DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is the parties' agreement with regard to the Processing of Personal Data and supplements all License, Subscription, Services or other written or electronic agreements (the "**Agreements**") between Trimble and Customer for the purchase of services (including Software as a Service, their associated Trimble offline or mobile applications, and support, and defined as "Services" or otherwise in the Agreement or hereinafter) in the course of which Trimble receives personal data from Customer.

Customer enters into this DPA (i) by signing or otherwise accepting the Agreement, (ii) upon signing it on behalf of itself and as required under applicable Data Protection Laws and Regulations, in the name and on behalf of Authorized Affiliates, if and to the extent Trimble processes Personal Data. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates.

In the course of providing the Services to Customer pursuant to the Agreement, Trimble may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data.

HOW TO EXECUTE THIS DPA:

I. This DPA consists of: the main body of the DPA, and Schedules 1 to 3
II. It has been pre-signed on behalf of Trimble. The Standard Contractual Clauses (as defined below) are incorporated by reference.
III. If Customer wants to complete this DPA Customer must:
    a. Complete the information in the signature box and sign on Page 6.
    b. Complete the information as the data exporter on Page 6.
IV. Send the completed and signed DPA to Trimble by email, indicating your organization's Customer's Account Number (as set out on the applicable Trimble invoice), to privacy@trimble.com.

HOW THIS DPA APPLIES:

- 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.
- If the Customer entity signing this DPA has submitted an order that has been accepted by Trimble or any of its Affiliates, but is not itself a party to the Agreement, this DPA is an addendum to that order (including any renewal order) and the Trimble entity on which such order has been placed is party to this DPA.
- If the Customer entity signing the DPA has purchased Trimble services via an authorized reseller of Trimble, Customer has to indicate so on page 6 and provide a Trimble or Reseller issued customer number, or, in lack thereof, confirmation from the reseller that Customer is subscribed to a Trimble service. In this case, this DPA will be considered as a direct agreement between Customer and Trimble.
- If the entity or individual signing this DPA is neither a party to an order nor an Agreement and not an indirect customer through a reseller, this DPA is not valid and is not legally binding. Such entity should request that its affiliated entity who is a party to the Agreement executes this DPA, or requests in writing to become part of the Agreement.

This DPA does not replace any comparable or additional rights relating to Processing of Customer Data contained in the Agreement (including any existing data processing addendum to the Agreement).

DATA PROCESSING TERMS

1. DEFINITIONS

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the outstanding voting interests of the subject entity.

"**Authorized Affiliate**" means any of Customer's Affiliate(s) which (i) is subject to one or more Data Protection Laws and (ii) is permitted to use the Services pursuant to the Agreement between Customer and Trimble, but has not signed their own order with Trimble and is not a "Customer" as defined under the Agreement.

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Customer**" means the entity that executed the Agreement, together with its Affiliates (for so long as they remain Affiliates) which have signed Order Forms.

"**Customer Data**" means what is defined in the Agreement as "Customer Data" or "Your Data."

"**Data Protection Laws and Regulations**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, the countries listed in Schedule 3 and all other countries in which Customer or a Customer affiliates has a seat, all as applicable to the Processing of Personal Data under the Agreement.

"**Data Subject**" means the individual to whom Personal Data relates.

"**Europe**" means the European Union (EU), the European Economic Area (EEA) and Switzerland.

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council.

"**Personal Data**" means any information relating to (i) an identified or identifiable person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), provided such data is Customer Data.

"**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, blocking, erasure or destruction.

"**Processor**" means the entity which processes Personal Data on instruction and on behalf of the Controller, including, as applicable, any "service provider" as that term is defined by the CCPA.

"**Public Authority**" means a government agency or law enforcement authority, including judicial authorities.

"**EU Standard Contractual Clauses**" means an agreement executed by and between either (i) a Trimble Affiliate and Trimble Inc. or (ii) Customer and Trimble Inc., each pursuant to the implementing decision (EU) 2021/914.

"**Sub-processor**" means any Processor engaged by Trimble or a member of the Trimble Group.

"**Trimble**" means the Trimble entity, which is a party to this DPA, as specified in the section "HOW THIS DPA APPLIES" above. Trimble entities acting as Processors are: Trimble Inc., a company incorporated in Delaware, Trimble Europe B.V., a company registered in the Netherlands, Trimble International B.V., a company incorporated in the Netherlands, Trimble UK Ltd, a company incorporated in England and Wales, Trimble Maps, Ltd, a company incorporated in England and Wales, Trimble Technologies Ireland Ltd, a company incorporated in Ireland, Trimble France SAS, a company incorporated in France, Trimble Solutions Sandvika AS, a company incorporated in Norway, Trimble Finland Corporation, a company incorporated in Finland, Trimble Forestry Europe Corporation, a company incorporated in Finland, Lakefield eTechnologies Ltd, a company incorporated in Ireland, Trimble GmbH, a company incorporated in Germany, or Trimble Germany GmbH, a company incorporated in Germany, each as applicable.

"**Trimble Group**" means Trimble and its Affiliates engaged in the Processing of Personal Data.

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, Trimble is a Processor and that Trimble or members of the Trimble Group will engage Sub-processors pursuant to the requirements set forth in Section 5 below, provided that for Processing of Customer Account Data, Trimble is the Controller.

2.2 Customer's Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Trimble shall immediately inform the Customer if, in its opinion, an instruction infringes Data Protection Laws and Regulations or other statutory provisions.

2.3 Trimble's Processing of Personal Data. Trimble shall only Process Personal Data on behalf of and in accordance with Customer's instructions including with regard to transfers of Personal Data to a third country or an international organization. Customer instructs Trimble to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and applicable orders; (ii) Processing initiated by users in their use of the Services; (iii) Processing to comply with other reasonable instructions provided by Customer where such

instructions are consistent with the terms of the Agreement; and (iv) processing for the purpose of anonymization in compliance with the Data Use Clauses in the Agreement (and included in Schedule 1).

TRIMBLE DOES NOT ACT AS PROCESSOR FOR THE FOLLOWING PERSONAL DATA: User login and contact details, software usage data and data generated by security measures ("**Customer Account Data**)".

2.4 Scope and Purpose; Categories of Personal Data and Data Subjects. The subject-matter of Processing of Personal Data by Trimble is the performance of the Services pursuant to the Agreement. The types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Description of the Processing) to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 Data Subject Rights. Taking into account the nature of the Processing, Trimble assists Customer by providing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests of Data Subjects for exercising their Data Subject rights pursuant to the Data Protection Laws and Regulations. To the extent Customer, in its use of the Services, does not have the ability to exercise these rights herself, Trimble shall comply with any commercially reasonable request by Customer to facilitate such actions to the extent Trimble is legally permitted to do so. To the extent legally permitted, Customer shall be responsible for any costs arising from Trimble's provision of such assistance.

