DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is the parties' agreement with regard to the Processing of Personal Data and is entered into to apply together with all agreements in the course of which Trimble Inc or it Affiliates process Personal Data on behalf of the Customer and its Authorized Affiliates, such as License, Subscription, Services, Support and Maintenance or any other written agreement or agreement in text form (the "**Agreements**") for purchase from Trimble of software as a service (including associated Trimble offline or mobile applications), hosting, support and similar data processing services, and defined as "Services" or otherwise in the Agreement(s) or hereinafter.

Entering into this DPA is offered by Trimble to Customers and their Authorized Affiliates that qualify as controllers under the applicable Data Protection Laws. Customer enters into this DPA upon signing it on behalf of itself and, as the case may be, in the name and on behalf of Authorized Affiliates if and to the extent Trimble processes Personal Data for which such Authorized Affiliates qualify as the Controller. 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 (including Appendices 1 to 3).
II. It has been pre-signed on behalf of Trimble. The Standard Contractual Clauses in Schedule 3 have been pre-signed by Trimble Inc. as the potential data importer.
III. 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. Complete the online signature process or download and 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.

Upon receipt of the validly completed DPA by Trimble at this email address, this DPA will become legally binding.

HOW THIS DPA APPLIES:

- If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreements. In such case, 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. This DPA will be considered as a direct agreement between Customer and Trimble.

This DPA shall 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 and considered Controller under the Data Protection Laws and Regulations 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.

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

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

"**Processor**" means the entity which Processes Personal Data on instruction and on behalf of the Controller.

"**Data Protection Laws and Regulations**" means all laws and regulations, including laws and regulations of the European Union, of the European Economic Area, and each of their member states, of Switzerland and of the United Kingdom, applicable to the Processing of Personal Data under the Agreement, including the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; hereinafter "GDPR"), and any implementation or successor legislation thereof.

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

"**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), where 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.

"**Trimble**" means the Trimble entity which is a party to this DPA, as specified in the section "HOW THIS DPA APPLIES" above, being Trimble Inc., a company incorporated in Delaware. Possible Trimble entities are: Trimble NV, a company registered in Belgium, PeopleNet Communications Corporation, a company, registered in the United States of America, LogicWay B.V., a company registered in the Netherlands, 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 France SAS, a company incorporated in France, Trimble Technologies Ireland Ltd, a company incorporated in Ireland, Trimble Solutions Sandvika AS, a company incorporated in Norway, Lakefield eTechnologies Ltd, a company incorporated in Ireland, Trimble Solutions Corporation, a company incorporated in Finland, Trimble Forestry Europe Corporation, a company incorporated in Finland, as applicable.

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

"**Standard Contractual Clauses**" means the agreement executed by and between Customer and Trimble Inc. and attached hereto as Schedule 3 pursuant to the European Commission's decision of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

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

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.

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 organisation. 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; and (iii) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

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 (Details 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, and undertake effort to inform Customer within 12 hours, 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 written consent 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 Date 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. Trimble shall not engage a Sub-processor without prior specific or general written authorization of Customer. In the case of general written authorization, Trimble shall inform Customer of any intended changes concerning the addition or replacement of Sub-processors, thereby giving Customer the opportunity to object to such changes. 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 the same 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. Trimble shall make available to Customer the current list of Sub-processors for the Services identified in Appendix 3 of the Standard Contractual Clauses attached hereto. Such Sub-processor lists shall include the identities of those Sub-processors and their country of location ("Sub-processor Lists"). Customer may find on the Trimble Privacy Center (accessible via www.Trimble.com/privacy a mechanism to subscribe to notifications of new Sub-processors for each applicable Service, to which Customer shall subscribe, and if Customer subscribes, Trimble shall provide notification of a new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

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 writing within ten (10) 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 thirty (30) days, Customer may terminate the applicable order(s) 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 2. 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 shall allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer. Trimble may have obtained third-party certifications and audits. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Trimble shall make available to Customer that is not a competitor of Trimble (or Customer's independent, third-party auditor that is not a competitor of Trimble) a copy of Trimble's then most recent third-party audits, certifications or any other information necessary to demonstrate Customer's compliance with the obligations set forth in this DPA.

