engangsbasis eller kontinuerlig):

Kontinuerlig basis, avhengig av kundens bruk av tjenestene.

5. BEHANDLINGENS ART

Behandlingens art er utførelsen av tjenestene i henhold til avtalen.

6. FORMÅLET MED BEHANDLINGEN, DATAOVERFØRINGEN OG DEN VIDERE BEHANDLINGEN

Trimble vil behandle personopplysninger som nødvendige for å utføre tjenestene i henhold til avtalen, som er nærmere spesifisert i dokumentasjonen, og som videre instruert av kunden i sin bruk av tjenestene. Trimble vil dessuten anonymisere personopplysninger for å kunne gjennomføre dataanalyser og tjenesteutvikling.

7. BEHANDLINGENS VARIGHET

Hvor lenge personopplysningene skal lagres, eller, hvis dette ikke er mulig, kriteriene som brukes for å fastsette denne perioden:

Trimble vil behandle personopplysninger som angitt i avtalen, med mindre annet er avtalt, for eksempel i punkt 9 i DPA-en.

8. OVERFØRINGER TIL UNDERDATABEHANDLERE

For overføringer til (under)databehandlere må også behandlingens formål, art og varighet spesifiseres:

Underdatabehandleren vil behandle personopplysninger som nødvendige for å utføre tjenestene i henhold til avtalen. I henhold til avsnitt 9 i denne DPA-en skal underdatabehandleren behandle personopplysninger så lenge avtalen gjelder, med mindre noe annet er skriftlig avtalt.

Identiteten til underdatabehandlerne som brukes til å tilveiebringe tjenestene, og hvilke land de befinner seg i, er oppført under fanen Tilleggsmateriale på trimble.com/privacy.

TILLEGG 2 – Tekniske og organisatoriske sikkerhetstiltak

Der det er relevant, vil dette Tillegg 2 også fungere som Vedlegg II til EUs standard avtalevilkår.

Tekniske og organisatoriske sikkerhetstiltak

1. Tiltak for pseudonymisering og kryptering av personopplysninger

Der det er mulig, krypterer Trimble data som overføres mellom kunder og Trimble-applikasjonen over offentlige nettverk ved hjelp av TLS 1.2 eller høyere. Kundedata som lagres på Trimble-administrerte systemer (for AICPA-sertifiserte produkter, se punkt 7 nedenfor for mer informasjon), krypteres ved hjelp av AES 256 eller sterkere krypteringskoder.

2. Tiltak for å sikre fortløpende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemer og -tjenester

Trimble har dedikert cybersikkerhetspersonell som er ansvarlig for overvåking av sikkerhet og personvern. Selskapet har utnevnt en leder for cybersikkerhet og personvern i tillegg til et kontor for vern av personopplysninger, samt et Engineering Leadership Council som møtes hvert kvartal for å diskutere personvern- og sikkerhetsrisikoer som håndteres i sektorens produktporteføljer. I tillegg spores produktrisiko i en intern portal med månedlig overvåking av etterlevelse.

3. Tiltak for å sikre muligheten til å gjenopprette tilgjengelighet og tilgang til personopplysninger i tide i tilfelle en fysisk eller teknisk hendelse

For å støtte tilgjengeligheten til Trimbles SaaS-produkter benytter Trimble bransjeledende skytjenesteleverandører (Amazon Web Services (AWS) og Microsoft Azure) for automatisk skalering, geografisk diversifiserte datasentre, omfattende applikasjons- og infrastrukturovervåking og supportmekanismer 24/7.
Trimble opprettholder sikkerhetskopier av datalagre, inkludert kundedata, som støtter de primære funksjonene i Trimble-applikasjonene. Sikkerhetskopier lagres på et sted som er geografisk atskilt fra det primære datalagringsstedet der det er mulig.
I tillegg til tiltakene til våre tjenesteleverandører, har Trimble en funksjon for respons på sikkerhetshendelser som omfatter en dokumentert policy og en plan for å håndtere sikkerhetshendelser og hendelser som involverer kundeopplysninger. Dette definerer responsprotokoller som inneslutning, utryddelse, gjenoppretting og kommunikasjonsaktiviteter for sikkerhetshendelser, samt roller og ansvarsområder for Trimble-personell og et krav om gjennomganger med Trimble-ledelsen etter en hendelse.

4. Prosesser for regelmessig testing, vurdering og evaluering av effektiviteten av tekniske og organisatoriske tiltak for å trygge behandlingssikkerheten

Trimble benytter uavhengige tredjeparter til å utføre periodiske inntrengningstester, inkludert Sarbanes-Oxley, PCI, SOC 1, Type II, SOC 2 Type II, ISO27001 eller NIST 800-171-ekvivalente revisjoner på årlig basis der det kreves med tanke på regelverksetterlevelse. I tillegg gjennomfører Trimble regelmessig intern sårbarhetstesting og inntrengningstesting på aktuelle produkter og plattformer i forbindelse med Trimbles cybersikkerhetsprogram og policykrav. Trimble kan utføre gjennomganger av nye leverandører eller partnere hvis forretningsrisikoen tilsier det. Trimble oppfordrer tredjeparter til å rapportere eventuelle cybersikkerhetsproblemer, hendelser og sårbarheter knyttet til våre produkter, tjenester eller nettsteder.

5. Tiltak for brukeridentifikasjon og autorisasjon

For produkter som bruker Trimble ID (TID, Trimble Identity) til autentisering, behandler Trimble passordet på en sikker måte. I tillegg kan enkelte Trimble-produkter støtte Single Sign On (SSO)-integrasjon med en

kundeidentitetsleverandør ved hjelp av Security Assertion Markup Language (SAML) og Multifactor Authentication (MFA).

6. Tiltak for beskyttelse av data under overføring

I henhold til punkt 1 krypterer Trimble kundeopplysninger som overføres over offentlige nettverk mellom kunder og Trimble-applikasjonen ved hjelp av gjeldende krypteringskoder når det er mulig.