3.2 Direct Requests of Data Subject. Trimble shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for exercising their Data Subject rights pursuant to Section 3.1. Trimble shall not respond to any such Data Subject request without Customer's prior consent in text form except to confirm that the request relates to Customer to which Customer hereby agrees.

4. TRIMBLE AND CUSTOMER PERSONNEL

4.1 General. Trimble and Customer shall take steps to ensure that any natural person acting under their respective authority who has access to Customer Data does not process Customer Data except on instructions from the Customer, unless he or she is required to do so by Data Protection Laws and Regulations.

4.2 Confidentiality. Trimble shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality undertakings. Trimble shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.3 Reliability. Trimble shall take commercially reasonable steps to ensure the reliability of any Trimble personnel engaged in the Processing of Personal Data.

4.4 Limitation of Access. Trimble shall ensure that personnel access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Customer acknowledges and agrees that (i) Trimble's Affiliates may be retained as Sub-processors; and (ii) Trimble and Trimble's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. In such case, Trimble and Trimble's Affiliate shall impose on any Sub-processor materially similar data protection obligations as set out in this DPA by way of a contract or other legal act. The contract or other legal act shall contain sufficient guarantees that any Sub-processor implements appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the Data Protection Laws and Regulations.

5.2 List of Current Sub-processors and Notification of New Sub-processors. The current list of Sub-processors engaged in Processing Personal Data for the performance of each applicable Service, including a description of their processing activities and countries of location is listed under the https://www.trimble.com/Corporate/Privacy.aspx under "Additional Materials" ("Sub-processor Lists"). Customer hereby consents to these Sub-processors, their locations and processing activities as it pertains to their Personal Data, and instructs Trimble accordingly. Trimble will inform about changes to sub-processors in its release notes, customer updates or similar communications which shall be considered notice for purposes of Section [9.2 of the EU Standard Contractual Clauses].

5.3 Objection Right for New Sub-processors. In order to exercise its right to object to Trimble's use of a new Sub-processor, Customer shall notify Trimble promptly in text form sent to privacy@trimble.com within thirty (30) business days after receipt of Trimble's notice in accordance with the mechanism set out in Section 5.2. In the event Customer objects to a new Sub-processor, and that objection is not unreasonable, Trimble will use

reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If Trimble is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable order(s) and Agreements with respect only to those Services which cannot be provided by Trimble without the use of the objected-to new Sub-processor by providing written notice to Trimble. Trimble will refund Customer any prepaid fees covering the remainder of the term of such order(s) following the effective date of termination with respect to such terminated Services.

5.4 **Liability**. Trimble shall be liable for the acts and omissions of its Sub-processors to the same extent Trimble would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. SECURITY, AUDITS AND ASSISTANCE

6.1 **Security of Processing**. Trimble shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, including Personal Data, as set forth in Schedule 1. Trimble regularly monitors compliance with these safeguards. Trimble will not materially decrease the overall security of the Services during the term of the Agreement.

6.2 **Audits**. Trimble performs from time to time audits and inspections (including where reasonable audits by external auditors) to ensure compliance with Data Protection Laws and this DPA as well as where reasonable with industry standards such as ISO 27001.Trimble shall make upon request available to the Customer all information necessary (including such audit reports) to demonstrate compliance with its obligation from applicable Data Protection Law and this DPA. Depending on the information requested, Trimble may require the Customer to sign an NDA.

6.3 **Assistance to Customer.** Trimble shall assist Customer in ensuring compliance with the obligations regarding security of Processing, notification and communication of Personal Data breaches, data protection impact assessments and prior consultations with the supervisory authority pursuant to the Data Protection Laws and Regulations.

6.4 **Security Breach Management and Notification.** In case of a Personal Data breach pursuant to the Data Protection Laws and Regulations, Trimble maintains security incident management policies and procedures and shall, to the extent permitted by law, notify Customer of such breach without undue delay.

7. RETURN AND DELETION OF CUSTOMER DATA

Trimble shall after the end of the provision of Services at the choice of Customer return Customer Data to Customer and/or delete Customer Data in accordance with the procedures and timeframes specified in the Agreement or its Service description unless legislation imposed on Customer requires the storage of Customer Data.

8. GOVERNMENT ACCESS REQUESTS

8.1 Unless prohibited by applicable law, Trimble shall inform the Customer in general terms about requests, orders or similar demands by a court, competent authority, law enforcement or other government body ("Law Enforcement Request") relating to the processing of Personal Data under these Clauses.

8.2 Trimble will object to and challenge any Law Enforcement Request by taking legal remedies to the extent they are reasonable given the circumstances. If compelled to disclose Personal Data transferred under these Clauses by a Law Enforcement Request, Trimble will, unless prohibited by applicable law, give Customer reasonable notice to allow Customer to seek a protective order or other appropriate remedy unless Trimble is legally prohibited from doing so.

8.3 In case Trimble makes Personal Data available to Sub-processors, Trimble will select Sub-processors in a country outside of the European Economic Area that is not subject of an adequacy finding by the European Union Commission, only after a due diligence that entails (i) a review of any transparency reports made available by Sub-processor, (ii) and carrying out a transfer risk assessment.

9. AUTHORIZED AFFILIATES

9.1 **Contractual Relationship**. The Customer enters into the DPA on behalf of itself and, as may be the case, in the name and on behalf of Authorized Affiliates, thereby establishing a separate DPA between Trimble and each such Authorized Affiliate. Each Authorized Affiliate is bound by the obligations under this DPA. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, but is only a party to the DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions

of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

9.2 Communication. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Trimble under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

9.3 Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with Trimble, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA. If Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA as Controller, Authorized Affiliate hereby authorizes the Customer to exercise any such right in lieu of Authorized Affiliate. Moreover, the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together

10. LIMITATION OF LIABILITY

Each party's and its Affiliates' liability arising out of or related to this DPA and all DPAs between Authorized Affiliates and Trimble, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, Trimble's and its Affiliates' total liability for all claims from the Customer and its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under such Agreement, including by any Authorized Affiliate, and, in particular, shall not be understood to apply individually and severally to each Authorized Affiliate that is a contractual party to any such DPA. For further avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules and Appendices.

If Customer has subscribed to, or purchased the Services, through a reseller or other business partner of Trimble, Trimble's and its Affiliates' liability arising out of or related to this DPA and all DPAs between Authorized Affiliates and Trimble, whether in contract, tort or under any other theory of liability shall be limited, to the extent legally permissible, in aggregate to the higher of amounts received by Trimble for these Services or EUR 50,000.