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 unless legislation imposed on Customer requires the storage of Customer Data.

8. AUTHORIZED AFFILIATES

8.1 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.

8.2 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.

8.3 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 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

9. 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 Agreements, 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 EUR 50,000.

10. PARTIES TO THIS DPA

The Section "HOW THIS DPA APPLIES" specifies which Trimble entity is party to this DPA. In addition, Trimble Inc. is a party to the Standard Contractual Clauses in Schedule 3. Notwithstanding the signatures below of any other Trimble entity, such other Trimble entities are not a party to this DPA or the Standard Contractual Clauses. Where Trimble is a different legal entity than Trimble Inc., Trimble is carrying out the obligations of the data importer as set out in Schedule 3 on behalf of Trimble Inc.

11. NOT USED

12. TERMS FOR THE USE OF STANDARD CONTRACTUAL CLAUSES

12.1 Application of Standard Contractual Clauses. The Standard Contractual Clauses apply to (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all Affiliates (as defined in the Agreement) of Customer established within the European Economic Area, Switzerland and the United Kingdom, which have signed order(s) ("Data Exporters" for the purpose of the Standard Contractual Clauses and this Section 12).

12.2 Sub-processors. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that Trimble's Affiliates as well as a third-party may be engaged as Sub-processors. Trimble shall make available to Customer the current list of Sub-processors in accordance with Section 5.2 of this DPA. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that Trimble may engage new Sub-processors as described in Sections 5 of the DPA.

12.3 Audits and Certifications. The parties agree that audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications. Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Trimble shall make available to Customer that is not a competitor of Trimble (or Customer's independent, third-party auditor that is not a competitor of Trimble) information regarding the Trimble Group's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits. Customer may contact Trimble to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer shall reimburse Trimble for any time expended for any such on-site audit at the Trimble Group's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Trimble shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Trimble. Customer shall promptly notify Trimble with information regarding any non-compliance discovered during the course of an audit.

12.4 Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Trimble to Customer only upon Customer's request.

12.5 Conflict. In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Schedule 3, the Standard Contractual Clauses shall prevail.

LIST OF SCHEDULES

Schedule 1: Details of the Processing

Schedule 2: Technical and Organizational Measures

Schedule 3: Standard Contractual Clauses

The parties' authorized signatories have duly executed this Agreement:

CUSTOMER (hereby signs this DPA and Schedule 3 with its Annexes)

Signature:_____

Print Name: _____

Title: _____

Date: _____

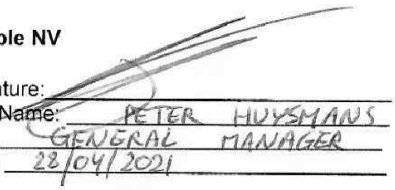
Customer Legal Name:_____

Address:

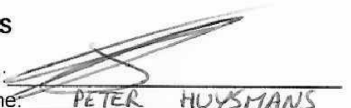
email:

Trimble Customer Number:_____

Trimble NV

Signature: 
Print Name: PETER HUYSMANS
Title: GENERAL MANAGER
Date: 28/04/2021

Solid SAS

Signature: 
Print Name: PETER HUYSMANS
Title: GENERAL MANAGER
Date: 28/04/2021

LogicWay B.V

Signature: 
Print Name: PETER HUYSMANS
Title: GENERAL MANAGER
Date: 28/04/2021

SCHEDULE 1 - DETAILS OF THE PROCESSING AND PROTECTION

This Schedule 1 specifies the generic set of Trimble's Data Processing and Protection information applicable to the Services Customer has subscribed to under the Agreements. Further information may be found in the Data Sheet applicable to the Service(s) you have subscribed to, and available at trimble.com/corporate/privacy under the tab additional materials. The applicable Data Sheet will serve as the DPA Schedule 1 and 2 to this DPA and Annexes to the data transfer agreement set forth in Schedule 3, if applicable. If there is no Data Sheet available for the Services you have subscribed to on the webpage above, the information reported in this document will apply. Data Sheets for our Service(s) will be made available and amended as the Services evolve, and any additional release replaces or amends the information previously provided. Please note that we have prepared the lists in Sections 1, 2.1 and 3 based on how we have designed the Services. Since you are a Controller, you may use the Services in different ways. If you believe that these lists need to be amended, please contact privacy@trimble.com.

Categories of Data Subjects
Data Subjects of any Customer Personal Data, that can be Processed in the Services, may include Customer's and its affiliates' employees, contractors, business partners, and clients
● Customers' and their affiliates' employees (including permanent, and temporary workers, contractors, and apprentices)
● Employees of Customers' and their affiliates' actual and prospective clients (including permanent, and temporary workers, contractors, and apprentices)
● Employees of Customers' and their affiliates' contractors and vendors (including permanent, and temporary workers, contractors, and apprentices)
● Customers' and their affiliates' actual and prospective clients (if those clients are individuals)
● Customers' and their affiliates actual and prospective contractors and vendors (if those contractors and vendors are individuals)
● Customers' visitors
● Recipients of deliveries which Customers and their affiliates make

2. Personal Data
The Types of Personal Data and Special Categories of Personal Data that generally can be Processed within the Service include, but are not limited to:

2.1 Types of Personal Data
● Person Name and contact details
● Identity of the Individual
● Address of the Individual
● Online Access and Authentication Credentials
● Online Connection and Network Connectivity Data
● Online Identifier
● Technology Identifiers
● Telephony
● Behavior
● Task related data as it relates to Individuals
● Design related data as it relates to Individuals
● Appointments, Schedules, Calendar Entries
● Physical Locations of the Individual
● Capabilities and Qualifications of the Individual
● Education and Professional Certifications
● Profession and Employment Information Data
● Professional Affiliations
● Characteristics of the Individual
● Biometric
● Demographic
● Economic and Financial
● Nationality and Citizenship
● Government Identities
● Identification Number
● Personal Preference and Interest

2.2 Special Categories of Personal Data
● Biometric data

3. Processing Activities
The Processing activities with regard to Customer Content (including Customer Personal Data) within the Services include, but are not limited to:
● Telematic Services
● Video Intelligence Services
● Fleet Management Services
● Driver Safety and Performance Services
● Design Services
● Workflow Management Services
● Logistics Management Services
● Project Management Services
● Workforce Management Services
● Geospatial Data Processing Services
● Mapping Data Services
● Land Management Services

4. Duration of Processing
The duration of Processing in the course of the Services corresponds to the duration of the Services, unless differently stated in the Data Sheet applicable to your Services(s).

5. Deletion and Return of Content
Trimble will delete all Customer Content (including Customer Personal Data) at termination or expiration of the Services within the agreed timeframes.

6. Processing locations
Trimble internal and external data hosting and Processing locations in Europe and the United States are utilized for the Services.

7. Third Party Sub-Processors
The Services may involve third party Subprocessors in the Processing of Content, including Customer Personal Data. The following companies may be involved: A list of sub-processor is available at trimble.com/privacy/subprocessors. AWS, Azure, SnowFlake, MongoDB Atlas, Sumo Logic, DataDog, PingDom, New Relic, FreshService, NetSuite, SalesForce, MailChimp, HubSpot, Atlassian StatusPage, Google.
Any changes to Subprocessors will be communicated in accordance with the DPA.