7. Tiltak for beskyttelse av data under lagring

I henhold til punkt 1 blir kundeopplysninger som er lagret på Trimble-administrert datalagring, kryptert med AES 256 eller sterkere for alle Trimble-produkter som for øyeblikket er AICPA SOC 1, Type II, SOC 2, Type II eller NIST 800-171-sertifisert. Se punkt 11 for mer detaljert informasjon.

8. Tiltak for å sikre fysisk sikkerhet på steder der personopplysninger behandles

Trimble SaaS-produkter, applikasjoner og tjenester er vanligvis hostet med kundedata som er lagret i datasentre levert av Amazon Web Services (AWS), Microsoft Azure eller Google Cloud Platform (GCP). Trimble er derfor avhengig av de fysiske, miljømessige og infrastrukturmessige kontrollene på disse plattformene. Trimble gjennomgår med jevne mellomrom sertifiseringer og tredjepartsattester fra disse leverandørene når det gjelder effektiviteten av datasenterkontrollene.

9. Tiltak for å sikre logging av hendelser

Trimble fører mange logger for cybersikkerhetsverktøy og sikkerhetsrevisjonslogger for applikasjoner og infrastruktur. Sikkerhetslogger analyseres ved hjelp av SIEM-teknologi i kombinasjon med hendelseskorrelasjon for å oppdage avvikende aktivitet.

10. Tiltak for å sikre systemkonfigurasjon, inkludert standardkonfigurasjon

Trimble benytter felles bransjestandarder for å styrke cybersikkerheten gjennom sikker konfigurasjon og dybdeforsvar. Trimble bruker sikkerhetsoppdateringer på sine systemer i samsvar med Trimble Secure Development Lifecycle Policy (TSDLCP).

11. Tiltak for intern styring og ledelse av IT og IT-sikkerhet

For SOC 1, Type II, SOC 2, Type II eller NIST 800-171 Trimble-sertifiserte produkter bruker personell med tilgang til kundeopplysninger rollebaserte prinsipper for tilgangskontroll. De ansatte får bare tilstrekkelig tilgang til kundeopplysninger til at de kan utføre arbeidsoppgavene sine på en sikker måte. Ekstern nettverkstilgang til Trimble-systemer krever kryptert kommunikasjon via sikrede protokoller og bruk av multifaktorautentisering. Trimble har etablert og vil opprettholde prosedyrer for passordadministrasjon for dette demografiske personellet, som er utformet for å sikre at passordene er unike for hver enkelt person, og utilgjengelige for uautoriserte personer, inkludert som et minimum:

- kryptografisk beskyttelse av passord når passordene lagres i datasystemer eller overføres via et offentlig nettverk
- endring av standardpassord fra leverandører
- opplæring i god passordpraksis, for eksempel bruk av passordfraser
- ansattes tilgang til produksjonsinfrastruktur krever multifaktorautentisering (MFA).

For å overholde ISO 27001-sertifikatet og for å sikre riktig og effektiv bruk av kryptografi til å beskytte konfidensialiteten og integriteten til data som eies eller administreres av Trimble In-Scope Divisions, må data som er klassifisert som konfidensielle eller begrensede, krypteres ved hjelp av gyldige krypteringsprosesser for data i ro og i bevegelse, som påkrevd i henhold til forskrifter og/eller risikovurdering. Dette omfatter, men er ikke begrenset til, sensitiv informasjon som er lagret på mobile enheter, flyttbare stasjoner og bærbare datamaskiner. Trimble In-Scope Divisions vil kun bruke umodifiserte, kommersielle kryptografiprogrammer til å kryptere data i ro og/eller under overføring.

Trimble-ansatte er underlagt konfidensialitetsforpliktelser og ulike retningslinjer, for eksempel Akseptabel bruk, Dataklassifisering, Sikker destruksjon og MFA. Trimble krever at de ansatte gjennomgår opplæring i informasjonssikkerhet, både når de begynner i jobben og deretter hvert år. Trimble krever også at de ansatte gjennomgår opplæring i personvern hvert år (blant annet for å overholde GDPR).

Trimble har implementert prinsipper for sikkerhet og innebygd personvern for aktuelle produkter, inkludert, men ikke begrenset til, trusselmodellering og inntrengningstester av produktapplikasjoner.

12. Tiltak for sertifisering/sikring av prosesser og produkter

Trimble skal opprettholde SOC 2, Type II, ISO 27001- eller NIST 800-171-sertifiseringer og gjennomgå periodisk ekstern overvåking og re-sertifiseringsrevisjoner for å sikre at selskapets styringssystem for informasjonssikkerhet (ISMS) oppfyller kravene i denne standarden for aktuelle produkter.

Trimble har retningslinjer for informasjonssikkerhet som oppfyller kravene i ISO 27001-standarden, et internt revisjonsprogram som vurderer Trimbles ISMS og informasjonssikkerhetskontroller, og en ledelseskomité som er ansvarlig for å føre tilsyn med Trimbles styringssystem for informasjonssikkerhet (ISMS).

13. Tiltak for å sikre dataminimering

Trimble kan tillate besøkende å bruke visse funksjoner i enkelte produkter anonymt, og minimerer de opplysningene som kreves fra kunder til det som er nødvendig for å levere den forespurte tjenesten i henhold til lokale lover og forskrifter.

14. Tiltak for å sikre datakvalitet

Trimble sikrer kvaliteten på opplysningene gjennom ulike verifiseringsmekanismer som er unike for de aktuelle Trimble-produktene. Trimble kan også tillate produktbrukere å oppdatere informasjonen i kontoene sine selv eller via forespørsler til kundestøttefunksjonene.

15. Tiltak for å sikre begrenset oppbevaring av data

Trimble kan implementere kundens retningslinjer for datalagring som angir lagringsperioder for ulike typer opplysninger.

16. Tiltak for å tillate dataportabilitet og sikre sletting

Aktuelle Trimble-produkter har en prosess for sletting av kundeopplysninger innen 30 dager etter mottak av kundebekreftede skriftlige forespørsler, og kan gjøre det mulig å laste ned kundeopplysninger for å gi dem til alternative tjenesteleverandører som påkrevd av GDPR.