11. INTERNATIONAL PROVISIONS

11.1 Cross Border Transfer Mechanism. To the extent Trimble processes Personal Data originating from and protected by Data Protection Laws and Regulations in one of the jurisdictions listed in Schedule 3 (Cross Border Transfer Mechanism) of this DPA, the terms specified in Schedule 3 with respect to the applicable jurisdiction(s) apply in addition to the terms of this DPA.

11.2 Cross Border Data Transfer Mechanisms. To the extent Customer's use of the Services requires an onward transfer mechanism to lawfully transfer Personal Data from one jurisdiction (i.e., the European Economic Area, the United Kingdom, Switzerland, Turkey or another jurisdiction listed in Schedule 3 (Cross Border Transfer Mechanism of this DPA) to Trimble located outside of that jurisdiction ("Transfer Mechanism"), the terms set forth in Schedule 4 (Cross Border Transfer Mechanisms) of this DPA will apply.

12. MISCELLANEOUS

12.1 Conflict. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms set forth in Schedule 4 (Cross Border Transfer Mechanism) of this DPA; (2) the terms of this DPA outside of Schedule 4 (Cross Border Transfer Mechanism); and (3) the Agreement.

12.2 Updates. Trimble may update the terms of this DPA from time to time; provided, however, Trimble will provide at least thirty (30) days prior written notice to Customer when an update is required as a result of (a) changes in Data Protection Laws and Regulations; (b) a merger, acquisition, or other similar transaction; or (c) the release of new products or services or material changes to any of the existing Services. The then-current terms of this DPA are available at trimble.com/privacy

Customer Legal Name:_____

Address

Trimble Customer Number:_____

☐ Customer has purchased the Services through Trimble's Authorized Reseller or Business Partner

Reseller Name

Address _____

Reseller Customer Number

☐ For EU/EEA/UK bill to customers. Customer wishes to enter into EU Standard Contractual Clauses directly with Trimble Inc. If this box is not checked the transfer mechanism for the transfer to Trimble Inc. is the one described in Section 2.2 of Schedule 4 or any other transfer mechanisms established between the Trimble Affiliate in Europe and Trimble Inc.

If the previous box is checked: Customer considers the following Modules as applicable:

☐ Module 1/Contract 1 ☐Module 2/Contract 2 ☐ Module 3/Contract 3

☐ Customer elects to execute this DPA
The parties' authorized signatories have duly executed this Agreement:

CUSTOMER (hereby signs this DPA)

Name:

Title

Date:

Trimble Inc.

Signature:_____
Print Name: Jennifer Allison
Title: Senior Vice President and General Counsel
Date: 15.7.2024

Trimble Europe BV

Signature:_____
Print Name: RHH Reeder
Title: Director
Date: 15.7.2024

Trimble UK Limited

Signature:_____
Print Name: RHH Reeder
Title: Director
Date: 15.7.2024

Trimble France SAS

Signature:_____
Print Name: RHH Reeder
Title: Director
Date: 15.7.2024

Trimble Solutions Sandvika AS

Signature:_____
Print Name: RHH Reeder
Title: Director
Date: 15.7.2024

Trimble Technologies Ireland Limited

Signature:_____
Print Name: RHH Reeder
Title: Director
Date: 15.7.2024

Lakefield eTechnologies Limited

Signature:_____
Print Name: RHH Reeder
Title: Director
Date: 15.7.2024

Trimble International BV

Signature:_____
Print Name: RHH Reeder
Title: Director
Date: 15.7.2024

Trimble Finland Corporation

Signature:_____
Print Name: Jürgen Kesper
Title: Director
Date: 15.7.2024

Trimble Germany GmbH

Signature:_____
Print Name: RHH Reeder
Title: Director
Date: 15.7.2024

Trimble MAPS Limited.

Signature:_____
Print Name: RHH Reeder
Title: Director
Date:15.7.2024

Trimble Forestry Europe Corporation

Signature:_____
Print Name: RHH Reeder
Title: Director
Date: 15.7.2024

Trimble GmbH

Signature:_____
Print Name: Jürgen Kesper
Title: Director
Date: 15.7.2024

Contact Details for all Trimble entities:

privacy@trimble.com

Addresses Trimble Entities	
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, France
Trimble Solutions Sandvika AS	**Trimble Technologies Ireland Limited**
Leif Tronstads plass 4 1337 Sandvika, Norway	North Point Business Park, Unit 3d North Point House, New Mallow Rd, Cork, T23 AT2P, Ireland
Lakefield eTechnologies Limited	**Trimble International BV**
North Point Business Park, Unit 3d North Point House, New Mallow Rd, Cork, T23 AT2P, Ireland	Industrieweg 187a 5683CC Best, the Netherlands
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 England WC2A 1QS UK	Hatsinanpuisto 8, 02600 Espoo, Finland
Trimble GmbH	
Am Prime Parc 11, 65479 Raunheim	

SCHEDULE 1 - DESCRIPTION OF PROCESSING

1. CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

- Employees, officers, directors and contractors of Customer
- Customer's customers (who are natural persons), often in their capacity as recipients of shipments, services and products
- Employees, agents, advisors, freelancers of Customer's customers, vendors and counterparties of transactions processed through the Services
- Customer's users authorized by Customer to use the Services

2. CATEGORIES OF PERSONAL DATA TRANSFERRED

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:
- Contact and Master Data (First and last name, Title, Position)
- Contact information (company, email, phone, physical business address)
- ID data such as passports, driver licenses, IP addresses, Unique identifiers (UUID)
- Occupational and educational data (qualifications, experiences, skills)
- Job related data (services rendered, project contributions, assigned jobs and tasks, performance related data, hours of service, expenses)
- Localisation data
- Contract related data (billing, payment, transaction history)
- History of Interactions

3. SENSITIVE DATA TRANSFERRED (IF APPLICABLE)

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:
Data exporter may submit special categories of data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
The applicable security measures are described in Section 11 of Schedule 2 of Schedule 2 below.

4. FREQUENCY OF THE TRANSFER

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Continuous basis depending on the use of the Services by Customer.

5. NATURE OF THE PROCESSING

The nature of the Processing is the performance of the Services pursuant to the Agreement.

6. PURPOSE OF PROCESSING, THE DATA TRANSFER AND FURTHER PROCESSING

Trimble will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Services. Trimble will further anonymize Personal Data in order to conduct data analytics and service development.

7. DURATION OF PROCESSING

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:

Trimble will Process Personal Data as set forth in the Agreement, unless otherwise agreed, for example in Section 9 of the DPA.

