Matterport™

Matterport Data Processing Addendum

Updated: April 1, 2022

This Data Processing Addendum (this "DPA") is incorporated into and forms an integral part of the Matterport Terms of Use, or one or more separate offline agreement(s), order forms or other contracts between the parties, as applicable (collectively, the "Agreement") between Matterport Inc. ("Matterport") and you ("Customer" or "you") for the purchase of Matterport Services.

Acceptance of the Terms of Use includes acceptance of this DPA. To the extent you are using the Services absent any offline agreement, you shall be deemed to have accepted this DPA and applicable Standard Contractual Clauses ("SCC") upon acceptance or execution of the applicable Terms of Use.

Scope of Addendum

The parties have agreed to enter into this DPA in an effort to ensure that adequate safeguards are put in place with respect to the protection of such personal data as required by the data protection laws. The parties acknowledge and agree that this DPA will only apply to the extent, as applicable, that (a) EU Data Protection Law applies to the processing of personal data of data subjects located in or from Customer located (or where Customer is a processor, where the relevant controller is located) in the EEA, UK, or Switzerland, (b) the PIPEDA applies to the processing of personal data of data subjects located in Canada and (c) the CCPA applies to the processing of personal data of data subjects located in the State of California, United States of America.

1 DEFINITIONS

"**Adequate Country**" means a country or territory that is recognized by the European Commission under Data Protection Law from time to time as providing adequate protection for personal data.

"**Applicable Data Protection Law**" means (i) EU Data Protection Law; and (ii) Non-EU Data Protection Law.

"**Addendum**" means the template addendum issued by the UK Information Commissioner's Office and laid before the UK Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of such addendum, effective March 21, 2022.

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., including any amendments and any implementing regulations thereto that become effective on or after the Effective Date of this DPA;

"**Controller**", "**Processor**", "**Personal Data Beach**", and **"Processing" (and "Process")** (whether or not capitalized) have the meanings ascribed to them by GDPR (as defined below) and include equivalent terms in the CCPA and other Non-EU Data Protection Law" , in each case as applicable to the Services provided by Matterport under the Agreement; provided, however, to the extent that the CCPA is applicable, the definition of "controller" includes "Business"; and the definition of "processor" includes "Service Provider", all as defined under the CCPA.

"**Controller Personal Data**" means any personal data that is provided or made available by a party to the other party under the Agreement in connection with the providing party's provision or use (as applicable) of the Services.

"**Customer Personal Data**" means all personal data provided by Customer to Matterport to enable the provision of the Services.

"**EU Data Protection Law**" means (i) the GDPR; (ii) the EU e-Privacy Directive (Directive 2002/58/EC); (iii) any national data protection laws made under or pursuant to (i) or (ii) including the UK Data Protection Law (defined below); and (iv) all other laws and regulations applicable to the processing of personal data under the Agreement within the EU, the EEA and their member states, and Switzerland.

"**Data Subject**" means an individual located within the UK, EU, or the United States who personal data is processed as a result of the aforementioned Services between the parties; provided, however, to the extent that the CCPA is applicable, the definition of "data subject" includes "Customer", as defined under the CCPA.

"**Data Subject Request**" means a request from or on behalf of a data subject relating to access to, or rectification, erasure, or data portability in respect of that person's personal data or an objection from or on behalf of a data subject to the processing of its personal data.

"**EEA**" means European Economic Area, the UK and Switzerland.

"**EU**" means the European Union.

"**GDPR**" means the General Data Protection Regulation 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, or, where applicable, the equivalent provision under Swiss data protection law.

"**Non-EU Data Protection Law**" means (i) the California Consumer Privacy Act ("CCPA"); (ii) the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"); (iii) all other laws and regulations applicable to the processing of personal data under the Agreement outside of the EU, the EEA and their member states, and Switzerland.

"**Matterport**" means Matterport and any of its Affiliates.

"**Personal data**" (weather capitalized or not) means (a) has the meaning provided in Applicable Data Protection Law in reference to residents of the EEA, Switzerland, and the UK, (b) means Personal Information as defined in the CCPA in reference to California residents, and (c) in reference to residents of other jurisdictions incorporates equivalent terms under other laws applicable to the Services.

"**Sell**" shall have the meaning assigned to it in the CCPA.

"**Services**" means the services as described in the Agreement.

