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 in the course of which Trimble receives personal data from Customer (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) from Trimble.

Customer enters into this DPA 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 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 2
II. It has been pre-signed on behalf of Trimble. The Standard Contractual Clauses are incorporated by reference.
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. 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 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 an Agreement, this DPA is an addendum to and forms part of thatAgreement 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 this DPA is neither a party to an order nor the Agreement, 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.
- 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.

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 one or more Data Protection Laws and Regulations of the European Union, The European Economic Area, their member states, Switzerland, and the United Kingdom 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."

"**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, the European Economic Area and their member states, Switzerland and the United Kingdom, 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, the European Economic Area, Switzerland and the United KIngdom.

"**GDPR**" means 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), including as implemented or adopted under the laws of the United Kingdom.

"**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.

"**Processor**" means the entity which Processes Personal Data 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.

"**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, as data importer for purposes of the standard contractual clauses. Possible Trimble entities acting as data processor are: Trimble Europe BV, a company registered in the Netherlands, Trimble International BV, 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 NV, a company incorporated in Belgium, Trimble Belgium BV, a company incorporated in Belgium, Trimble Solutions Sandvika AS, a company incorporated in Norway, Trimble Solutions Corporation, a company incorporated in Finland, Trimble Forestry Europe Corporation, a company incorporated in Finland, Lakefield eTechnologies Ltd, a company incorporated in Ireland, or Trimble GmbH, a company incorporated in Germany, 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. pursuant to the European Commission's decision of 4 June 2021 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 where such instructions are consistent with the terms of the Agreement.

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.

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/Transfer) 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 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 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 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. 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. The Sub-processor List contains a mechanism to subscribe to notifications of new Sub-processors for each applicable Service, and if Customer subscribes, Trimble shall provide notification of a new Sub-processor(s) before authorizing any 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 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) 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 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 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 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. 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 theEU C-to-P Transfer Clauses. Notwithstanding the signatures below of any other Trimble entity, such other Trimble entities are not a party to this DPA or the EU C-to-P Transfer Clauses.

12. EUROPE SPECIFIC PROVISIONS

12.1. **Definitions**. For the purposes of this section 12 these terms shall be defined as follows:
"EU C-to-P Transfer Clauses" means Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent they reference Module Two (Controller-to-Processor).
"EU P-to-P Transfer Clauses" means Standard Contractual Clauses sections I, II III and IV (as applicable) to the extent they reference Module Three (Processor-to-Processor).

12.2. **GDPR**. Trimble will Process Personal Data in accordance with the GDPR requirements directly applicable to Trimble 's provision of its Services.

12.3. **Customer Instructions**. Trimble shall inform Customer immediately (i) if, in its opinion, an instruction from Customer constitutes a breach of the GDPR and/or (ii) if Trimble is unable to follow Customer's instructions for the Processing of Personal Data.

12.4. **Transfer mechanisms for data transfers**. If, in the performance of the Services, Personal Data that is subject to the GDPR or any other law relating to the protection or privacy of individuals that applies in Europe is transferred out of Europe to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws and Regulations of Europe, the transfer mechanisms listed below shall apply to such transfers and can be directly enforced by the Parties to the extent such transfers are subject to the Data Protection Laws and Regulations of Europe:

● The EU P-to-P Transfer Clauses. Trimble's Affiliates in Europe acting as Processor and data exporter to Trimble Inc as sub-processor and data importer have entered into EU P-to-P Transfer Clauses for the benefit of Customer and its Affiliates. The EU P-P Transfer Clauses are available at trimble.com/privacy,apx under "Additional Materials". Customer and its Affiliates hereby consent to the transfer pursuant to these EU P-P Transfer Clauses. Customer and its Affiliates can always withdraw such consent by informing Trimble that they want to enter into the following Clauses.

● Such other transfer mechanisms as Trimble and its Affiliates implement and maintain..

● The EU C-to-P Transfer Clauses. Where Customer and/or its Authorized Affiliate is a Controller and a data exporter of Personal Data and Trimble Inc. is a Processor and data importer in respect of that Personal Data, then the Parties incorporate by reference the EU C-to-P Transfer Clauses and shall comply with them. In addition to the EU C-to-P Transfer Clauses , the terms in Section 13 below apply.