8. SUB-PROCESSOR TRANSFERS

For transfers to (Sub-) Processors, also specify subject matter, nature and duration of the Processing:

Sub-processor will Process Personal Data as necessary to perform the Services pursuant to the Agreement. Subject to Section 9 of this DPA, the Sub-processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

Identities of the Sub-processors used for the provision of the Services and their country of location are listed under the Additional Materials Tab in the trimble.com/privacy.

SCHEDULE 2 - Technical and Organizational Security Measures

Where applicable, this Schedule 2 will serve also as Annex II to the EU Standard Contractual Clauses.

Technical and Organizational Security Measure

1. Measures of pseudonymisation and encryption of personal data

Where possible, Trimble encrypts Data transmitted between customers and the Trimble application over public networks using TLS 1.2 or higher. Customer Data stored on Trimble managed systems (for AICPA certified products - see item 7 below for more information) is encrypted using AES 256 or stronger ciphers.

2. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Trimble has dedicated Cybersecurity personnel responsible for oversight of security and privacy. It has appointed Cybersecurity and Privacy leadership in addition to an Office of Data Protection, together with an Engineering Leadership Council which meets quarterly to discuss privacy and security risks managed within Sector product portfolios. In addition, product risk is tracked in an internal portal with compliance monitoring performed monthly.

3. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

In order to support availability of Trimble SaaS products, Trimble leverages industry leading cloud service providers (Amazon Web Services (AWS) and Microsoft Azure) for auto-scaling, geographically diverse data centers, extensive application and infrastructure monitoring, and 24x7 support mechanisms.
Trimble maintains backups of data stores, including Customer Data, that support the primary functionalities of the Trimble applications. Backups are stored in a location geographically-separated from the primary data storage location where possible.
In addition to the measures of our service providers, Trimble maintains a security incident response function that includes a documented Incident Response Policy and plan to triage security events and incidents involving Customer Data. This defines response protocol such as containment, eradication, restoration and communication activities for security incidents, as well as roles and responsibilities of Trimble personnel and a requirement for post-incident reviews with Trimble Management.

4. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Trimble employs independent third parties to conduct periodic penetration testing, including Sarbanes-Oxley, PCI, SOC 1, Type II, SOC 2 Type II, ISO27001 or NIST 800-171 equivalent audits on an annual basis where required for regulatory compliance. In addition, Trimble conducts regular internal vulnerability testing and penetration testing on applicable products and platforms in conjunction with Trimble's Cybersecurity program and policy requirements. Trimble may perform assessments of new vendors or partners if the business risk warrants review. Trimble encourages 3rd parties to report any cybersecurity issues, incidents and vulnerabilities associated with our products, services or websites.

5. Measures for user identification and authorisation

For products leveraging Trimble ID (TID, Trimble Identity) for authentication, Trimble processes the password securely. In addition, some Trimble products may support Single Sign On (SSO) integration with a customer identity provider using Security Assertion Markup Language (SAML) and Multifactor Authentication (MFA).

6. Measures for the protection of data during transmission

As per item 1, Trimble encrypts Customer Data transmitted over public networks between customers and the Trimble application using current encryption ciphers whenever possible.

7. Measures for the protection of data during storage

As per item 1, Customer Data stored on Trimble managed data storage is encrypted using AES 256 or stronger for any Trimble products currently AICPA SOC 1, Type II, SOC 2, Type II or NIST 800-171 certified. Refer to Item 11 for more detailed information.

8. Measures for ensuring physical security of locations at which personal data are processed

Trimble SaaS products, applications and services are typically hosted with Customer Data stored within data centers provided by Amazon Web Services (AWS), Microsoft Azure or Google Cloud Platform (GCP). As such, Trimble relies on the physical, environmental and infrastructure controls of these platforms. Trimble periodically reviews certifications and third-party attestations provided by these providers relating to the effectiveness of their data center controls.

9. Measures for ensuring events logging

Trimble maintains many cybersecurity tooling logs and application and infrastructure security audit logs. Security logs are analyzed using SIEM technology in combination with event correlation to detect anomalous activity.

10. Measures for ensuring system configuration, including default configuration

Trimble leverages common industry standards to strengthen cybersecurity through secure configuration and defense in depth. Trimble applies security patches to its systems in accordance with the Trimble Secure Development Lifecycle Policy (TSDLCP).

11. Measures for internal IT and IT security governance and management

For SOC 1, Type II, SOC 2, Type II or NIST 800-171 Trimble certified products, personnel with access to Customer Data leverage role-based and least privilege principles for access control. Staff are only provided with sufficient access to Customer Data to be able to carry out their job duties securely. Remote network access to Trimble systems requires encrypted communication via secured protocols and use of multi-factor authentication. Trimble has established and will maintain procedures for password management for this personnel demographic, designed to ensure passwords are unique to each individual, and inaccessible to unauthorized persons, including at minimum:

- cryptographically protecting passwords when stored in computer systems or in transit over any public network;
- altering default passwords from vendors; and
- education on good password practices such as using passphrases
- staff access to production infrastructure requires multi-factor authentication (MFA).

For ISO 27001 certificate compliance and to ensure proper and effective use of cryptography to protect the confidentiality and integrity of data owned or managed by Trimble In-Scope Divisions, data classified as Confidential or Restricted must be encrypted by the use of valid encryption processes for data at rest and in motion as required by regulation and/or Risk Assessment. This includes but is not limited to sensitive information stored on mobile devices, removable drives and laptop computers. Trimble In-Scope Divisions will employ only unmodified, commercial cryptography applications to encrypt data at rest and/or in-transit.

Trimble staff are subject to confidentiality obligations and various policies, such as Acceptable Use, Data Classification, Secure Destruction and MFA. Trimble requires its staff to undergo information security awareness training, both at the commencement of their employment and then annually thereafter. Trimble also requires its staff to undergo privacy training annually (including to comply with GDPR).

For applicable products, Trimble has implemented security and privacy by design principles, including but not limited to, threat modeling and product application penetration tests.

12. Measures for certification/assurance of processes and products

Trimble will maintain SOC 2, Type II, ISO 27001 or NIST 800-171 certifications, undergoing periodic external surveillance and recertification audits to ensure that its Information Security Management System (ISMS) meets the requirements of this standard for applicable products.

Trimble will maintain information security policies that meet the requirements of the ISO 27001 standard, an internal audit program that assesses Trimble's ISMS and information security controls, and a management committee that is responsible for oversight of Trimble's Information Security Management System (ISMS).

13. Measures for ensuring data minimization

Trimble may allow visitors to use certain functionalities of some products anonymously and minimizes the Data it requires from Customers to only what is necessary to provide the service requested under localized laws and regulations.