17. Kontroll og administrasjon av tredjeparter (underdatabehandlere)

Trimble benytter kun underdatabehandlere som behandler personopplysninger på Trimbles vegne som en del av gjeldende abonnementstjenester i samsvar med personvernlover og -forskrifter. Trimble verifiserer også underdatabehandlerens tekniske og organisatoriske tiltak for å sørge for et sikkerhetsnivå som er tilpasset risikoen ved behandling av kundenes opplysninger, før Trimble velger en underdatabehandler og overfører data. Trimble treffer også rimelige tiltak for å sørge for sikkerheten ved overføring av kundeopplysninger til tredjeparts underdatabehandlere. Som et minimum omfatter slike tiltak identifisering av risikoene for kundens og den registrertes rettigheter basert på behandlingens art, omfang og kontekst; gjennomgang av sikkerhets- og personvernkontrollene som er implementert av underdatabehandleren for å beskytte kundens opplysninger (inkludert SOC 2 Type II-revisjonsrapporter og/eller ISO 27001-sertifikater, alt etter hva som er aktuelt); pålegge kontraktsvilkår for personvern som beskytter personopplysninger til samme eller tilsvarende standard som Trimble er forpliktet til å tilby sine kunder (inkludert gyldige mekanismer for overføring over landegrensene, håndtering av underdatabehandleren og samsvarsprogrammer); kreve at underdatabehandleren kun behandler kundedata på vegne av Trimble og deres kunder, og begrense behandlingen av kundeopplysninger til omfanget som angis av Trimbles instruksjoner.

TILLEGG 3 – Overføringsmekanisme over landegrensene

1. Det europeiske økonomiske samarbeidsområdet (EØS):

1.1 Definisjonen av «personvernlover og -forskrifter» omfatter Generell personvernforordning (EU 2016/679) (***«GDPR»***).

1.2 Når Trimble engasjerer en underdatabehandler i henhold til avsnitt 5.1 (Utnevnelse av underdatabehandlere) i denne DPA-en, vil Trimble:

(a) kreve at enhver utnevnt underdatabehandler beskytter kundeopplysningene i henhold til den standard som kreves av personvernlover og -forskrifter, herunder de samme personvernforpliktelsene som nevnt i artikkel 28(3) i den GDPR, særlig ved å gi tilstrekkelige garantier for å iverksette egnede tekniske og organisatoriske tiltak på en slik måte at behandlingen vil oppfylle kravene i GDPR

(b) kreve at enhver utnevnt underdatabehandler (i) skriftlig samtykker i å kun behandle personopplysninger i et land som EU har erklært at har et «adekvat» beskyttelsesnivå, eller (ii) kun behandler personopplysninger på grunnlag av EUs standard avtalevilkår eller i henhold til bindende virksomhetsregler som er godkjent av kompetente personvernmyndigheter i EU.

1.3 Uavhengig av det motsatte i denne DPA-en eller i avtalen (inkludert, uten begrensning, en av partenes erstatningsforpliktelser), skal ingen av partene være ansvarlig for eventuelle GDPR-bøter som utstedes eller ilegges i henhold til artikkel 83 i GDPR mot den andre parten av en tilsynsmyndighet eller statlig organ i forbindelse med den andre partens brudd på GDPR.

1.4 Kunden erkjenner at Trimble, som behandlingsansvarlig, kan være pålagt i henhold til personvernlover og -forskrifter å varsle en tilsynsmyndighet om sikkerhetshendelser som involverer kundens bruksdata. Hvis en tilsynsmyndighet krever at Trimble skal varsle berørte registrerte som Trimble ikke har et direkte forhold til (f.eks. kundens sluttbrukere), skal Trimble varsle kunden om dette kravet. Kunden skal gi Trimble rimelig assistanse til å varsle de registrerte som er berørt.

2. Storbritannia (UK):

2.1 Henvisninger til «GDPR» i denne DPA-en skal anses som henvisninger til de tilsvarende lovene og forskriftene i Storbritannia, inkludert, uten begrensning, Storbritannias GDPR and Data Protection Act 2018.

2.2 Når Trimble engasjerer en underdatabehandler i henhold til avsnitt 5.1 (Utnevnelse av underdatabehandlere) i denne DPA-en, vil Trimble:

(a) kreve at enhver utnevnt underdatabehandler beskytter kundeopplysningene i henhold til den standard som kreves av personvernlover og -forskrifter, herunder de samme personvernforpliktelsene som nevnt i artikkel 28(3) i den britiske GDPR, særlig ved å gi tilstrekkelige garantier for å iverksette egnede tekniske og organisatoriske tiltak på en slik måte at behandlingen vil oppfylle kravene i britiske GDPR

(b) kreve at enhver utnevnt underdatabehandler (i) skriftlig samtykker i å kun behandle personopplysninger i et land som Storbritannia har erklært at har et «adekvat» beskyttelsesnivå eller (ii) kun behandler personopplysninger på vilkår som tilsvarer Storbritannias International Data Transfer Agreement eller EUs standard avtalevilkår og Storbritannias International Data Transfer Addendum eller i henhold til bindende virksomhetsregler som er godkjent av kompetente britiske personvernmyndigheter.

2.3 Uavhengig av det motsatte i denne DPA-en eller i avtalen (inkludert, uten begrensning, en av partenes erstatningsforpliktelser), skal ingen av partene være ansvarlig for eventuelle britiske GDPR-bøter som utstedes eller ilegges i henhold til artikkel 83 i britiske GDPR mot den andre parten av en tilsynsmyndighet eller statlig organ i forbindelse med den andre partens brudd på britiske GDPR.

2.4 Kunden erkjenner at Trimble, som behandlingsansvarlig, kan være pålagt i henhold til personvernlover og -forskrifter å varsle en tilsynsmyndighet om sikkerhetshendelser som involverer kundens bruksdata. Hvis en tilsynsmyndighet krever at Trimble skal varsle berørte registrerte som Trimble ikke har et direkte forhold til (f.eks. kundens sluttbrukere), skal Trimble varsle kunden om dette kravet. Kunden skal gi Trimble rimelig assistanse til å varsle de registrerte som er berørt.