12.5. **Impact of local laws**. As of the Effective Date, Trimble has no reason to believe that the laws and practices, including requirements to disclose Personal Data to or measures authorising access by a Public Authority, in any third country where it Processes Personal Data, prevent Trimble from fulfilling its obligations under this DPA. If Trimble reasonably determines that any existing or future enacted or enforceable laws and practices in the third country of destination applicable to its Processing of the Personal Data ("Local Laws") prevent it from fulfilling its obligations under this DPA, it shall promptly notify Customer. In such a case, Trimble shall use reasonable efforts to modify the Services for the affected Customer, or recommend a commercially reasonable change to Customer's configuration or use of the Services to facilitate compliance with the Local Laws without unreasonably burdening Customer. If Trimble is unable to make available such change, Customer may terminate the applicable Order Form(s) and suspend the transfer of Personal Data in respect only to those Services which cannot be provided by Trimble in accordance with the Local Laws by providing written notice in accordance with the "Notices" section of the Agreement.

13. ADDITIONAL TERMS FOR THE USE OF STANDARD CONTRACTUAL CLAUSES

If Customer opts for the EU C-to-P Clauses and for their purposes, Customer is the data exporter and Trimble is the data importer and the Parties agree to the following. If and to the extent an Authorized Affiliate relies on the EU C-to-P Transfer Clauses for the transfer of Personal Data, any references to 'Customer' in this Section 13, include such Authorized Affiliate.

13.1. **Reference to the Standard Contractual Clauses**. The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA. The information required for the purposes of the Appendix to the Standard Contractual Clauses are set out in this Section 13.

13.2. **Docking clause**. The option under clause 7 shall not apply.

13.3. **Instructions**. This DPA and the Agreement are Customer's complete and final documented instructions at the time of signature of the Agreement to Trimble for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Agreement. For the purposes of clause 8.1(a), the instructions by Customer to Process Personal Data are set out in section 2.3 of this DPA and include onward transfers to a third party located outside Europe for the purpose of the performance of the Services.

13.4. **Certification of Deletion**. The parties agree that the certification of deletion of Personal Data that is described in clause 8.5 and 16(d) of the Standard Contractual Clauses shall be provided by Trimble to Customer only upon Customer's written request.

13.5. **Security of Processing**. For the purposes of clause 8.6(a), Customer is solely responsible for making an independent determination as to whether the technical and organisational measures set forth in Schedule 1 meet Customer's requirements and agrees that (taking into account the state of the art, the costs of implementation, and

the nature, scope, context and purposes of the Processing of its Personal Data as well as the risks to individuals) the security measures and policies implemented and maintained by Trimble provide a level of security appropriate to the risk with respect to its Personal Data. For the purposes of clause 8.6(c), personal data breaches will be handled in accordance with section 7 (Customer Data Incident Management and Notification) of this DPA.

13.6. **Audits of the SCCs**. The parties agree that the audits described in clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with section 6.2 of this DPA.

13.7. **General authorisation for use of Sub-processors**. Option 2 under clause 9 shall apply. For the purposes of clause 9(a), Trimble has Customer's general authorisation to engage Sub-processors in accordance with section 5 of this DPA. Trimble shall make available to Customer the current list of Sub-processors in accordance with section 5.2 of this DPA. Where Trimble enters into the EU P-to-P Transfer Clauses with a Sub-processor in connection with the provision of the Services, Customer hereby grants Trimble and Trimble 's Affiliates authority to provide a general authorisation on Controller's behalf for the engagement of sub-processors by Sub-processors engaged in the provision of the Services, as well as decision making and approval authority for the addition or replacement of any such sub-processors.

13.8. **Notification of New Sub-processors and Objection Right for new Sub-processors**. Pursuant to clause 9(a), Customer acknowledges and expressly agrees that Trimble may engage new Sub-processors as described in sections 5.2 and 5.3 of this DPA. Trimble shall inform Customer of any changes to Sub-processors following the procedure provided for in section 5.2 of this DPA.

13.9. **Complaints - Redress**. For the purposes of clause 11, and subject to section 3 of this DPA, Trimble shall inform data subjects on its website of a contact point authorised to handle complaints. Trimble shall inform Customer if it receives a complaint by, or a dispute from, a Data Subject with respect to Personal Data and shall without undue delay communicate the complaint or dispute to Customer. Trimble shall not otherwise have any obligation to handle the request (unless otherwise agreed with Customer). The option under clause 11 shall not apply.

13.10. **Liability**. Trimble's liability under clause 12(b) shall be limited to any damage caused by its Processing where Trimble has not complied with its obligations under the GDPR specifically directed to Processors, or where it has acted outside of or contrary to lawful instructions of Customer, as specified in Article 82 GDPR.