"**Standard Contractual Clauses**" "**SCCs**" means (a) with respect to data transfers from the EU to third countries that are not deemed adequate jurisdictions by the European Commission Module 1 Controller-

Controller SCCs (the "C2C SCCs") and/or Module 2 Controller-Processor SCCs (the "C2P SCCs") (as applicable) approved by the European Commission, as set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as may be updated from time to time (the "EU SCCs") or, (b) with respect to data transfers from the UK, the C2C SCCs and/or the C2P SCCs as further amended by the Mandatory Clauses of the Approved Addendum, as may be updated by the UK Information Commissioner's Office from time to time (the "UK SCCs"), for so long as this DPA is effective, subject to the following: (i) only the provisions pertaining to Module One are deemed applicable under the C2C SCCs; (ii) only the provisions pertaining to Module Two are deemed applicable under the C2P SCCs; (iii) except with respect to the UK SCCs, the governing law will be as set forth in the applicable annex to the applicable SCCs.

"**UK**" means the The United Kingdom of Great Britain and Northern Ireland.

"**UK GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 , The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the EU (Withdrawal) Act of 2018.

"**UK Data Protection Law**" means 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.

2 CUSTOMERS USE OF THE SERVICES.

Matterport provides to Customer the Services pursuant to the parties Agreement. In connection with the Services, the parties anticipate that Matterport may from time-to-time process certain personal data as a Controller or Processor in respect of which Customer may be a Controller under Applicable Data Protection Law.

2.1 *Controller Services*. Controller Services as used herein shall refer to Customer's use of the Matterport Services pursuant to the Terms of Use or the Agreement, for which the parties act as independent Controllers.

2.2 *Processor Services*. Processor Services as used herein shall refer to Customer's use of the Matterport Services pursuant to the Terms of Use or the Agreement, for which Matterport acts as a Processor.

3 CONTROLLER-CONTROLLER TERMS.

3.1 Application. The Controller-Controller Terms set forth in this Section 3 will apply only in connection with Customer's use of Controller Services and Matterport's processing of personal data in connection therewith.

3.2 Independent Controllers. For purposes of Applicable Data Protection Law, each party is an independent Controller of the Controller Personal Data that it collects or Processes pursuant to the Agreement. Each party shall be individually and separately responsible for complying with the obligations that apply to it as a Controller under Applicable Data Protection Law. The parties agree that they are not joint Controllers of any Controller personal data. Each party will individually determine the

purposes and means of its Processing of Controller personal data. For purposes of the CCPA, each party is considered to be a "third party".

3.3 Obligations of the Parties. Each party shall comply with all applicable requirements of Applicable Data Privacy Laws. Each party represents and warrants at all times that: (i) it has the necessary right and authority to enter into this DPA and to perform its obligations herein; (ii) its execution and performance under this DPA and the Agreement will not violate any agreement to which it is a party; and (iii) it has provided all required information to Data Subjects including, where required, that Controller Personal Data that may be passed to third parties for the purposes of the Agreement.

3.3.1 Without limiting the foregoing, each party will maintain a publicly accessible privacy policy on its website that complies with Data Privacy Laws.

3.3.2 Each party will notify the other party in writing of any action or instruction of the other party under this DPA or the Agreement which, in its opinion, infringes Applicable Data Privacy Law.

3.3.3 Subject to this DPA, each party, acting as a Controller, may process the Controller Personal Data in accordance with, and for the purposes in, the Agreement, and may permit the disclosure of the Controller Personal Data described in the Agreement or otherwise herein for the applicable Controller Services to which Customer subscribes for the purposes described in such parties' Privacy Policy (the "Permitted Purpose"). Notwithstanding the foregoing, data obtained by a party independent of Customer's use of the Services that is the same, or similar to the Controller Personal Data described herein shall not be restricted by this Addendum, any license agreement, or any terms or conditions for such Services. For the avoidance of doubt, either party may use all Controller Personal Data collected on an aggregated or de-identified basis as set out in such parties' Privacy Policy, provided that such use does not reveal Matterport or Customer directly or indirectly.

3.3.4 The types of Controller Personal Data may include, but are not necessarily limited to, email, login credentials and username, IP address, and/or Cookie identifiers.

3.3.5 Data Subjects whose information is contained in the Controller Personal Data may include, but are not necessarily limited to, end users of the Services and/or, to the extent applicable under Applicable Data Protection Law, personal data of employees, consultants, or other contacts of a party.