3. Sveits:

3.1 Definisjonen av «lover og forskrifter om personvern» inkluderer den sveitsiske føderale loven om personvern, som revidert (***«FADP»***).

3.2 Når Trimble engasjerer en underdatabehandler i henhold til avsnitt 5.1 (Utnevnelse av underdatabehandlere) i denne DPA-en, vil Trimble:

(a) kreve at enhver utnevnt underdatabehandler beskytter kundeopplysningene i henhold til den standard som kreves av personvernlover og -forskrifter, særlig ved å gi tilstrekkelige garantier for å iverksette egnede tekniske og organisatoriske tiltak på en slik måte at behandlingen vil oppfylle kravene i FADP

(b) kreve at enhver utnevnt underdatabehandler (i) skriftlig samtykker i å kun behandle personopplysninger i et land som Sveits har erklært at har et «adekvat» beskyttelsesnivå, eller (ii) kun behandler personopplysninger på vilkår som tilsvarer EUs standard avtalevilkår, inkludert endringene nevnt i punkt 3.3, eller i henhold til bindende virksomhetsregler som er godkjent av kompetente personvernmyndigheter i Den europeiske union eller Sveits.

3.3 I den grad overføring av personopplysninger fra Sveits er underlagt EUs standard avtalevilkår i samsvar med avsnitt 2.3 i Tillegg 3 (EUs standard avtalevilkår), er partene enige om at alle endringer som anses som nødvendige av den sveitsiske føderale personvern- og informasjonskommissæren, skal gjøres i EUs standard avtalevilkår. Disse er spesifikt på tidspunktet for inngåelse av DPA-en:

(a) henvisninger til «EU-medlemsstat» og «medlemsstat» skal tolkes slik at de omfatter Sveits

(b) i den grad overføringen eller videreoverføringen er underlagt FADP:

(i) henvisninger til «forordning (EU) 2016/679» skal tolkes som henvisninger til FADP

(ii) den «kompetente tilsynsmyndigheten» i Vedlegg I, del C vil være den sveitsiske føderale personvern- og informasjonskommissæren

(iii) i Bestemmelse 17 (Alternativ 1) vil EUs standard kontraktsbestemmelser være underlagt lovgivningen i Sveits

(iv) i Bestemmelse 18(b) i EUs standard kontraktsbestemmelser skal tvister løses ved domstolene i Sveits

(v) Bestemmelse 18(c) i EUs standard kontraktsbestemmelser gjelder, mens den registrerte også kan anlegge sak mot dataeksportøren og/eller dataimportøren ved domstolene i Sveits, der den registrerte har sitt vanlige bosted.

4. Amerikas forente stater:

4.1 ***«Amerikanske delstaters personvernlover»*** betyr alle delstatslover knyttet til beskyttelse og behandling av personopplysninger som gjelder i USA, som kan omfatte, uten begrensning, California Consumer Privacy Act, som endret ved California Privacy Rights Act (***«CCPA»***), Virginia Consumer Data Protection Act, Colorado Privacy Act, Connecticut Data Privacy Act og Utah Consumer Privacy Act.

4.2 Definisjonen av «lover og forskrifter om databeskyttelse» inkluderer personvernlover i amerikanske delstater.

4.3 Følgende vilkår gjelder der Trimble behandler personopplysninger som er underlagt CCPA:

(a) Begrepet ***«personopplysning»***, slik det brukes i denne avsnitt 4.3, vil ha den betydningen som er angitt i CCPA

(b) Trimble er en tjenesteleverandør ved behandling av kundedata. Trimble vil kun behandle personopplysningene i kundedataene for de forretningsformålene som er angitt i avtalen, inkludert formålet med behandlingen og behandlingsaktivitetene som er angitt i denne DPA-en (***«Formål»***). Som tjenesteleverandør skal ikke Trimble selge eller dele kundeopplysninger eller oppbevare, bruke eller utlevere kundeopplysninger (i) for andre formål enn formålet, inkludert å oppbevare, bruke eller utlevere kundeopplysninger for et annet kommersielt formål enn formålet, eller som på annen måte tillatt av CCPA; eller (ii) utenfor det direkte forretningsforholdet mellom kunden og Trimble.

(c) Trimble skal (i) overholde forpliktelsene som gjelder for Trimble som tjenesteleverandør i henhold til CCPA, og (ii) gi personopplysninger samme nivå av personvernbeskyttelse som kreves av CCPA. Kunden er ansvarlig for å sikre at den har overholdt, og vil fortsette å overholde, kravene i CCPA i sin bruk av tjenestene og sin egen behandling av personopplysninger.

(d) Kunden vil ha rett til å ta rimelige og hensiktsmessige skritt for å bidra til å sikre at Trimble bruker personopplysninger på en måte som er i samsvar med kundens forpliktelser i henhold til CCPA.

(e) Trimble vil varsle kunden dersom Trimble fastslår at de ikke lenger kan oppfylle sine forpliktelser som tjenesteleverandør i henhold til CCPA.

(f) Ved varsel vil kunden ha rett til å ta rimelige og hensiktsmessige skritt i samsvar med avtalen for å stoppe og utbedre uautorisert bruk av personlig informasjon.

(g) Trimble skal yte rimelig ekstra og rettidig assistanse for å hjelpe kunden med å overholde sine forpliktelser med hensyn til forbrukerforespørsler som angitt i avtalen.

(h) For enhver underdatabehandler som Trimble bruker til å behandle personopplysninger som er underlagt CCPA, vil Trimble sikre at Trimbles avtale med en slik underdatabehandler er i samsvar med CCPA, inkludert, uten begrensning, de kontraktsmessige kravene til tjenesteleverandører og entreprenører.

(i) Trimble skal ikke kombinere kundedata som de mottar fra, eller på vegne av, kunden med personopplysninger som de mottar fra, eller på vegne av, en annen person eller andre personer, eller samler inn fra sin egen interaksjon med forbrukeren, med mindre en slik kombinasjon er nødvendig for å utføre et forretningsformål som er tillatt av CCPA, inkludert eventuelle forskrifter til denne, eller av forskrifter vedtatt av California Privacy Protection Agency.