13.11. **Supervision**. Clause 13 shall apply as follows:

13.11.1. Where Customer is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by Customer with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

13.11.2. Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.

13.11.3. Where Customer is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, Autoriteit Persoonsgegevens, PO Box 93374, 2509 AJ DEN HAAG, The Netherlands, shall act as competent supervisory authority.

2.11.4. Where Customer is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office shall act as competent supervisory authority.

2.11.5. Where Customer is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

13.12. **Notification of Government Access Requests**. For the purposes of clause 15(1)(a), Trimble shall notify Customer (only) and not the Data Subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the Data Subject as necessary.

13.13. **Governing Law**. The governing law for the purposes of clause 17 shall be the law that is designated in the Governing Law section of the Agreement. If the Agreement is not governed by an EU Member State law, the Standard Contractual Clauses will be governed by either (i) the laws of the Netherlands; or (ii) where the Agreement is governed by the laws of the United Kingdom, the laws of the United Kingdom.

13.14. **Choice of forum and jurisdiction**. The courts under clause 18 shall be those designated in the Venue section of the Agreement. If the Agreement does not designate an EU Member State court as having exclusive jurisdiction to resolve any dispute or lawsuit arising out of or in connection with this Agreement, the parties agree

that the courts of either (i) the Netherlands; or (ii) where the Agreement designates the United Kingdom as having exclusive jurisdiction, the United Kingdom, shall have exclusive jurisdiction to resolve any dispute arising from the Standard Contractual Clauses. For Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

13.15. **Appendix**. The Appendix shall be completed as follows:

- The contents of section 1 of Schedule 1 shall form Annex I.A to the Standard Contractual Clauses
- The contents of sections 2 to 9 of Schedule 1 shall form Annex I.B to the Standard Contractual Clauses
- The contents of section 10 of Schedule 1 shall form Annex I.C to the Standard Contractual Clauses
- The contents of section 11 of Schedule 1 to this Exhibit shall form Annex II to the Standard Contractual Clauses.

13.16. **Data Exports from the United Kingdom and Switzerland under the Standard Contractual Clauses**. In case of any transfers of Personal Data from the United Kingdom and/or transfers of Personal Data from Switzerland subject exclusively to the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws"), (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the Data Protection Laws and Regulations of the United Kingdom ("UK Data Protection Laws") or Swiss Data Protection Laws, as applicable; and (ii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under UK Data Protection Laws or Swiss Data Protection Laws, as applicable. In respect of data transfers governed by Swiss Data Protection Laws, the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity.

13.17. **Conflict**. The Standard Contractual Clauses are subject to this DPA and the additional safeguards set out hereunder. The rights and obligations afforded by the Standard Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

14. TERMS GOVERNING THE PROCESSING OF RESIDENTS OF THE UNITED STATES

In relation the data of US residents, and to the extent this DPA is concluded in the context of a contract with Customer for the worldwide provision of services from Trimble, Customer agrees to the terms posted in Trimble's Privacy Center (Customer US Data Processing Addendum (information shared with Trimble), which are hereby incorporated in this Data Processing Addendum.

LIST OF SCHEDULES

Schedule 1: Details of the Processing

The parties' authorized signatories have duly executed this Agreement:

CUSTOMER (hereby signs this DPA)

Signature:_____

Print Name: _____

Title: _____

Date: _____

Customer has purchased the Services through

Trimble's Authorized Reseller or Business Partner

Customer Legal Name:_____

Address

Reseller Name

Address_____

Trimble Customer Number:_____

Reseller Customer Number_____

☐ Customer acts as data exporter and the EU C-to-P Transfer Clauses shall apply as set forth in this DPA.

Trimble Inc

James. A. Kirkland

Signature:_____

Print Name:James. A. Kirkland

Title: Senior Vice President and General Counsel

Date: 15.12.2022_

Trimble Europe BV

Signature:_____

Print Name: RHH Reeder

Title: Director

Date: 15.12.2022

Trimble UK Ltd

Signature:_____

Print Name: RHH Reeder

Title: Director

Date: 15.12.2022

Trimble France SAS

Signature:_____

Print Name: RHH Reeder

Title: Director

Date: 15.12.2022

Trimble Solutions Sandvika AS

Signature:_____

Print Name: RHH Reeder

Title: Director

Date: 15.12.2022

Trimble Technologies Ireland Ltd

Signature:_____

Print Name: RHH Reeder

Title: Director

Date: 15.12.2022_

Lakefield eTechnologies Ltd

Signature:_____

Print Name: RHH Reeder

Title: Director

Date: 15.12.2022

Trimble International BV

Signature:_____

Print Name:RHH Reeder

Title:Director

Date: 15.12.2022

Trimble Solutions Corporation

Trimble GmbH

Signature:_____
Print Name:Jürgen Kesper
Title: Director
Date: 15.12.2022

Signature:_____
Print Name:RHH Reeder
Title: Director
Date: 15.12.2022

Trimble MAPS Ltd.