8. International Data Transfer
Please refer to attached Schedule 3 of this DPA

9. Privacy Contact
The privacy contacts for Trimble's Services is at privacy@trimble.com and trimble.com/privacy

SCHEDULE 2 – TECHNICAL AND ORGANIZATIONAL MEASURES

1. Technical and Organization Security Measures

This Appendix describes the technical and organizational security measures and procedures that Trimble shall, as a minimum, maintain to protect the security of personal data created, collected, received, or otherwise obtained. Trimble will keep documentation of technical and organizational measures identified below to facilitate audits and for the conservation of evidence. Trimble will conduct periodic reviews of its security practices and evaluate the adequacy of its measures and reserves the right to modify the standards set forth below.

In addition Trimble has been granted the ISO 27001-certificate, that can be found under this link: https://www.schellman.com/certificate-directory?certificateNumber=1650760-4

Access Control to Processing Areas

Trimble implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment where the personal data are processed or used. This is accomplished by:

- establishing security areas; 24 hours security service provided by property owner;
- protection and restriction of access paths;
- securing the data processing equipment;
- establishing access authorizations for staff and third parties, including the respective documentation;
- regulations on card-keys;
- restriction on card-keys;
- all access to the data centre where personal data are hosted is logged, monitored, and tracked; and
- the data centre where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

Access Control to Data Processing Systems

Trimble implements suitable measures to prevent its data processing systems from being used by unauthorized persons. This is accomplished by:

- identification of the terminal and/or the terminal user to Trimble systems;
- automatic time-out of user terminal if left idle, identification and password required to reopen;
- automatic turn-off of the user ID when several erroneous passwords are entered, log file of events (monitoring of break-in-attempts);
- issuing and safeguarding of identification codes;
- dedication of individual terminals and/or terminal users, identification characteristics exclusive to specific functions;
- staff policies in respect of each staff access rights to personal data (if any), informing staff about their obligations and the consequences of any violations of such obligations, to ensure that staff

will only access personal data and resources required to perform their job duties and training of staff on applicable privacy duties and liabilities;

- all access to data content is logged, monitored, and tracked; and
- use of state of the art encryption technologies.

Access Control to Use Specific Areas of Data Processing Systems

Trimble commits that the persons entitled to use its data processing system are only able to access the data within the scope and to the extent covered by its access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This shall be accomplished by:

- staff policies in respect of each staff member's access rights to the personal data;
- allocation of individual terminals and/or terminal user, and identification characteristics exclusive to specific functions;
- monitoring capability in respect of individuals who delete, add or modify the personal data and at least yearly monitoring and update of authorization profiles;
- release of data to only authorized persons;
- policies controlling the retention of backup copies; and
- use of state of the art encryption technologies.

Transmission Control

Trimble implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:

- use of state-of-the-art firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
- as far as possible, all data transmissions are logged, monitored and tracked; and
- monitoring of the completeness and correctness of the transfer of data (end-to-end check).

Input Control

Trimble implements suitable measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems or removed. This is accomplished by:

- an authorization policy for the input of data into memory, as well as for the reading, alteration and deletion of stored data;
- authentication of the authorized personnel; individual authentication credentials such as user IDs that, once assigned, cannot be re-assigned to another person (including subsequently);
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- utilization of user codes (passwords) of at least eight characters or the system maximum permitted number and modification at first use and thereafter at least every 90 days in case of processing of sensitive data;

- following a policy according to which all staff of Trimble who have access to personal data processed for Customer and its Authorized Affiliates shall reset their passwords at a minimum once in a 180 day period;

- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked;

- automatic log-off of user ID's (requirement to re-enter password to use the relevant work station) that have not been used for a substantial period of time;

- automatic deactivation of user authentication credentials (such as user IDs) in case the person is disqualified from accessing personal data or in case of non use for a substantial period of time (at least six months), except for those authorized solely for technical management;

- proof established within Trimble's organization of the input authorization; and

- electronic recording of entries.

Job Control

Trimble ensures that personal data may only be processed in accordance with written instructions issued by Controller. This is accomplished by:

- binding policies and procedures for Trimble's employees, subject to Customer and its Authorized Affiliates' review and approval.