14. Measures for ensuring data quality

Trimble ensures the quality of its data through various verification mechanisms unique to applicable Trimble products. Trimble may also allow product users to update the information in their accounts themselves or via requests to its customer support functions.

15. Measures for ensuring limited data retention

Trimble can implement the Data Retention Policy of the Customer setting out the retention periods for various types of data.

16. Measures for allowing data portability and ensuring erasure

Applicable Trimble products have a process for deleting Customer Data within 30 days of receiving customer verified written requests and may enable the download of Customer Data to provide to alternative service providers as required by GDPR.

17. Third Party (Sub-processor) Control and Management

Trimble only employs Sub-processors that process Personal Data on Trimble's behalf as part of applicable subscription services in compliance with Data Protection Laws and Regulations. Trimble also verifies before choosing a Sub-processor and transferring any data the Sub-processor's technical and organizational measures to ensure a level of security appropriate to the risk of its customers data Processing. Trimble also takes reasonable measures to ensure security of the transfers of Customer Data to third party Sub-processors. At a minimum, such measures include identifying the risks to Customer and Data Subject rights based upon nature, scope and context of Processing; reviewing the security and data protection controls implemented by the Sub-processor to protect Customer Data (including SOC 2 Type II audit reports and/or ISO 27001 certificates as applicable); imposing data protection contractual terms that protect Personal Data to the same or similar standard Trimble is obligated to provide its customers (including valid cross border transfer mechanisms, Sub-processor management, and compliance programs); requiring the Sub-processor to only process Customer Data on behalf of Trimble and its customers and, limiting its Processing of Customer Data to the scope of Trimble's instructions.

SCHEDULE 3 – Cross Border Transfer Mechanism

1. European Economic Area (EEA):

1.1 The definition of "Data Protection Laws and Regulations" includes the General Data Protection Regulation (EU 2016/679) ("***GDPR***").

1.2 When Trimble engages a Sub-processor under Section 5.1 (Appointment of Sub-processors) of this DPA, it will:

(a) require any appointed Sub-processor to protect the Customer Data to the standard required by Data Protection Laws and Regulations and imposes the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the GDPR, and

(b) require any appointed Sub-processor to (i) agree in writing to only process Personal Data in a country that the European Union has declared to have an "adequate" level of protection or (ii) only process Personal Data on the basis of the EU Standard Contractual Clauses or pursuant to Binding Corporate Rules approved by competent European Union data protection authorities.

1.3 Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under

Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

1.4 Customer acknowledges that Trimble, as a Controller, may be required under Data Protection Laws and Regulations to notify a regulatory authority of Security Incidents involving Customer Usage Data. If a regulatory authority requires Trimble to notify impacted Data Subjects with whom Trimble does not have a direct relationship (e.g., Customer's end users), Trimble will notify Customer of this requirement. Customer will provide reasonable assistance to Trimble to notify the impacted Data Subjects.

2. United Kingdom (UK):

2.1 References in this DPA to "GDPR" will be deemed references to the corresponding laws and regulations of the United Kingdom, including, without limitation, the UK GDPR and Data Protection Act 2018.

2.2 When Trimble engages a Sub-processor under Section 5.1 (Appointment of Sub-processors) of this DPA, it will:

(a) require any appointed Sub-processor to protect the Customer Data to the standard required by Data Protection Laws and Regulations, such as including the same data protection obligations referred to in Article 28(3) of the UK GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the UK GDPR, and

(b) require any appointed Sub-processor to (i) agree in writing to only process Personal Data in a country that the United Kingdom has declared to have an "adequate" level of protection or (ii) only process Personal Data on terms equivalent to the UK International Data Transfer Agreement or the EU Standard Contractual Clauses and the UK International Data Transfer Addendum or pursuant to Binding Corporate Rules approved by competent United Kingdom data protection authorities.

2.3 Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any UK GDPR fines issued or levied under Article 83 of the UK GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the UK GDPR.

2.4 Customer acknowledges that Trimble, as a Controller, may be required under Data Protection Laws and Regulations to notify a regulatory authority of Security Incidents involving Customer Usage Data. If a regulatory authority requires Trimble to notify impacted Data Subjects with whom Trimble does not have a direct relationship (e.g., Customer's end users), Trimble will notify Customer of this requirement. Customer will provide reasonable assistance to Trimble to notify the impacted Data Subjects.

3. Switzerland:

3.1 The definition of "Data Protection Laws and Regulations" includes the Swiss Federal Act on Data Protection, as revised ("***FADP***").

3.2 When Trimble engages a Sub-processor under Section 5.1 (Appointment of Sub-processors) of this DPA, it will:

(a) require any appointed Sub-processor to protect the Customer Data to the standard required by Data Protection Laws and Regulations in particular, providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the FADP, and

(b) require any appointed Sub-processor to (i) agree in writing to only process Personal Data in a country that Switzerland has declared to have an "adequate" level of protection or (ii) only process Personal Data on terms equivalent to the EU Standard Contractual Clauses including the amendments named in Section 3.3 or pursuant to Binding Corporate Rules approved by competent European Union or Swiss data protection authorities.

3.3 To the extent that Personal Data transfers from Switzerland are subject to the EU Standard Contractual Clauses in accordance with Section 2.3 of Schedule 3 (EU Standard Contractual Clauses), the parties agree that all amendments shall be made to the EU Standard Contractual Clauses that are deemed as necessary by the Swiss Federal Data Protection and Information Commissioner. Specifically, these are at the time of conclusion of the DPA:

(a) references to "EU Member State" and "Member State" will be interpreted to include Switzerland, and

(b) insofar as the transfer or onward transfers are subject to the FADP:

(i) references to "Regulation (EU) 2016/679" are to be interpreted as references to the FADP;

(ii) the "competent supervisory authority" in Annex I, Part C will be the Swiss Federal Data Protection and Information Commissioner;

(iii) in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by the laws of Switzerland; and

(iv) in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Switzerland.

(v) Clause 18(c) of the EU Standard Contractual Clauses applies whereas a Data Subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland where the Data Subject has their habitual residence.

4. United States of America:

4.1 "***US State Privacy Laws***" means all state laws relating to the protection and Processing of Personal Data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("***CCPA***"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act.