(j) Trimble bekrefter at selskapet forstår og vil overholde sine forpliktelser i henhold til CCPA.

4.4 Trimble erkjenner og bekrefter at de ikke mottar kundeopplysninger som vederlag for noen tjenester som leveres til kunden.

5. Australia:

5.1 Definisjonen av «personvernlover og -forskrifter» omfatter Australian Privacy Principles og Australian Privacy Act (1988).

5.2 Definisjonen av «personopplysninger» omfatter «Personal Information» som definert i henhold til personvernlover og -forskrifter.

5.3 Definisjonen av «sensitive data» omfatter «Sensitive Information» som definert i henhold til personvernlover og -forskrifter.

6. Brasil:

6.1 Definisjonen av «lover og forskrifter om personvern» omfatter Lei Geral de Proteção de Dados (den generelle personvernloven).

6.2 Definisjonen av «sikkerhetshendelse» omfatter en sikkerhetshendelse som kan føre til en relevant risiko eller skade for de registrerte.

6.3 Definisjonen av «databehandler» inkluderer «operatør» som definert i henhold til personvernlover og -forskrifter.

7. Canada:

7.1 Definisjonen av «personvernlover og -forskrifter» inkluderer Federal Personal Information Protection og Electronic Documents Act.

7.2 Trimbles underdatabehandlere, som angitt i punkt 5 (underdatabehandlere) i denne DPA-en, er tredjeparter i henhold til personvernlover og -forskrifter, som Trimble har inngått en skriftlig kontrakt med som inneholder vilkår som i det vesentlige ligner på denne DPA-en. Trimble har gjennomført en passende aktsomhetsvurdering av sine underdatabehandlere.

7.3 Trimble skal iverksette tekniske og organisatoriske tiltak som beskrevet i punkt 11 i Tillegg 2 (Sikkerhet) i denne DPA-en.

8. Israel:

8.1 Definisjonen av «personvernlover og -forskrifter» inkluderer personvernloven.

8.2 Definisjonen av «behandlingsansvarlig» omfatter «Database Owner» som definert i henhold til personvernlover og -forskrifter.

8.3 Definisjonen av «databehandler» inkluderer «Holder» som definert i henhold til personvernlover og -forskrifter.

8.4 Trimble vil kreve at alt personell som er autorisert til å behandle kundeopplysninger, overholder prinsippet om taushetsplikt og er blitt behørig instruert om personvernlover og -forskrifter. Personellet undertegner konfidensialitetsavtaler med Trimble i samsvar med punkt 6 (Konfidensialitet) i denne DPA-en.

8.5 Trimble må iverksette tilstrekkelige tiltak for å sikre personvernet til de registrerte ved å implementere og opprettholde sikkerhetstiltakene som er spesifisert i avsnitt 11 i Tillegg 2 (Sikkerhet) i denne DPA-en og overholde vilkårene i avtalen.

8.6 Trimble må sørge for at personopplysningene ikke overføres til en underdatabehandler med mindre en slik underdatabehandler har inngått en avtale med Trimble i henhold til punkt 5.1 (Utnevnelse av underdatabehandlere) i denne DPA-en.

9. Japan:

9.1 Definisjonen av «personvernlover og -forskrifter» inkluderer lov om beskyttelse av personopplysninger (***«APPI»***).

9.2 Definisjonen av «personopplysninger» omfatter informasjon om en bestemt person som gjelder i henhold til § 2(1) i APPI, som kunden overlater til Trimble i forbindelse med Trimbles tilveiebringelse av tjenestene til kunden.

9.3 Trimble samtykker i at de har og vil opprettholde et personvernprogram som er i samsvar med standardene som er foreskrevet av regler fra Personal Information Protection Commission vedrørende håndtering av personopplysninger i henhold til bestemmelsene i kapittel 4 i APPI. Følgelig skal:

(a) Trimble (i) behandle personopplysninger som nødvendig for å levere tjenestene til kunden i henhold til avtalen og som angitt i Tillegg 1 (Beskrivelse av behandlingen) i denne DPA-en (*«Formålet med behandlingen»*) og (ii) ikke behandle personopplysninger for noe annet formål enn Formålet med behandlingen uten kundens samtykke.

(b) Trimble implementere og opprettholde tiltak som er hensiktsmessige og nødvendige for å forhindre uautorisert utlevering og tap av personopplysninger og for sikker håndtering av personopplysninger i samsvar med APPI som we angitt i Tillegg 2 (Tekniske og organisatoriske tiltak) i denne DPA-en.

(c) Trimble varsle kunden om (i) manglende overholdelse av punkt 9.3(a) i dette Tillegg 3 eller (ii) Trimbles oppdagelse av en sikkerhetshendelse som påvirker kundeopplysningene, i begge tilfeller i samsvar med punkt 6.4 i denne DPA-en. Trimble skal yte rimelig assistanse til kunden i tilfelle kunden er pålagt å varsle en tilsynsmyndighet eller noen registrerte som er berørt av en sikkerhetshendelse.

(d) Trimble sørge for at alle ansatte som har tilgang til personopplysninger, (i) har undertegnet medarbeideravtaler som krever at de holder slike personopplysninger konfidensielle, og (ii) som bryter konfidensialiteten, vil bli gjenstand for disiplinærtiltak og mulig oppsigelse; (iii) utfører passende tilsyn og opplæring av ansatte for sikker håndtering av personopplysninger; og (iv) begrenser antallet autorisert personell, inkludert Trimbles ansatte, som har tilgang til personopplysninger, og kontrollerer slik tilgang slik at den kun er tillatt i den tidsperioden som er nødvendig for formålet med behandlingen.

(e) Trimble ikke utlevere personopplysninger til noen tredjepart, med mindre kunden har autorisert Trimble til å gjøre dette i avtalen. Når Trimble engasjerer underdatabehandlere, vil Trimble overholde forpliktelsene i avsnitt 9 (Underdatabehandlere) i denne DPA-en for å sikre at prosedyrer er på plass for å opprettholde konfidensialiteten og sikkerheten til personopplysningene.