3.4 **Security and Confidentiality.** Each party shall implement appropriate technical and organizational measures to protect the Controller Personal Data from unauthorized, accidental, or unlawful access, loss, disclosure, or destruction. In the event that a party suffers a personal data breach, as defined by Applicable Data Protection Law, which is known or reasonably suspected to affect Controller Personal Data, such party shall notify the other party without undue delay, but in any event within forty-eight (48) hours of such party validating same. Both parties shall cooperate in good faith to agree and take such measures as may be necessary to mitigate or remedy the effects of the personal data breach. Nothing herein prohibits either party from providing notification of the personal data breach to regulatory authorities as may be required by Applicable Data Protection Law prior to notification of the other party so long as the notifying party provides notification to the other party without undue delay. Each party shall ensure that all of its personnel who have access to and/or process Controller Personal Data are obliged to keep the Controller Personal Data confidential.

3.5 **Transfers Outside the EEA.** Where a party receiving Controller Personal Data is located in a country not recognized by the European Commission as providing an adequate level of protection for personal data within the meaning of Applicable Data Protection Law, no Controller Personal Data

processed within the EEA, by either of the parties pursuant to this DPA shall be exported outside the EEA (or transferred onward to another non-EEA location) unless such party has taken such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Without prejudice to the foregoing the parties agree to transfers outside of the EEA where they have implemented a transfer solution compliant with Applicable Data Protection Law, which for example may include: (a) where such transfer is subject to an adequacy decision by the European Commission; (b) the SCCs, set out in Schedule 1, which are incorporated herein by reference; (c) another appropriate safeguard that applies pursuant to Article 46 of the GDPR or other provisions of Applicable Data Protection Law; or (d) a derogation pursuant to Article 49 of the GDPR.

3.6 **Data Subject Requests.** Each party will process its own requests for Data Subjects to exercise their rights. With respect to objections from, or on behalf of Data Subjects to the processing of personal data that is shared between the parties, including requests to opt-out from the Sale of personal Information pursuant to CCPA, the parties will collaborate to honor such objections or opt-out requests.

3.7 Compliance Cooperation. Both parties agree to reasonably cooperate and assist each other in relation to any regulatory inquiry, complaint or investigation concerning the Controller Personal Data shared between the parties.

3.8 Data Retention. Both parties shall fulfill their obligations with regards to their respective data retention periods as stated in their respective privacy policies.

4 CONTROLLER-PROCESSOR TERMS.

4.1 Application. The Controller-Processor Terms set forth in this Section 4 will apply only in connection with Customer's use of Processor Services and Matterport's processing of personal data in connection therewith.

4.2 Role of the Parties

4.2.1 Processing *in Accordance with Applicable Data Protection Law*. With respect to personal data of Data Subjects: (a) Matterport will act as "processor" of personal data and Customer will act as a "controller" as defined by GDPR; and (b) Matterport will act as a Service Provider as defined by the CCPA. If required to process personal data by Customer, Matterport will process personal data in compliance with Applicable Data Protection Law and other laws, enactments, regulations, orders, standards, and other similar instruments binding upon it in the performance of this DPA; and if and to the extent Customer processes personal data in connection with the Services, Customer will do the same. Customer shall have sole responsibility for the accuracy, quality, and legality of personal data and the means by which Customer acquired personal data.

4.2.2 *Processing in Accordance with California Law*. In accordance with the CCPA, and with respect to personal data to which CCPA applies: (a) Matterport will not "sell" (as defined in the CCPA) any Customer Personal Data; and (b) Matterport will not collect, share, or use any Customer Personal Data except as necessary to perform Services for Customer. Matterport certifies that it understands the restrictions in this clause and will comply with them.

4.3 Obligations of the Parties.

4.3.1 *General Processing Conditions*. Matterport will only process Customer Personal Data in order to perform its obligations under the Agreement or with Customer's prior written consent. Matterport shall immediately inform Customer if it is unable to follow those instructions. The parties agree that the Agreement and DPA are deemed to be the sole Instructions. Any additional or alternate instructions must be agreed separately agreed upon by Customer and Matterport. Matterport will promptly notify Customer if, in Matterport's opinion, Customer's Instructions would not comply with Applicable Data Protection Law. Customer retains control of the Customer Personal Data and remains responsible for its compliance obligations under the Applicable Data Protection Law, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to Matterport.