4.2 The definition of "Data Protection Laws and Regulations" includes US State Privacy Laws.

4.3 The following terms apply where Trimble processes Personal Data subject to the CCPA:

(a) The term "***personal information***", as used in this Section 4.3, will have the meaning provided in the CCPA;

(b) Trimble is a service provider when Processing Customer Data. Trimble will process any personal information contained in Customer Data only for the business purposes set forth in the Agreement, including the purpose of Processing and processing activities set forth in this DPA ("***Purpose***"). As a service provider, Trimble will not sell or share Customer Data or retain, use, or disclose Customer Data (i) for any purpose other than the Purpose, including retaining, using, or disclosing Customer Data for a commercial purpose other than the Purpose, or as otherwise permitted by the CCPA; or (ii) outside of the direct business relationship between Customer and Trimble;

(c) Trimble will (i) comply with obligations applicable to it as a service provider under the CCPA and (ii) provide personal information with the same level of privacy protection as is required by the CCPA. Customer is responsible for ensuring that it has complied, and will continue to comply, with the requirements of the CCPA in its use of the Services and its own Processing of personal information;

(d) Customer will have the right to take reasonable and appropriate steps to help ensure that Trimble uses personal information in a manner consistent with Customer's obligations under the CCPA;

(e) Trimble will notify Customer if it makes a determination that it can no longer meet its obligations as a service provider under the CCPA;

(f) Upon notice, Customer will have the right to take reasonable and appropriate steps in accordance with the Agreement to stop and remediate unauthorized use of personal information;

(g) Trimble will provide reasonable additional and timely assistance to assist Customer in complying with its obligations with respect to consumer requests as set forth in the Agreement;

(h) For any Sub-processor used by Trimble to process personal information subject to the CCPA, Trimble will ensure that Trimble's agreement with such Sub-processor complies with the CCPA, including, without limitation, the contractual requirements for service providers and contractors;

(i) Trimble will not combine Customer Data that it receives from, or on behalf of, Customer, with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, unless such combination is required to perform any business purpose as permitted by the CCPA, including any regulations thereto, or by regulations adopted by the California Privacy Protection Agency; and

(j) Trimble certifies that it understands and will comply with its obligations under the CCPA.

4.4 Trimble acknowledges and confirms that it does not receive Customer Data as consideration for any Services provided to Customer.

5. Australia:

5.1 The definition of "Data Protection Laws and Regulations" includes the Australian Privacy Principles and the Australian Privacy Act (1988).

5.2 The definition of "Personal Data" includes "Personal Information" as defined under Data Protection Laws and Regulations.

5.3 The definition of "Sensitive Data" includes "Sensitive Information" as defined under Data Protection Laws and Regulations.

6. Brazil:

6.1 The definition of "Data Protection Laws and Regulations" includes the Lei Geral de Proteção de Dados (General Personal Data Protection Act).

6.2 The definition of "Security Incident" includes a security incident that may result in any relevant risk or damage to Data Subjects.

6.3 The definition of "Processor" includes "operator" as defined under Data Protection Laws and Regulations.

7. Canada:

7.1 The definition of "Data Protection Laws and Regulations" includes the Federal Personal Information Protection and Electronic Documents Act.

7.2 Trimble's Sub-processors, as set forth in Section 5 (Sub-processors) of this DPA, are third parties under Data Protection Laws and Regulations, with whom Trimble has entered into a written contract that includes terms substantially similar to this DPA. Trimble has conducted appropriate due diligence on its Sub-processors.

7.3 Trimble will implement technical and organizational measures as set forth in Section 11 of Schedule 2 of Schedule 2 (Security) of this DPA.

8. Israel:

8.1 The definition of "Data Protection Laws and Regulations" includes the Protection of Privacy Law.

8.2 The definition of "Controller" includes "Database Owner" as defined under Data Protection Laws and Regulations.

8.3 The definition of "Processor" includes "Holder" as defined under Data Protection Laws and Regulations.

8.4 Trimble will require that any personnel authorized to process Customer Data comply with the principle of data secrecy and have been duly instructed about Data Protection Laws and Regulations. Such personnel sign confidentiality agreements with Trimble in accordance with Section 6 (Confidentiality) of this DPA.

8.5 Trimble must take sufficient steps to ensure the privacy of Data Subjects by implementing and maintaining the security measures as specified in Section 11 of Schedule 2 (Security) of this DPA and complying with the terms of the Agreement.

8.6 Trimble must ensure that the Personal Data will not be transferred to a Sub-processor unless such Sub-processor has executed an agreement with Trimble pursuant to Section 5.1 (Appointment of Sub-processors) of this DPA.

9. Japan:

9.1 The definition of "Data Protection Laws and Regulations" includes the Act on the Protection of Personal Information ("***APPI***").

9.2 The definition of "Personal Data" includes information about a specific individual applicable under Section 2(1) of the APPI, which Customer entrusts to Trimble during Trimble's provision of the Services to Customer.

9.3 Trimble agrees it has and will maintain a privacy program conforming to the standards prescribed by rules of the Personal Information Protection Commission concerning the handling of Personal Data pursuant to the provisions of Chapter 4 of the APPI. Accordingly:

(a) Trimble will (i) process Personal Data as necessary to provide the Services to Customer in accordance with the Agreement and as set forth in Schedule 1 (Description of the Processing) of this DPA ("*Purpose of the processing*") and (ii) not process Personal Data for any purpose other than the Purpose of the processing without Customer's consent;

(b) Trimble will implement and maintain measures appropriate and necessary to prevent unauthorized disclosure and loss of Personal Data and for the secure management of Personal Data in accordance with the APPI as set forth in Schedule 2 (Technical and Organizational Measures) of this DPA;

(c) Trimble will notify Customer for (i) a failure to comply with Section 9.3(a) of this Schedule 3 or (ii) Trimble's discovery of a Security Incident impacting Customer Data, in either case, in accordance with Section 6.4 of this DPA. Trimble will provide reasonable assistance to Customer in the event that Customer is required to notify a regulatory authority or any Data Subjects impacted by a Security Incident;

(d) Trimble will ensure that any of its employees who have access to Personal Data (i) have executed employee agreements requiring them to keep such Personal Data confidential and (ii) who violate confidentiality will be subject to disciplinary action and possible termination; (iii) carry out appropriate employee supervision and training for the secure management of Personal Data; and (iv) limit the number of authorized personnel, including Trimble's employees, who have access to Personal Data and control such access such that it is only permitted for the time period necessary for the Purpose of the processing;

(e) Trimble will not disclose Personal Data to any third party, except as Customer has authorized Trimble to do so in the Agreement. When engaging Sub-processors, Trimble will comply with the obligations in Section 9 (Sub-processors) of this DPA to ensure that procedures are in place to maintain the confidentiality and security of Personal Data;

(f) Trimble will keep records of the handling of Personal Data entrusted to it by, and performed for, Customer;

(g) Customer may assess Trimble's compliance with its obligations under Data Protection Laws and Regulations and as set forth in Section 6 of this DPA.