(f) Trimble føre register over håndteringen av personopplysninger som er betrodd Trimble av, og utført for, kunden.

(g) kunden vurdere Trimbles overholdelse av sine forpliktelser i henhold til personvernlover og -forskrifter og som angitt i punkt 6 i denne DPA-en.

(h) Trimble yte rimelig samarbeid til kunden ved skriftlig forespørsel, der kunden rapporterer til Personal Information Protection Commission eller andre regulerende myndigheter.

(i) Trimbles primære behandlingsanlegg være lokalisert i USA, og, avhengig av kundens bruk av tjenestene, fra de stedene som er angitt på https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center under «Tilleggsressurser» («Lister over underdatabehandlere»). Trimble vil varsle kunden om enhver endring og gi kunden muligheten til å protestere i samsvar med punkt 9 i denne DPA-en. Der Trimble behandler personopplysninger i et annet land enn Japan, vil Trimble sørge for å overholde sitt personvernprogram som beskrevet i denne DPA-en.

9.4 Følgende vilkår for samtykke fra den registrerte gjelder:

(a) Kunden overlater personopplysninger til Trimble for formålet med behandlingen. Kunden samtykker i at Trimble ikke er en «tredjepart» slik begrepet brukes i APPI-bestemmelsene som begrenser utlevering av personopplysninger til tredjeparter. Kravet om å innhente samtykke fra den registrerte på forhånd gjelder derfor ikke.

(b) hvis samtykke fra den registrerte er påkrevd i henhold til artikkel 4 i lov om telekommunikasjonsvirksomhet, vil kunden overholde eventuelle samtykkekrav som er spesifikke for kundens bruk av tjenestene.

10. Mexico:

10.1 Definisjonen av «personvernlover og -forskrifter» omfatter den føderale loven om beskyttelse av personopplysninger som innehas av private parter og tilhørende forskrifter.

10.2 Når Trimble fungerer som behandler, skal Trimble:

(a) behandle personopplysninger i samsvar med kundens instruksjoner slik det er beskrevet i avsnitt 5 i denne DPA-en.

(b) behandle personopplysninger kun i den grad det er nødvendig for å levere tjenestene.

(c) iverksette sikkerhetstiltak i samsvar med personvernlover og -forskrifter og Tillegg 2 (Tekniske og organisatoriske tiltak) i denne DPA-en.

(d) bevare konfidensialitet om personopplysningene som behandles i henhold til avtalen.

(e) slette alle personopplysninger ved opphør av avtalen i samsvar med avsnitt 10 (Retur eller sletting av kundedata) i denne DPA-en.

(f) kun overføre personopplysninger til underdatabehandlere i samsvar med avsnitt 9 (Underdatabehandlere) i denne DPA-en.

11. Singapore:

11.1 Definisjonen av «personvernlover og -forskrifter» inkluderer Personal Data Protection Act 2012 (***«PDPA»***).

11.2 Trimble skal behandle personopplysninger i henhold til en beskyttelsesstandard som er i samsvar med PDPA ved å implementere tilstrekkelige tekniske og organisatoriske tiltak som angitt i Tillegg 2 (Tekniske og organisatoriske tiltak) i denne DPA-en og overholde vilkårene i avtalen.

12. Tyrkia

12.1 Definisjonen av «personvernlover og -forskrifter» omfatter (i) lov om beskyttelse av personopplysninger («PDPL»), lov nr. 6698, fra 24. mars 2016, som endret ved lov om endringer i straffeprosessloven og andre lover, lov nr. 7499, fra 2. mars 2024, og (ii) forskrift om prinsipper for prosedyrer og regler for overføring av personopplysninger til utlandet fra de tyrkiske personvernmyndighetene, publisert i Official Gazette 10. juli, nummer 32598.

12.2 Kunden erkjenner at Trimble, som behandlingsansvarlig, kan være pålagt i henhold til personvernlover og -forskrifter å varsle en tilsynsmyndighet om sikkerhetshendelser som involverer kundens bruksdata. Hvis en tilsynsmyndighet krever at Trimble skal varsle berørte registrerte som Trimble ikke har et direkte forhold til (f.eks. kundens sluttbrukere), skal Trimble varsle kunden om dette kravet. Kunden skal gi Trimble rimelig assistanse til å varsle de registrerte som er berørt.

TILLEGG 4 - MEKANISME FOR GRENSEOVERSKRIDENDE OVERFØRING
(Gjelder for opplysninger som overføres fra EU, EØS, Storbritannia og Sveits)

1. Definisjoner

- ***«EUs standard avtalevilkår»*** betyr standardkontraktsbestemmelsene som er godkjent av Europakommisjonen i beslutning 2021/914.
- ***«Storbritannias International Data Transfer Agreement»*** betyr det internasjonale dataoverføringstillegget til EU-kommisjonens standard avtalevilkår utstedt av Storbritannias Information Commissioner, versjon B1.0, som trådte i kraft 21. mars 2022.
- ***«Rammeverk for personvern»*** betyr rammeverket for personvern mellom EU og USA og/eller Sveits og USA, et egensertifiseringsprogram som drives av det amerikanske handelsdepartementet (Department of Commerce).
- ***«Personvernprinsipper»*** betyr prinsippene i rammeverket for personvern (som supplert av Tilleggsprinsippene).
- ***«Tyrkiske standard avtalevilkår»*** betyr standardkontrakten som skal brukes ved overføring av personopplysninger til utlandet 1-4 som akseptert ved beslutning 2024/959 fra 4. juni 2024 av de tyrkiske personvernmyndighetene.