4.3.2 *Details of Processing*. The subject matter, duration, nature and purpose of processing and the Customer Personal Data categories and Data Subject types, which Matterport may process to fulfil the Business Purpose of the Agreement are set forth in Schedule 2 annexed hereto and incorporated herein.

4.3.3 *Local Implementation Agreement*. If and when necessary to accommodate laws, regulations, and/or local business requirements in a particular country outside the United States, EU, the EEA and their member states, and Switzerland, the parties may enter into a Local Implementation Addendum covering additional requirements under such laws that are not already addressed in the Agreement or this DPA.

4.3.4 *Sub processing- General Authorization.* You agree that Matterport has general written authorization to appoint Sub-processors under Clause 9 of the SCCs. To the extent required by Applicable Data Protection Law, you authorize Matterport to subcontract processing of Customer Personal Data under this DPA to Sub-processors, provided that Matterport: (a) maintains an up-to-date list of its Sub-processors as may be reasonably requested by Customer from time to time; and (b) imposes data protection terms on any Sub-processor it appoints as required to protect Customer Personal Data equivalent to those imposed on Matterport in this DPA. Matterport will update its list of Sub-processors with details of any change in Sub-processors at least ten (10) days prior to any such change, thereby giving you the opportunity to object to such changes. In the event you reasonably object to a new Sub-processor, you may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Services that cannot be provided by Matterport without the use of the objected-to Sub-processor by providing Matterport with written notice provided that all amounts due under the Terms of Use shall be duly paid to Matterport.

4.4 **Security and Confidentiality.**

4.4.1 *Matterport Security Responsibilities*. Matterport will: (a) use procedural, technical, and administrative safeguards on its Services designed to ensure the confidentiality, security, integrity, availability, and privacy of Customer Personal Data when cached by the Services and in transit between Customer's data sources and target systems; and (b) protect against any unauthorized processing, loss, use, disclosure, or acquisition of or access to Customer Personal Data via the Services. A description of Matterport's security measures is set out in Schedule 3.

4.4.2 *Confidentiality of Processing*. Matterport will treat Customer Personal Data as Customer's Confidential Information (as that term is defined in the Agreement). Matterport will protect the Customer Personal Data in accordance with the confidentiality obligations under the Agreement.

4.4.3 *Audit*. Upon Customer's request and subject to the confidentiality obligations set forth in the Agreement or an appropriate NDA in the case of third parties, Matterport will make available to you a summary of its most recent third-party audits, certifications, or other similar documentation, which demonstrates its compliance with its obligations under the GDPR or UK

GDPR. Upon your written request at reasonable intervals, but not more than once per year, Matterport will provide a copy of Matterport's then most recent summaries of third-party audits or certifications or other similar documentation, as applicable, that Matterport generally makes available to its Customers at the time of such request. The parties agree that the audit rights described in Article 28 of the GDPR and, where applicable, as stipulated in the SCCs, will be satisfied by Matterport's provision of such summaries and/or reports.

4.5 **Transfers outside the EEA.**

4.5.1 Transfer Mechanism. Matterport shall not transfer the Data outside of the EEA (or transferred onward to another non-EEA location) unless it has taken such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Without prejudice to the foregoing, Customer consents to transfers outside of the EEA where Matterport has implemented a transfer solution compliant with Applicable Data Protection Law, which for example may include: (a) where such transfer is subject to an adequacy decision by the European Commission; (b) the SCCs, set out in Schedule 1, which are incorporated herein by reference; (c) another appropriate safeguard that applies pursuant to Article 46 of the GDPR or other provisions of Applicable Data Protection Law; or (d) a derogation pursuant to Article 49 of the GDPR.

4.5.2 *Personal Data Subject to the UK and Swiss Data Protection Law.* To the extent that the processing of Customer Personal Data is subject to UK or Swiss data protection laws, the UK Addendum and/or Swiss Addendum (as applicable) set out in Schedules 4. shall apply.

4.5.3 *Support for Cross-Border Transfers*. Matterport will provide Customer reasonable support to enable Customer's compliance with the requirements imposed on the transfer of Customer Personal Data to third countries with respect to data subjects located in the EEA, Switzerland, and UK.

