

STANDARD CONTRACTUAL CLAUSES
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) 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 [Specify time period] 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 (c), 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.

ANNEX I

A Controller/Exporter

Netherlands

1. Trimble Europe BV, Industrieweg 187a, NL-5683CC Best, the Netherlands

Office of Data Protection, privacy@trimble.com



15.12.2022

Signature

accession date

RHH Reeder

Director

2. Logicway BV, Zandbreeuweg 10a BE4, 7577 BZ Oldenzaal, the Netherlands



15.12.2022

Signature

accession date

RHH Reeder

Director

United Kingdom

3. Trimble UK Ltd., 1 Bath St, Ipswich IP2 8SD, United Kingdom

4. Amtech Ltd. Cygna House, 3 Opal Dr, Milton Keynes MK15 0DF, United Kingdom



15.12.2022

Signature

accession date

RHH Reeder

Director

5. Viewpoint Construction Software Ltd., 4th Floor Central Square, Forth St. Newcastle upon Tyne, NE13PJ, United Kingdom



15.12.2022

Signature

accession date

James. A. Kirkland

Director

6. AgileAssets Ltd. 8 Lincoln's Field, London, W2C3BP, United Kingdom



15.12.2022

Signature

accession date

RHH Reeder

Director

Ireland

7. Trimble Technologies Ireland Ltd. Unit 3d North Point House, North Point Business Park, Cork, T23 AT2P, Ireland

8. Lakefield eTechnologies Ltd. The National Software Centre, Mahon, Cork, T12DVF8, Ireland



15.12.2022

Signature

accession date

RHH Reeder

Director

Norway

9. Trimble Solutions Sandvika AS, Leif Tronstads plass 41337 Sandvika, Norway



15.12.2022

Signature

accession date

Jürgen Kesper

Director

Sweden

10. Pocketmobile AB, Rinkebyvägen 17, 182 36 Danderyd, Sweden



15.12.2022

Signature

accession date

RHH Reeder

Board Member

Finland

11. Trimble Solutions Corporation, Hatsinanpuisto 8, 02600 Espoo, Finland

12. Trimble Forestry Corporation, Revontulentie 8c, 02100 Espoo, Finland



Signature
Jürgen Kesper
Board Member

15.12.2022
accession date

France

13. Trimble France SAS, 1 Quai Gabriel Péri, 94340 Joinville-le-Pont, France

14. Bilberry SAS, 44 Av. Raspail, 94250 Gentilly, France

15. Solid SAS, 11-21 Rue Hubble Parc, Scientifique de la Haute Borne, Singhin en Melantois,
59262 France



Signature
RHH Reeder
President

15.12.2022
accession date

Belgium

16. Trimble NV, Ter Waarde 50. 8600 Ieper, Belgium



Signature
Jürgen Kesper
Managing Director

15.12.2022
accession date:

17. Trimble Belgium BV, Geldenaaksebaan 329, 3001 Leuven, Belgium



Signature
Ruud Kats
Director

15.12.2022
accession date

Germany

18. Trimble GmbH, Am Prime Parc 11, 65479 Raunheim, Germany

19. Müller-Elektronik GmbH, Franz-Kleine-Straße 18, 33154 Salzkotten, Germany

20. HHK Datentechnik GmbH, Hamburger Str. 277, 38114 Braunschweig, Germany

21. Stabiplan GmbH, Am Prime Parc 11, 65479 Raunheim, Germany

22. Trimble Axio-Net GmbH, Osterstraße 24, 30159 Hannover, Germany

Contact Details Thorsten Feldmann, Data Protection Officer, datenschutz@trimble.com



Signature
Jürgen Kesper
Managing Director

15.12.2022
accession date:

23. Trimble Railway GmbH, Korbacherstraße 15, 97353 Wiesentheid, Germany

Contact Details Thorsten Feldmann, Data Protection Officer, datenschutz@trimble.com



Signature
Andreas Sinning
Managing Director

15.12.2022
accession date:

Processor(s)/Importer:

1. Name: Trimble Inc. 10368 Westmoor Dr, Westminster, CO 80021, United States.
Office of Data Protection, privacy@trimble.com



Signature

James A. Kirkland
SVP, Secretary and General Counsel

15.12.2022
accession date:

B. DESCRIPTION OF TRANSFER

MODULE THREE: Transfer Controller to processor

FOR PROCESSING OF USER DATA FOR TRIMBLE'S PURPOSES		
Processing Purposes	Categories of Customer Data involved	Legal basis
Access Management, Rights, License and entitlement Management related Purposes	<ul style="list-style-type: none"> ● Master Data ● Account Related Data ● Organizational Details ● History of interactions ● Data related to visits of websites ● Type of HW and Software Used ● Use related data 	<ul style="list-style-type: none"> ● Contract Justification; or ● Justified Interest Justification.
Customer Support and Services related Purposes	<ul style="list-style-type: none"> ● Master Data ● Further Identification Data ● History of interactions ● Data related to visits of websites ● Type of HW and Software Used ● Use related data 	<ul style="list-style-type: none"> ● Contract Justification; ● Legal Obligation Justification; or ● Justified Interest Justification.
Security and Fraud Prevention-related Purposes	<ul style="list-style-type: none"> ● Master Data ● Further Identification Data ● Organizational Details ● Product Use related Details ● Used system related details 	<ul style="list-style-type: none"> ● Legal Obligation Justification; or ● Justified Interest Justification.
Marketing related Purposes	<ul style="list-style-type: none"> ● Master Data ● Further Identification Data ● Association with Organization ● Job Role ● Interest in Products and services ● History of interactions ● Use related Information ● Data related to visits of websites ● Type of HW and Software Used ● Use related data 	<ul style="list-style-type: none"> ● Contract Justification; or ● Justified Interest Justification.
Customer Relationship Management Related Purposes	<ul style="list-style-type: none"> ● Master Data ● Further Identification Data ● Association with Organization ● Job Role ● Interest in Products and services ● History of interactions ● Data related to visits of websites ● Type of HW and Software Used ● Use related data 	<ul style="list-style-type: none"> ● Contract Justification; or ● Justified Interest Justification.

Receive Payment related Purposes	<ul style="list-style-type: none"> ● Master Data ● Further Identification Data ● Bank account, credit card details 	<ul style="list-style-type: none"> ● Contract Justification; or ● Justified Interest Justification.
Product and Services Development and Related Purposes	<ul style="list-style-type: none"> ● Master Data ● Further Identification Data ● Computer Usage Data ● Organizational details ● Project Related Details 	<ul style="list-style-type: none"> ● Contract Justification

Categories of data subjects whose personal data is transferred

End Users of Trimble software and services

Categories of personal data transferred

See table above

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.

N/A

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

Continuous basis, as long as the Exporter uses the services of the importer. On a customer level, depending on the duration of the use of the Services by Customer.

Nature of the processing

Please see table above.

Purpose(s) of the data transfer and further processing

Exporter distributes software services, and/or integrates software components provided by Importer, and makes them available to end users. Exporter acts as controller for the following data: User login and contact details, software usage data and data generated by security measures. The other data inputted by end users employed and contracted by customers of Trimble, or generated by their use, does not fall under this Transfer Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The data retained by the instructions of the Controller and longest for the duration of the subscription of the customer plus 60 days.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Please see table below (Annex III)

C. COMPETENT SUPERVISORY AUTHORITY

Autoriteit Persoonsgegevens, The Hague, the Netherlands

Identify the competent supervisory authority/ies in accordance with Clause 13 . .

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

(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.

ANNEX III

LIST OF SUB-PROCESSORS

Annex III: List of Sub-Processors

Sub-Processor Name	Address	Safeguards acc. to Art. 44 - 50 GDPR	Description
Amazon Web Services, Inc.	440 Terry Ave. N., Seattle, WA 98109, USA	Data Agreement with Standard Contractual Clauses.	Processing with Infrastructure as a Service
Salesforce.com, Inc.	The Landmark, 1 Market Street, San Francisco, CA, 94105 USA	Data Agreement with Standard Contractual Clauses.	Processing with Profile Management
Microsoft, Inc	Microsoft Redmond Campus, Redmond, WA, USA	Data Agreement with Standard Contractual Clauses.	Processing with Infrastructure as a Service
Gemalto NV	Barbara Strozilaan 382, 1083HN Amsterdam, The Netherlands	Data Agreement with Standard Contractual Clauses.	Processing with Security
Google, Inc.	1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Data Agreement with Standard Contractual Clauses. DPA: https://support.google.com/analytics/answer/3379636	Processing with Analytics
The Rocket Science Group LLC, dba as Mailchimp	675 Ponce de Leon Ave NE, Suite 5000, Atlanta, GA, 30308, USA	Data Agreement with Standard Contractual Clauses.	Processing with Communication
Crowdstrike, Inc.	150 Mathilda Place, Sunnyvale, CA 94068, USA	Data Agreement with Standard Contractual Clauses.	Processing with Security