2. Mekanismer for dataoverføring på tvers av landegrensene

2.1 Prioritetsrekkefølge. Dersom tjenestene dekkes av flere enn én overføringsmekanisme, vil overføringen av personopplysninger være underlagt én enkelt overføringsmekanisme, alt etter hva som er aktuelt, og i samsvar med følgende rekkefølge: (a) rammeverket for personvern som det henvises til i avsnitt 2.2 (Rammeverk for personvern) i dette tillegget; (b) EUs standard avtalevilkår som det henvises til i avsnitt 2.3 (EUs standard avtalevilkår) i dette tillegget; (c) Storbritannias International Data Transfer Addendum som det henvises til i avsnitt 2.4 (Storbritannias International Data Transfer Addendum) i dette tillegget; og hvis verken (a), (b), (c), (d) eller (e) er relevante, gjelder (f) andre gjeldende dataoverføringsmekanismer som er tillatt i henhold til personvernlover og -forskrifter.

2.2 Rammeverk for personvern. I den grad Trimble Inc. behandler personopplysninger via tjenester som stammer fra EØS eller Sveits, er Trimble Inc. selvsertifisert i henhold til rammeverket for personvern og overholder personvernprinsippene ved behandling av slike personopplysninger. I den grad kunden er (a) lokalisert i USA og også er selvsertifisert i henhold til rammeverket for personvern eller (b) lokalisert i EØS eller Sveits, samtykker Trimble videre i (i) å gi minst det samme beskyttelsesnivået for alle personopplysninger som kreves av personvernprinsippene; (ii) å varsle kunden skriftlig, uten unødig forsinkelse, dersom egenerklæringen til rammeverket for personvern trekkes tilbake, avsluttes, tilbakekalles eller på annen måte ugyldiggjøres (i så fall vil en alternativ overføringsmekanisme gjelde i samsvar med prioritetsrekkefølgen i avsnitt 2.1 (Prioritetsrekkefølge) i dette Tillegg 4; og (iii) etter skriftlig varsel, samarbeide med kunden for å iverksette rimelige og hensiktsmessige tiltak for å stanse og utbedre enhver uautorisert behandling av personopplysninger.

2.3 EUs standard avtalevilkår. EUs standard avtalevilkår skal gjelde for personopplysninger som overføres via tjenestene fra EØS, Sveits eller Storbritannia, enten direkte eller via videre overføring, til et land eller en mottaker utenfor EØS, Sveits eller Storbritannia som ikke er anerkjent av den relevante kompetente myndigheten som et land eller en mottaker som gir et tilstrekkelig beskyttelsesnivå for personopplysninger. For dataoverføringer som er underlagt EUs standard avtalevilkår, skal EUs standard avtalevilkår anses som inngått og innlemmet i denne DPA-en ved denne henvisningen, og utfylt på følgende måte:

(a) Modul én (behandlingsansvarlig til behandlingsansvarlig) i EUs standard avtalevilkår skal gjelde der (i) Trimble behandler kundekontodata og (ii) kunden er behandlingsansvarlig for kundens bruksdata og Trimble behandler kundens bruksdata.

(b) Modul to (behandlingsansvarlig til databehandler) i EUs standard avtalevilkår skal gjelde der kunden er behandlingsansvarlig for personopplysningene og Trimble behandler personopplysningene på kundens vegne.

(c) Modul tre (databehandler til databehandler) i EUs standard avtalevilkår skal gjelde der kunden er behandler av personopplysninger og Trimble behandler som underdatabehandler på kundens vegne.

(d) For hver modul, der det er aktuelt:

(i) I bestemmelse 7 i EUs standard avtalevilkår skal den valgfrie inntredelsesklausulen ikke gjelde.

(ii) I bestemmelse 9 i EUs standard avtalevilkår skal alternativ 2 gjelde, og tidsfristen for skriftlig forhåndsvarsel om endringer av underdatabehandler vil være som angitt i punkt 5.2 (Liste over nåværende underdatabehandlere og melding om nye underdatabehandlere) i denne DPA-en.

(iii) I bestemmelse 11 i EUs standard avtalevilkår skal det valgfrie språket ikke gjelde.

(iv) Identifisere den eller de kompetente tilsynsmyndighetene i samsvar med bestemmelse 13;

(v) I bestemmelse 17 (alternativ 1) skal EUs standard avtalevilkår være underlagt nederlandsk lov.

(vi) i bestemmelse 18(b) i EUs standard avtalevilkår skal tvister løses ved domstolene i Amsterdam, Nederland.

(vii) I Vedlegg I, del A i EUs standard avtalevilkår:

Dataeksportør: Kunde (hvis boksen på side 6 er krysset av).

Kontaktinformasjon: E-postadressen(e) som er angitt av kunden i kundens konto via varslingspreferansene.

Dataeksportørrolle: Dataeksportørens rolle er beskrevet på side 6.

Underskrift og dato: Ved å inngå avtalen anses dataeksportøren å ha undertegnet disse standard EU-avtalevilkårene som er innlemmet i avtalen, inkludert vedleggene, ved avtalens ikrafttredelsesdato.

Dataimportør: Trimble Inc.

Kontaktinformasjon: Trimble Privacy Team - privacy@Trimble.com

Dataimportørrolle: Dataimportørens rolle er beskrevet på side 6

Underskrift og dato: Ved å inngå avtalen anses dataimportøren å ha undertegnet disse standard EU-avtalevilkårene som er innlemmet i avtalen, inkludert vedleggene, ved avtalens ikrafttredelsesdato.

(viii) I Vedlegg I, del B i EUs standard avtalevilkår:

Kategoriene av registrerte er angitt i avsnitt 1 i Vedlegg 1 (Beskrivelse av behandlingen) i denne DPA-en.

De sensitive opplysningene som overføres, er angitt i avsnitt 3 i Tillegg 1 (Beskrivelse av behandlingen) i denne DPA-en.

Overføringshyppigheten er kontinuerlig under hele avtalens varighet.

Arten av behandlingen er beskrevet i avsnitt 5 i Tillegg 1 (Beskrivelse av behandlingen) i denne DPA-en.

Formålet med behandlingen er beskrevet i avsnitt 6 i Tillegg 1 (Beskrivelse av behandlingen) i denne DPA-en.

Perioden som personopplysningene vil bli oppbevart, er angitt i avsnitt 7 i Tillegg 1 (Beskrivelse av behandlingen) i denne DPA-en.