(h) Trimble will provide reasonable cooperation to Customer upon written request, where Customer is reporting to the Personal Information Protection Commission or other regulatory authorities; and

(i) Trimble's primary processing facilities are located in the United States of America, and, depending on Customer's use of the Services, from the locations set forth under the https://www.trimble.com/Corporate/Privacy.aspx under "Additional Materials" ("Sub-processor Lists"). Trimble will notify customer of any change and provide Customer the opportunity to object in accordance with Section 9 of this DPA. Where Trimble processes Personal Data in a country other than Japan, Trimble will ensure it complies with its privacy program as described in this DPA.

9.4 The following Data Subject consent terms apply:

(a) Customer entrusts Trimble with Personal Data for the Purpose of the processing. Customer agrees that Trimble is not a "third party" as the term is used in the APPI provisions that restrict the provision of Personal Data to third parties. As such, the requirement to obtain Data Subject consent in advance do not apply;

(b) if Data Subject consent is required under Article 4 of the Telecommunications Business Act, Customer will comply with any consent requirements specific to its use of the Services.

10. Mexico:

10.1 The definition of "Data Protection Laws and Regulations" includes the Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations.

10.2 When acting as a Processor, Trimble will:

(a) treat Personal Data in accordance with Customer's instructions set forth in Section 5 of this DPA;

(b) process Personal Data only to the extent necessary to provide the Services;

(c) implement security measures in accordance with Data Protection Laws and Regulations and Schedule 2 (Technical and Organizational Measures) of this DPA;

(d) keep confidentiality regarding the Personal Data processed in accordance with the Agreement;

(e) delete all Personal Data upon termination of the Agreement in accordance with Section 10 (Return or Deletion of Customer Data) of this DPA; and

(f) only transfer Personal Data to Sub-processors in accordance with Section 9 (Sub-processors) of this DPA.

11. Singapore:

11.1 The definition of "Data Protection Laws and Regulations" includes the Personal Data Protection Act 2012 ("***PDPA***").

11.2 Trimble will process Personal Data to a standard of protection in accordance with the PDPA by implementing adequate technical and organizational measures as set forth in Schedule 2 (Technical and Organizational Measures) of this DPA and complying with the terms of the Agreement.

12. Republic of Türkiye

12.1 The definition of "Data Protection Laws and Regulations" includes (i) the Law on the Protection of Personal Data ("PDPL), Law Number 6698, from March 24 2016 as amended by the Law on the Construction of Amendments to the Code of Criminal Procedure and other Laws, Law Number 7499, from March 2 2024 and (ii) the Regulation on Principles regarding Procedures and Rules for Transferring Personal Data Abroad from the Personal Data Protection Authority as published in the Official Gazette July 10, Number 32598.

12.2 Customer acknowledges that Trimble, as a Controller, may be required under Data Protection Laws and Regulations to notify a regulatory authority of Security Incidents involving Customer Usage Data. If a regulatory authority requires Trimble to notify impacted Data Subjects with whom Trimble does not have a direct relationship (e.g., Customer's end users), Trimble will notify Customer of this requirement. Customer will provide reasonable assistance to Trimble to notify the impacted Data Subjects.

SCHEDULE 4 - CROSS BORDER TRANSFER MECHANISM
(Applies to Data transferred from the EU, EEA, UK and Switzerland)

1. Definitions

- ***"EU Standard Contractual Clauses"*** means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.
- ***"UK International Data Transfer Agreement"*** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.
- ***"Data Privacy Framework"*** means the EU-US and/or Swiss-US Data Privacy Framework self-certification program operated by the US Department of Commerce.
- ***"Data Privacy Principles"*** means the Data Privacy Framework principles (as supplemented by the Supplemental Principles).
- ***"Turkish Standard Contractual Clauses"*** means the Standard Contract to be used in the Transfer of Personal Data Abroad 1 – 4 as accepted by the decision 2024/959 from June 4 2024 by the Turkish Personal Data Protection Authority.

2. Cross Border Data Transfer Mechanisms

2.1 Order of Precedence. In the event the Services are covered by more than one Transfer Mechanism, the transfer of Personal Data will be subject to a single Transfer Mechanism, as applicable, and in accordance with the following order of precedence: (a) the Data Privacy Framework as referenced in Section 2.2 (Data Privacy Framework) of this Schedule; (b) the EU Standard Contractual Clauses as referenced in Section 2.3 (EU Standard Contractual Clauses) of this Schedule; (c) the UK International Data Transfer Addendum as referenced in Section 2.4 (UK International Data Transfer Addendum) of this Schedule; and, if neither (a), (b), (c), (d) nor (e) is applicable, then (f) other applicable data Transfer Mechanisms permitted under Data Protection Laws and Regulations.

2.2 Data Privacy Framework. To the extent Trimble Inc. processes any Personal Data via the Services originating from the EEA or Switzerland, Trimble Inc. is self-certified under the Data Privacy Framework and complies with the Data Privacy Principles when Processing any such Personal Data. To the extent that Customer is (a) located in the United States of America and is also self-certified under the Data Privacy Framework or (b) located in the EEA or Switzerland, Trimble further agrees (i) to provide at least the same level of protection to any Personal Data as required by the Data Privacy Principles; (ii) to notify Customer in writing, without undue delay, if its self-certification to the Data Privacy Framework is withdrawn, terminated, revoked, or otherwise invalidated (in which case, an alternative Transfer Mechanism will apply in accordance with the order of precedence in Section 2.1 (Order of Precedence) of this Schedule 4; and (iii) upon written notice, to work with Customer to take reasonable and appropriate steps to stop and remediate any unauthorized Processing of Personal Data.

2.3 EU Standard Contractual Clauses. The EU Standard Contractual Clauses will apply to Personal Data that is transferred via the Services from the EEA, Switzerland, or UK either directly or via onward transfer, to any country or recipient outside the EEA, Switzerland or UK that is not recognized by the relevant competent authority as providing an adequate level of protection for Personal Data. For data transfers that are subject to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will be deemed entered into, and incorporated into this DPA by this reference, and completed as follows:

(a) Module One (Controller to Controller) of the EU Standard Contractual Clauses will apply where (i) Trimble is Processing Customer Account Data and (ii) Customer is a Controller of Customer Usage Data and Trimble is Processing Customer Usage Data;

(b) Module Two (Controller to Processor) of the EU Standard Contractual Clauses will apply where Customer is a Controller of the Personal Data and Trimble is Processing Personal Data on Customer's behalf; and

(c) Module Three (Processor to Processor) of the EU Standard Contractual Clauses will apply where Customer is a Processor of Personal Data and Trimble is Processing as Sub-processor on Customer's behalf.