Trimble Forestry Europe Corporation

Signature:_____
Print Name: RHH Reeder
Title: Director
Date:15.12.2022

Signature:_____
Print Name:RHH Reeder
Title: Director
Date: 15.12.2022

Trimble NV

Signature:_____
Print Name:Jürgen Kesper
Title: Director
Date: 15.12.2022

Contact Details for all Trimble entities:

privacy@trimble.com
10368 Westmore Drive, Westminster, CO 80021, USA

Addresses Trimble Entities	
Trimble Inc.	**Trimble Europe B.V.**
10368 Westmoor Drive Westminster, CO 80021, USA	Industrieweg 187a 5683CC Best, the Netherlands
Trimble UK Ltd.	**Trimble France SAS**
1 Bath Street, Ipswich, Suffolk, IP2 8SD, United Kingdom	1 Quai Gabriel Péri 94340 Joinville-le-Pont, France
Trimble Solutions Sandvika AS	**Trimble Technologies Ireland Ltd**
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 Ltd	**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 Solutions Corporation	**Trimble GmbH**
Hatsinanpuisto 8, 02600 Espoo, Finland	Am Prime Parc 11, 65479 Raunheim
Trimble MAPS Ltd.	**Trimble Forestry Europe Corporation**

Baird House, 15-17 St Cross Street, London, EC1N 8UW, UK	Hatsinanpuisto 8, 02600 Espoo, Finland
Trimble NV	
Ter Waarde 50, 8900 Ieper, Belgium	

SCHEDULE 1 - DESCRIPTION OF PROCESSING/TRANSFER
(Annex I of the Standard Contractual Clauses)

A

1. LIST OF PARTIES

Data exporter(s): Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union

Name: Customer and its Authorized Affiliates.

Address:

Contact person's name, position and contact details:

If there is a list of several group companies, please attach.

Activities relevant to the data transferred under these clauses:

Performance of the Services pursuant to the Agreement and as further described in the Documentation.

Signature and date:

Data importer(s): Identity and contact details of the data importer(s), including any contact person with responsibility for data protection
Name: Trimble Inc..
Address: 10368 Westmoor Dr, Westminster, CO 80021, United States

Contact person's name, position and contact details:

Office of Data Protection, privacy@trimble.com

Signature and date:15.12.2022
Trimble Inc.

James A. Kirkland
Senior Vice President and General Counsel

B.

2. 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 or 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

3. 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

4. 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 below.

5. 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.

6. NATURE OF THE PROCESSING
The nature of the Processing is the performance of the Services pursuant to the Agreement.

7. 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.

8. 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 for the duration of the Agreement, unless otherwise agreed, for example in Section 9 of the DPA.

9. SUB-PROCESSOR TRANSFERS
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

As per 7 above, the 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.

10. COMPETENT SUPERVISORY AUTHORITY
Identify the competent supervisory authority/ies in accordance with clause 13:
● Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.
● Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as the competent supervisory authority.

● Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: Autoriteit Persoonsgegevens, PO Box 93374, 2509 AJ DEN HAAG, The Netherlands, shall act as the competent supervisory authority.
● Where the data exporter is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws and Regulations, the Information Commissioner's Office shall act as the competent supervisory authority.
● Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

11. TECHNICAL AND ORGANISATIONAL MEASURES
(Annex II of the Standard Contractual Clauses)

This document describes Trimble's Technical and Organizational Security Measures implemented to protect the security and privacy of Customer Data. All related measures are focused on protecting risks posed to the privacy rights of natural persons whose personal data may be processed as a part of Customer Data.

This document contains an overview of the technical and organizational measures for the protection of personal data implemented by Trimble in accordance with Article 32 GDPR.

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 applicable data protection laws. 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 2
Applies if Customer has checked the box on page 9

STANDARD CONTRACTUAL CLAUSES
Module 2
Controller to Processor

SECTION I

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clause

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e)

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 **Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the

personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([4]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([8]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(a) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Netherlands.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

The Annexes to the Standard Contractual Clauses are set forth in Schedule 1 to the Data Protection Agreement.