Trimble ensures that if security measures are adopted through external entities it obtains written description of the activities performed that guarantees compliance of the measures adopted with this document. Trimble further implements suitable measures to monitor its system administrators and to ensure that they act in accordance with instructions received. This is accomplished by:

- individual appointment of system administrators;

- adoption of suitable measures to register system administrators' access logs and keep them secure, accurate and unmodified for at least six months;

- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by Processor and applicable laws; and

- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to Customer and its Authorized Affiliates upon request.

Availability Control

Trimble implements suitable measures to ensure that personal data are protected from accidental destruction or loss. This is accomplished by:

- infrastructure redundancy to ensure data access is restored within seven days and backup performed at least weekly;

- only the Customer and its Authorized Affiliates may authorize the recovery of backups (if any) or the movement of data outside of the location where the physical database is held, and security measures will be adopted to avoid loss or unauthorized access to data, when moved;

- regular check of all the implemented and herein described security measures at least every six months;

- backup tapes are only re-used if information previously contained is not intelligible and cannot be re-constructed by any technical means; other removable media is destroyed or made unusable if not used; and

- any detected security incident is recorded, alongside the followed data recovery procedures, and the identification of the person who carried them out.

Separation of processing for different purposes

Trimble implements suitable measures to ensure that data collected for different purposes can be processed separately. This is accomplished by:

- access to data is separated through application security for the appropriate users;
- modules within Trimble's database separate which data is used for which purpose, i.e. by functionality and function; and
- at the database level, data is stored in different areas, separated per module or function they support; and
- interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

Trimble system administrators (if any):

Trimble implements suitable measures to monitor its system administrators and to ensure that they act in accordance with instructions received. This is accomplished by:

- individual appointment of system administrators;
- adoption of suitable measures to register system administrators' access logs and keep them secure, accurate and unmodified for at least six months;
- continuous audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by Processor and applicable laws; and
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to Customer and its Authorized Affiliate upon request.

SCHEDULE 3 – STANDARD CONTRACTUAL CLAUSES (Processors)

In addition to the Standard Contractual Clauses set forth below, the following provisions apply:

1. Unless prohibited by applicable law, data importer shall inform the data exporter 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 (as defined below).

2. Data importer shall 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, data importer will give data exporter reasonable notice to allow data exporter to seek a protective order or other appropriate remedy unless data importer is legally prohibited from doing so.

3. Should a new/updated version of the Clauses become available, data importer shall upon data exporter's reasonable request agree to the new/amended version of the Clauses.

4. In case data importer makes personal data available to sub-processors, data importer 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.

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

See Information on page 6 of the DPA
……

(the data **exporter**)

and

Trimble Inc
935 Stewart Drive, Sunnyvale, CA 94085, USA

privacy@trimble.com

(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; [*If these Clauses are governed by a law which extends the protection of data protection laws to corporate persons, the words “except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the definition of "personal data" is expanded to include those data” are added.*]

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these

measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a

summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

For the data exporter
Executed on page 6 of the Data Processing Agreement.

On behalf of the data importer:

Name James A. Kirkland
Position: Senior Vice President and General Counsel

Signature……

On behalf of the data exporter:

Signature……

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter
The data exporter is: The Customer (see page 6 of the DPA)

Data importer
The data importer is:
Trimble Inc.

Data subjects
The personal data transferred concern the following categories of data subjects:
See Schedule 1 of the DPA

Categories of data
The personal data transferred concern the following categories of data:
See Schedule 1 of the DPA

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:
See Schedule 1 of the DPA

Processing operations
The personal data transferred will be subject to the following basic processing activities:

See Schedule 1 of the DPA

For the data exporter
Executed on page 6 of the Data Processing Agreement.

On behalf of the data importer:

Name James A. Kirkland
Position: Senior Vice President and General Counsel

Signature……

On behalf of the data exporter:

Signature……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

See Schedule 2 to the DPA