For overføringer til underdatabehandlere er behandlingens formål, art og varighet angitt på https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center under «Tilleggsressurser» («Lister over underdatabehandlere»).

(ix) I Vedlegg I, del C i EUs standard avtalevilkår: Der det er aktuelt, skal den nederlandske personvernkommisjonen være ledende tilsynsmyndighet. Ellers, der en Trimble-enhet som er hjemmehørende i EU er dataeksportør, er den kompetente tilsynsmyndigheten tilsynsmyndigheten i den medlemsstaten Trimble-enheten er hjemmehørende i. Når kunden er dataeksportør, er den kompetente tilsynsmyndigheten tilsynsmyndigheten i det medlemslandet kunden er bosatt i.

(x) Tillegg 2 (Tekniske og organisatoriske sikkerhetstiltak) i denne DPA-en fungerer som Vedlegg II i EUs standard avtalevilkår.

2.4 Storbritannias utvidelse av rammeverket for personvern og tillegget om internasjonal dataoverføring. Kunden og Trimble er enige om at den britiske utvidelsen av rammeverket for personvern skal gjelde, og i mangel av dette vil EUs standard avtalevilkår og Storbritannias International Data Transfer Addendum til EU-kommisjonens standard avtalevilkår i sin nyeste versjon gjelde for personopplysninger som overføres via tjenestene fra Storbritannia, enten direkte eller via videre overføring, til et land eller en mottaker utenfor Storbritannia som ikke er anerkjent av den kompetente britiske tilsynsmyndigheten eller myndighetsorganet for Storbritannia som et land eller en mottaker som gir et adekvat beskyttelsesnivå for personopplysninger. For dataoverføringer fra Storbritannia som er underlagt EUs standard avtalevilkår og Storbritannias International Data Transfer Addendum, skal EUs standard avtalevilkår anses som inngått og innlemmet i denne DPA-en som beskrevet i avsnitt 2.3 i dette avsnitt 4, og Storbritannias International Data Transfer Addendum skal anses som inngått og innlemmet i denne DPA-en ved denne referansen, og utfylt på følgende måte:

(a) I tabell 1 i Storbritannias International Data Transfer Addendum er kundens og Trimbles detaljer og nøkkelkontaktinformasjon angitt i avsnitt 2.3 (e)(vii) i dette Tillegg 3.

(b) I tabell 2 i Storbritannias International Data Transfer Addendum er informasjon om versjonen av EUs standard avtalevilkår og utvalgte bestemmelser som Storbritannias International Data Transfer Addendum lagt ved, angitt i avsnitt 2.3 (EUs standard avtalevilkår) i dette Tillegg 4.

(c) I tabell 3 i Storbritannias International Data Transfer Addendum:

(i) Listen over parter er angitt i punkt 2.3(e)(vii) i dette Tillegg 3.

(ii) Beskrivelsen av overføringen er angitt i avsnitt 1 (Behandlingens art og formål) i Tillegg 1 (Beskrivelse av behandlingen).

(iii) Vedlegg II finnes i Tillegg 2 (Tekniske og organisatoriske sikkerhetstiltak) i denne DPA-en.

(iv) Listen over underdatabehandlere finnes på https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center under «Tilleggsressurser» («Lister over underdatabehandlere»)

(d) I tabell 4 i Storbritannias International Data Transfer Addendum kan både importøren og eksportøren avslutte UK International Data Transfer Agreement i samsvar med vilkårene i Storbritannias International Data Transfer Addendum.

2.5 Tyrkiske standard avtalevilkår. De tyrkiske standard avtalevilkårene skal gjelde for personopplysninger som overføres via tjenestene fra Tyrkia, enten direkte eller via videre overføring, til et land eller en mottaker utenfor Tyrkia som ikke er anerkjent av den kompetente myndigheten som et land som gir et tilstrekkelig beskyttelsesnivå for personopplysninger. For dataoverføringer som er underlagt tyrkisk standard avtalevilkår, skal Tyrkisk standard avtalevilkår anses som inngått og innlemmet i denne DPA-en ved denne henvisningen, og utfylt på følgende måte:

For hver modul, der det er aktuelt:

(i) I artikkel 8 i kontrakt 2 og kontrakt 3 i de tyrkiske standard avtalevilkårene, skal alternativ 2 gjelde, og tidsperioden for skriftlig forhåndsvarsel om endringer av underdatabehandler skal være som angitt i avsnitt 5.2 (Liste over nåværende underdatabehandlere og melding om nye underdatabehandlere) i denne DPA-en.

(ii) Partene er enige om at kunden skal varsle det kompetente tyrkiske personvernmyndighetene innen fem (5) virkedager for å informere om inngåelsen av de tyrkiske standard avtalevilkårene.

(iii) Dataimportøren skal være: Trimble med adresser, navn og etternavn, tittel og kontaktinformasjon for Trimble og underskriveren som angitt i DPA-en.

(iv) Underskrift og dato: Ved å inngå avtalen anses Trimble og dataeksportøren å ha undertegnet disse tyrkiske standard avtalevilkårene som er innlemmet i avtalen, inkludert vedleggene, fra og med ikrafttredelsesdatoen for avtalen.

(v) Opplysningene i Vedlegg I til de tyrkiske standard avtalevilkårene er gjengitt i Tillegg 1:

(vi) Tillegg 2 (Tekniske og organisatoriske sikkerhetstiltak) i denne DPA-en fungerer som Vedlegg II i de tyrkiske standard avtalevilkårene.

(vii) Listen over underdatabehandlere finnes på https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center under «Tilleggsressurser» («Lister over underdatabehandlere»).

2.6 Konflikt. I den grad det er noen konflikt eller uoverensstemmelse mellom EUs standard avtalevilkår, Storbritannias internasjonale dataoverføringsavtale eller de tyrkiske standard avtalevilkårene og andre vilkår i denne DPA-en, inkludert Tillegg 4 (Overføringsmekanisme over landegrensene), skal avtalen, bestemmelsene i EUs standard avtalevilkår, Storbritannias internasjonale dataoverføringstillegg og de tyrkiske standard avtalevilkår, alt etter hva som er aktuelt, ha forrang.