4.6 **Data Subject Requests.** Upon request, Matterport will provide reasonable and timely assistance to Customer to enable Customer to respond to: (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including rights of access, correction, objection, erasure, and data portability, as applicable); and (b) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Customer Personal Data. If any such request, correspondence, enquiry, or complaint is made directly to Matterport, Matterport will (unless prohibited by applicable law) promptly inform Customer providing full details of the same.

4.7 **Compliance Cooperation.**

4.7.1 *Data Protection Impact Assessment*. Matterport will provide reasonable cooperation to Customer (at Customer's expense) in connection with any data protection impact assessment obligations that Customer may be required to perform under Applicable Data Protection Law, taking into account the nature of Matterport's processing and the information available to Matterport.

4.7.2 *Personal Data Breach Notification and Resolution*. (i) Notification. Matterport will notify Customer without undue delay, but in any event within forty-eight (48) hours, after Matterport's validation of a personal data breach, for which it has received notification by email to the notice email address on the signature page below, or Customer's principal contact for the Services if none is provided, and which is known or reasonably suspected to affect Customers personal data. Such notification of data breaches, if applicable, will be delivered to one or more of Customer's account

administrators or other contact information provided in the Agreement by any reasonable notification means, including via email. It is Customer's sole responsibility to ensure Customer's administrators and contacts maintain accurate contact information on the Customer account at all times. (ii) Mitigation. Matterport will further take reasonably necessary measures to remedy or mitigate the effects of the breach and will keep Customer informed of all material developments in connection with the breach. Matterport will provide reasonable information and cooperation to Customer so that Customer can fulfil any data breach reporting obligations it may have under (and in accordance with the timescales required by) applicable law. (iii) Unsuccessful Personal Data Breach. Customer agrees that an unsuccessful personal data breach will not be subject to this Section. An unsuccessful personal data breach is one that results in no unauthorized access to personal data or to any of Matterport's equipment or facilities storing Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents. (iv) No Admission. Matterport's obligation to report or respond to a personal data breach under this Section is not and will not be construed as an acknowledgment by Matterport of any fault or liability of Matterport with respect to the personal data breach.

4.8 **Data Retention.** Within thirty (30) days after a written request by Customer or the termination or expiration of the Agreement, Matterport will: (a) if requested by Customer, provide Customer with a copy of any Customer Personal Data in Matterport's possession that Customer does not already have; and (b) securely destroy all Customer Personal Data in Matterport's possession in a manner that makes such Customer Personal Data non-readable and non-retrievable. Notwithstanding the foregoing, Matterport may retain copies of Customer Personal Data: (x) to the extent Matterport has a separate legal right or obligation to retain some, or all, of the Customer Personal Data; and (y) in backup systems until the backups have been overwritten or expunged in accordance with Matterport's backup policy. Until the data is deleted or returned, Matterport shall continue to ensure compliance with its security and privacy obligations in the Agreement and this DPA.

5 ALLOCATION OF COSTS. Each party shall perform its obligations under this DPA at its own cost, except as otherwise specified herein.

6 LIABILITY. The liability of the parties under or in connection with this DPA will be subject to the exclusions and limitations of liability in the Agreement.

7 MISCELLANEOUS.

7.1 *Construction; Interpretation*. This DPA is not a standalone agreement and is only effective if an Agreement is in effect between Matterport and Customer. This DPA is part of the Agreement and is governed by its terms and conditions, including limitations of liability as set forth herein. This DPA and the Agreement are the complete and exclusive statement of the mutual understanding of the parties and supersede and cancel all previous written and oral agreements and communications relating to the subject matter hereof. Headings contained in this DPA are for convenience of reference only and do not form part of this DPA.

7.2 *Severability*. If any provision of this DPA is adjudicated invalid or unenforceable, this DPA will be amended to the minimum extent necessary to achieve, to the maximum extent possible, the same legal and commercial effect originally intended by the parties. To the extent permitted by

applicable law, the parties waive any provision of law that would render any clause of this DPA prohibited or unenforceable in any respect.

7.3 *Enforcement of Rights*. No waiver of any rights under this DPA, will be effective unless in writing signed by the parties to this DPA. The failure by either party to enforce any rights under this DPA will not be construed as a waiver of any rights of such party.

7.4 *Assignment*. This DPA may be assigned only in connection with a valid assignment pursuant to the Agreement. If the Agreement is assigned by a party in accordance with its terms, this DPA will be automatically assigned by the same party to the same assignee.