(d) For each Module, where applicable:

(i) in Clause 7 of the EU Standard Contractual Clauses, the optional docking clause shall not apply;

(ii) in Clause 9 of the EU Standard Contractual Clauses, Option 2 will apply and the time period for prior written notice of Sub-processor changes will be as set forth in Section 5.2 (List of Current Sub-processors and Notification of New Sub-processors) of this DPA;

(iii) in Clause 11 of the EU Standard Contractual Clauses, the optional language will not apply;

(iv) Identify the competent supervisory authority/ies in accordance with clause 13;

(v) in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by Dutch law;

(vi) in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Amsterdam, the Netherlands;

(vii) in Annex I, Part A of the EU Standard Contractual Clauses:

Data Exporter: Customer (if the box on page 6 is checked).

Contact details: The email address(es) designated by Customer in Customer's account via its notification preferences.

Data Exporter Role: The Data Exporter's role is set forth on page 6.

Signature and Date: By entering into the Agreement, Data Exporter is deemed to have signed these EU Standard Contractual Clauses incorporated herein, including their Annexes, as of the effective date of the Agreement.

Data Importer: Trimble Inc.

Contact details: Trimble Privacy Team - privacy@Trimble.com

Data Importer Role: The Data Importer's role is set forth on page 6

Signature and Date: By entering into the Agreement, Data Importer is deemed to have signed these EU Standard Contractual Clauses, incorporated herein, including their Annexes, as of the effective date of the Agreement;

(viii) in Annex I, Part B of the EU Standard Contractual Clauses:

The categories of Data Subjects are set forth in Section 1 of Schedule 1 (Description of Processing) of this DPA.

The Sensitive Data transferred is set forth in Section 3 of Schedule 1 (Description of Processing) of this DPA.

The frequency of the transfer is a continuous basis for the duration of the Agreement.

The nature of the Processing is set forth in Section 5 of Schedule 1 (Description of Processing) of this DPA.

The purpose of the Processing is set forth in Section 6 of Schedule 1 (Description of Processing) of this DPA.

The period for which the Personal Data will be retained is set forth in Section 7 of Schedule 1 (Description of Processing) of this DPA.

For transfers to Sub-processors, the subject matter, nature, and duration of the Processing is set forth at https://www.trimble.com/Corporate/Privacy.aspx under "Additional Materials" ("Sub-processor Lists").

(ix) in Annex I, Part C of the EU Standard Contractual Clauses: Where applicable the Dutch Data Protection Commission shall be the lead supervisory authority. Otherwise, where a Trimble entity residing in the EU is the Data Exporter, the competent supervisory authority is the supervisory authority of the member state the Trimble entity resides in. Where the Customer is the Data Exporter the competent supervisory authority is the supervisory authority of the member state the Customer resides in.

(x) Schedule 2 (Technical and Organizational Security Measures) of this DPA serves as Annex II of the EU Standard Contractual Clauses.

2.4 UK Extension to the Data Privacy Framework and International Data Transfer Addendum. Customer and Trimble agree that the UK Extension to the Data Privacy Framework will apply, and in absence of such, the EU Standard Contractual Clauses and the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses in its most recent version will apply to Personal Data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for Personal Data. For data transfers from the United Kingdom that are subject to the EU Standard Contractual Clauses and the UK International Data Transfer Addendum, the EU Standard Contractual Clauses will be deemed entered into, and incorporated into this DPA as described in Section 2.3 of this Section 4 and the UK International Data Transfer Addendum will be deemed entered into, and incorporated into this DPA by this reference, and completed as follows:

(a) In Table 1 of the UK International Data Transfer Addendum, Customer's and Trimble's details and key contact information are set forth in Section 2.3 (e)(vii) of this Schedule 3;

(b) In Table 2 of the UK International Data Transfer Addendum, information about the version of the EU Standard Contractual Clauses, and selected clauses, which the UK International Data Transfer Addendum is appended to, are set forth in Section 2.3 (EU Standard Contractual Clauses) of this Schedule 4;

(c) In Table 3 of the UK International Data Transfer Addendum:

(i) The list of Parties is set forth in Section 2.3(e)(vii) of this Schedule 3.

(ii) The description of the transfer is set forth in Section 1 (Nature and Purpose of the Processing) of Schedule 1 (Description of the Processing).

(iii) Annex II is located in Schedule 2 (Technical and Organizational Security Measures) of this DPA.

(iv) The list of Sub-processors is set forth at https://www.trimble.com/Corporate/Privacy.aspx under “Additional Materials” (“Sub-processor Lists”).; and

(d) In Table 4 of the UK International Data Transfer Addendum, both the Importer and the Exporter may end the UK International Data Transfer Agreement in accordance with the terms of the UK International Data Transfer Addendum.

2.5 Turkish Standard Contractual Clauses. The Turkish Standard Contractual Clauses will apply to Personal Data that is transferred via the Services from Turkey either directly or via onward transfer, to any country or recipient outside Turkey that is not recognized by the competent authority as providing an adequate level of protection for Personal Data. For data transfers that are subject to the Turkish Standard Contractual Clauses, the Turkish Standard Contractual Clauses will be deemed entered into, and incorporated into this DPA by this reference, and completed as follows:

For each Module, where applicable:

(i) in Article 8 of Contract 2 and Contract 3 of the Turkish Standard Contractual Clauses, Option 2 will apply and the time period for prior written notice of Sub-processor changes will be as set forth in Section 5.2 (List of Current Sub-processors and Notification of New Sub-processors) of this DPA;

(ii) The parties agree that the Customer shall notify the competent Turkish Personal Data Protection Authority within five (5) business days to inform about the conclusion of the Turkish Standard Contractual Clauses.

(iii) The Data Importer shall be: Trimble with Addresses, Name and Surname, Title and Contact Information of Trimble and Signatory as stated in the DPA.

(iv) Signature and Date: By entering into the Agreement, Trimble and Data Exporter are deemed to have signed these Turkish Standard Contractual Clauses incorporated herein, including their Appendices, as of the effective date of the Agreement.

(v) The information for in Annex I of the Turkish Standard Contractual Clauses is set forth in Schedule 1:

(vi) Schedule 2 (Technical and Organizational Security Measures) of this DPA serves as Annex II of the Turkish Standard Contractual Clauses.

(vii) The list of Sub-processors is set forth at https://www.trimble.com/Corporate/Privacy.aspx under “Additional Materials” (“Sub-processor Lists”).

2.6 Conflict. To the extent there is any conflict or inconsistency between the EU Standard Contractual Clauses, UK International Data Transfer Agreement or the Turkish Standard Contractual Clauses and any other terms in this DPA, including Schedule 4 (Cross Border Transfer Mechanism), the Agreement, the provisions of the EU Standard Contractual Clauses, UK International Data Transfer Addendum and Turkish Standard Contractual Clauses, as applicable, will prevail.