Joyent, Inc	655 Montgomery Street, Suite 1600, San Francisco, CA94111, USA	Data Agreement Standard Clauses.	Processing with Contractual	Security and Data Management
Sumo Logic, Inc.	305 Main Street, Redwood City, CA 94063, USA	Data Agreement Standard Clauses.	Processing with Contractual	Security and Data Management
Trimble Information Technology India Pvt Ltd	Lakshmi Tech Park, 5/639, Rajiv Gandhi Salai, Tirumalai Nagar, Perungudi, Chennai, Tamil Nadu 600096, India	Data Agreement Standard Clauses.	Processing with Contractual	Support and data management, Application Development, Data Entry and Management
Trimble New Zealand Ltd.	11-15 Birmingham Drive, Middleton, Christchurch 8024, New Zealand	Adequacy Decision		Support and data management, Application Development, Data Entry and Management
SendGrid, Inc.	1801 California Street, Suite 500, Denver, CO 80202, USA	Data Agreement Standard Clauses.	Processing with Contractual	
Elastic Path Software, Inc.	1400-745 Thurlow Street, Vancouver, CB, V6E OC5, Canada	Data Agreement Standard Clauses.	Processing with Contractual	Security and Data Management
Aha! Labs, Inc.	20 Gloria Cir., Menlo Park, CA 94025, USA	Data Agreement Standard Clauses.	Processing with Contractual	Product Development and Testing
DataDog Inc.	620 8th Ave, 45th Floor, New York, NY 10018, USA	Data Agreement Standard Clauses.	Processing with Contractual	Data Monitoring and Management, Security
CenterCode Inc.	23332 Mill Creek Dr # 230 Laguna Hills, CA 92653-7930, USA	Data Agreement Standard Clauses.	Processing with Contractual	Product Development and Testing
Amplitude Inc.	631 Howard St. Floor 5 San Francisco, CA 94105	Data Agreement Standard Clauses.	Processing with Contractual	Product Analytics

Trimble Authorized Resellers	See Trimble Reseller Locators at trimble.com	Dealer Agreement	Sales support, First Level Support
Gainsight Inc.	350 Bay Street, Suite 100, San Francisco, CA 94133, USA	Data Processing Agreement with Standard Contractual Clauses.	Product Analytics

2.....

Applies to UK exporters only

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

Table 1: Parties

Start date	1 May 2022	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	<p>Full legal name: See Annex 1 Processor</p> <p>Trading name (if different):</p> <p>Main address (if a company registered address): See Annex 1</p> <p>Official registration number (if any) (company number or similar identifier):</p>	<p>Full legal name: See Annex 1 Controller(s)</p> <p>Trading name (if different):</p> <p>Main address (if a company registered address): See Annex 1</p> <p>Official registration number (if any) (company number or similar identifier):</p>

Key Contact	See Annex 1 Full Name (optional): Job Title: Contact details including email:	See Annex 1 Full Name (optional): Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	<p>The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:</p> <p>Date: 15 December 2022</p>
-------------------------	--

Module	Module operation in	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2		No	No	General Authorization	30 days	
3						
4						

Table 3: Appendix Information

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Annex 1A

Annex 1B: Description of Transfer: See Annex 2B

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

Annex III: List of Sub processors (Modules 2 and 3 only):

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Neither
--	--

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.

Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
- a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
 - b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
 - c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
- a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
 - b. In Clause 2, delete the words:

"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";
 - c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";
 - d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";
 - e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"
 - f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;
 - g. References to Regulation (EU) 2018/1725 are removed;
 - h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";
 - i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";
 - j. Clause 13(a) and Part C of Annex I are not used;
 - k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";
 - l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply.”;

m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties have not agreed to change Clauses 17 and/or 18 of the Addendum EU SCCs.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

- a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
- b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

- a. its direct costs of performing its obligations under the Addendum; and/or
- b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.