7.5 *Counterparts*. This DPA may be executed and delivered by facsimile or electronic signature and in two or more counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

7.6 *Modification*. Matterport may update the terms of this Addendum from time to time, including, but not limited to: (a) as required to comply with Applicable Data Protection Law, applicable regulation, court order, or regulatory guidance; or (c) to add new additional terms to comply with new or data protection laws or regulations. If such update will have a material adverse impact on Customer, as reasonably determined by Matterport, then Matterport will use reasonable efforts to inform Customer at least thirty (30) days (or such shorter period as may be required to comply with Applicable Data Protection Law) before the change will take effect. If Customer objects to any such change, Customer may terminate this DPA by giving written notice to Matterport within thirty (30) days of being informed by Matterport of the change.

7.7 *Control/Application of the DPA*. In the event of any conflict or discrepancy between the SCCs, the Terms of Use, the terms and conditions of this DPA, and any Agreement, the following order of precedence will apply: (a) the SCCs (where applicable), (b) this DPA, (c) any Agreement; and (d) the Terms of Use. This DPA applies only to Customer, and Matterport and does not confer any rights to any third party hereunder.

8 GOVERNING LAW. Without prejudice to the SCCs, this DPA shall be governed by and construed in accordance with the laws of the country of territory stipulated for this purpose in the Agreement and each of the parties agrees to submit to the choice of jurisdiction as stipulated in the Agreement in respect of any claim or matter arising under this DPA. If otherwise required by GDPR or Applicable Data Protection Law, this DPA will be governed by the laws of the country as set forth in the SCCs.

9 TERMINATION. This DPA will remain in full force and effect so long as: (a) any Agreement remains in effect; or (b) Matterport retains any personal data related to the Agreement in its possession or control to comply with its legal obligations.

By signing the parties agree to be bound by this DPA, and the applicable Schedules hereto, including (if applicable) the UK Addendum to the EU Commission Standard Contractual Clauses.

CUSTOMER

Signature: _____

Printed Name: _____

Title: _____

Date: _____

MATTEPORT, INC.

DocuSigned by:
Judi Otteson
0B47D4A34690484...

Signature: _____

Printed Name: Judi Otteson

Title: General Counsel

Date: 11-May-2022 | 8:32:07 AM PDT

DPA SCHEDULE 1

STANDARD CONTRACTUAL CLAUSES (SCCs)

1. Incorporation of Standard Contractual Clauses.

The Parties agree that the applicable Standard Contractual Clauses ("SCC") are hereby entered into and form of the parties DPA:

1.1 Where Matterport Processes Personal Data as a Controller pursuant to the terms of the Agreement, Matterport and its relevant Affiliates are located in non-adequacy approved third countries, and Customer and its relevant Affiliates are established in the EEA, Module 1: Transfer controller to controller, Clauses 1 to 6, 8 and 10 to 18 apply.

1.2 Where Matterport Processes Personal Data as a Processor pursuant to the terms of the Agreement, Matterport and its relevant Sub-Processor Affiliates are located in non-adequacy approved third countries, and Customer and its relevant Affiliates are established in the EEA, Module 2: Transfer controller to processor, Clauses 1 to 6 and 8 to 18 apply.

2. Standard Contractual Clause Optional Provisions

In addition to Section 1.1, where the Standard Contractual Clauses identify optional provisions (or provisions with multiple options) the following shall apply in the following manner:

2.1 Clause 7 (Docking Clause) is omitted;

2.2 In Clause 9(a) (Use of sub-processors) (Module 2 only) – Option 2 shall apply and the parties shall follow the process and timings agreed in the DPA to appoint sub-processors;

2.3 In Clause 11(a) (Redress) (Module 1, 2) – the Optional provision shall NOT apply;

2.5 In Clause 17 (Governing Law) (Module 1,2) the Parties agree that option two shall apply according to the following:

(a) where the Customer is established in the EEA, the law of the Member State in which the Customer is established, provided such Member State law allows for third-party beneficiary rights;
(b) where the Customer is established in the UK, the law of England and Wales;
(c) where the Customer is established other than in the UK or EEA, the law of the Member State in which the Customer has appointed its representative under Article 27 of the GDPR; or
(d) otherwise, the law of the Republic of Ireland.

