Data Processing Addendum

Between **Trimble GmbH** (Supplier) and the Customer. This data processing addendum ("DPA") is entered into between Supplier and Customer referring to the following service contracts:

Data Protection Legislation: All applicable data protection, privacy and data security laws, regulations in effect during the Term (including any applicable laws, regulations, guidelines and industry standards in the jurisdiction where Supplier performs the Services) ("Data Protection and Privacy Laws") including (i) General Data Protection Regulation (*(EU) 2016/679*) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, (ii) any successor legislation to the GDPR.

1. DATA PROTECTION

1.1 Both parties will comply with all applicable requirements of the Data Protection Legislation. This DPA is an addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Legislation.

1.2 The parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the controller and the Provider is the processor (where **Controller** and **Processor** have the meanings as defined in the Data Protection Legislation). The Schedule sets out the scope, nature and purpose of processing by the Provider, the duration of the processing and the types of personal data (as defined in the Data Protection Legislation, "**Personal Data"**) and categories of data subject.

1.3 Without prejudice to the generality of clause 1.1, the Customer will ensure that it fulfills all necessary requirements to enable lawful transfer of the Personal Data to the Provider for the duration and purposes of this agreement.

1.4 Without prejudice to the generality of clause 1.1, the Provider shall, in relation to any Personal Data processed in connection with the performance by the Provider of its obligations under this agreement:

(a) process that Personal Data only on the written instructions of the Customer subject to Art. 28 (3) GDPR. Instructions may be handled as a change request at the cost of Customer. Processor shall immediately inform the Controller if, in its opinion, an instruction infringes Data Protection Legislation;

(b) ensure that it has in place appropriate technical and organizational measures, reviewed and approved by the Customer (for the Provider's list of measures see the Schedule). Such measures shall ensure a level of security appropriate to the risks presented by processing and are subject to change depending on Provider`s recurring risk assessments;

(c) ensure that all personnel or any other person acting on behalf of the Provider who have access to and/or process Personal Data are obliged to keep the Personal Data confidential and any natural person acting under the authority of the Provider who has access to personal data does not process them except on instructions from the controller;

(d) not transfer any Personal Data outside of the European Economic Area unless the prior written consent of the Customer has been obtained and the necessary requirements for a transfer pursuant to the Data Protection Legislation are fulfilled;

(e) assist the Customer, at the Customer's cost, in responding to any request from a data subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications,

impact assessments and consultations with supervisory authorities or regulators;

(f) assist the Customer by providing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights pursuant to Data Protection Regulation;

(g) notify the Customer without undue delay on becoming aware of a Personal Data breach;

(h) at the written direction of the Customer, delete or return Personal Data and copies thereof to the Customer on termination of the agreement unless required by Applicable Law to store the Personal Data; and

(i) maintain complete and accurate records and information to demonstrate its compliance with this clause and the Data Protection Legislation and allow for audits by the Customer or the Customer's designated auditor.

1.5 The Provider shall not engage a third-party processor without prior specific or general written authorization of the Customer. The Customer consents to the Provider appointing the parties named in the Schedule as third-party processors of Personal Data under this agreement. The Provider confirms that it has entered or (as the case may be) will enter with the third-party processor into a written agreement in which he imposes on that other processor the obligations as set out in this DPA. The Provider informs the Customer of any intended changes concerning the addition or replacement of other processors. The Customer has the right to object to such changes. As between the Customer and the Provider, the Provider shall remain liable for all acts or omissions of any third-party processor appointed by it pursuant to this clause 1.5 to the same extent Supplier 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.

1.6 Either party may, at any time on not less than 30 days' notice, revise this clause data processing addendum by replacing it with any applicable controller to processor standard clauses or similar terms forming party of an applicable certification scheme (which shall apply when replaced by attachment to this agreement).

1.7 Each party's and its affiliates' liability arising out of or related to this DPA, 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, Supplier's and its affiliates' total liability for all claims from the Customer and its 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.

Appendices

Trimble Tilos

Appendix 1: Processing Specification Form 1

Type of data	Type and purpose (Subject matter) of the Data Processing	Categories of data subject affected

• Contact Details and Location (e.g. name, email, address, phone) • Language preference • IP address • Online IDs (social logins)	• User authentication • SSO session • User profile details • Forgot password • Logging, debugging and customer support	• Direct end users and customers • Employees and contractors of customers
• Project Related Information	• Information you make available to us for support purposes	•

Appendix 2: Technical and Organizational Measures

This Appendix describes the technical and organizational security measures and procedures that the Data Processor shall, as a minimum, maintain to protect the security of personal data created, collected, received, or otherwise obtained. Data processor will keep documentation of technical and organizational measures identified below to facilitate audits and for the conservation of evidence.

Access Control to Processing Areas

Data processor 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 center 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

Data processor 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 the Data processor 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

Data processor 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

Data processor 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

Data processor 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 Data processor who have access to personal data processed for Data Exporters 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 Data processor's organization of the input authorization; and
- electronic recording of entries.

Job Control

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

- binding policies and procedures for Data processor's employees, subject to Data Exporters' review and approval.

Data processor 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. Data processor 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 importer 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 Data Exporters upon request.

Availability Control

Data processor 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;

- tape backup is stored off-site and available for restore in case of failure of SAN infrastructure for Database server;
- only the Data Exporters 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

Data processor 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 the Data processor's data base 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.

Data processor system administrators (if any):

Data processor 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 importer 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 data exporter upon request.

Appendix 3: List of Sub-Processors

Sub-Processor Name	Address	Safeguards acc. to Art. 44 - 50 GDPR
Amazon Web Services, Inc.	440 Terry Ave. N., Seattle, WA 98109, USA	Data Processing Agreement
Trimble Inc.	935 Stewart Drive, Sunnyvale, CA 94085, USA	Data Processing Agreement with standard clauses