2.6 In Clause 18 (Choice of forum and jurisdiction) (Module 1, 2) – the Parties submit themselves to the jurisdiction of the courts of that country whose law applies according to this Schedule 1.

3. Supplementary Terms to Standard Contractual Clauses

3.1 **Documentation and compliance**. For the purposes of Clause 8.9(b) – Module One and Clause 8.9(e) – Module Two the review and audit provisions in the Agreement and DPA, if applicable, shall apply.

3.2 **Notification and Transparency**.

(a) The Parties acknowledge and agree that Matterport, where required by the Standard Contractual Clauses, to notify the competent supervisory authority, shall first provide Customer with the details of the notification, permitting Customer to have prior written input into the relevant notification, where Customer so desires to do, and without delaying the timing of the notification unduly.

(b) For purposes of Clause 8.2 – Module 1, Clause 8.3 – Module 2 and Clause 15.1(a), the Parties agree and acknowledge that it may not be possible for Matterport to make the appropriate communications to data subjects and accordingly, Customer shall (following notification by the Data Importer) have the option to be the party who makes any communication to the data subject, and Vendor shall provide the level of assistance set out in the DPA.

3.3 **Liability**. For the purposes of Clause 12(a), the liability of the Parties shall be limited in accordance with the limitation of liability provisions in the Agreement.

3.5 **Signatories**. Notwithstanding the fact that the Standard Contractual Clauses are incorporated herein by reference without being signed directly, Matterport and Customer each agrees that their execution of the Agreement is deemed to constitute its execution of the Standard Contractual Clauses, and that it is duly authorized to do so on behalf of, and to contractually bind, the Data Exporter or Data Importer (as applicable) accordingly.

4. **Annexes**.

4.1 For the Purpose of Annex I of the Standard Contractual Clauses, Schedule 2 contains the specifications regarding the parties, the description of transfer, and the competent supervisory authority

4.2 For the Purpose of Annex II of the Standard Contractual Clauses, Schedule 3 contains the technical and organizational measures.

4.3 The specifications for Annex III of the Standard Contractual Clauses regarding subprocessors, are determined by the DPA.

DPA SCHEDULE 2
(SCC ANNEX I)

DETAILS OF PROCESSING

A. LIST OF PARTIES

1. Data Exporter & Data Importer:

The full name, address and contact details for the Data Exporter and Data Importer (as defined below) are set out in the Agreement; and

(a) In the case of Module 1, the data exporter and Controller is Customer and its relevant Affiliates which are established in the EEA, and the data importer and Controller is Matterport and its relevant Affiliates located in non-adequacy approved third countries;

(b) In the case of Module 2, the data exporter and Controller is Customer and its relevant Affiliates which are established in the EEA, and the data importer and Processor is Matterport and its relevant Sub-Processors located in non-adequacy approved third countries;

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects

The categories of data subjects whose personal data are transferred: Employees of Customer, as well as Customer's customers and their employees, as well as the individual recipients of marketing communications and other individuals being targets of other marketing activities of the Customer or their customers.

2. Categories of personal data

The transferred categories of personal data are: Determined by Customer's configuration of the Services, and may include name, phone number, email address, address data, IP address, device identifiers, usage data (such as interactions between a user and Matterport's online system, website or email, used browser, used operating system, referrer URL).

Moreover, Customer and Customer Affiliate may include further personal data of data subjects (in particular in unstructured form) in connection with their use the Services according to the Agreement.

3. Special categories of personal data (if applicable)

The transferred personal data includes the following special categories of data: N/A – Matterport's Terms of Use prohibits Customer from using the Services to solicit, display, store, process, send or transmit special categories of data.

The 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 are: N/A

4. Frequency of the transfer

The frequency of the transfer is: The transfer is performed on a continuous basis and is determined by Customer's configuration of the Services.

5. Subject matter and nature of the processing

The subject matter of the processing is: to provide a virtual representation of real-world physical spaces known as a digital twin, and accompanying software platform to Customer.

6. Purpose(s) of the data transfer and further processing:

The purpose/s of the data transfer and further processing is: to provide the Services to Customer pursuant to the Agreement, for technical support, issue diagnosis and error correction to ensure the efficient and proper running of the systems and to identify, analyze and resolve technical issues both generally in the provision of the Service, URL scanning for the purposes of the provision of targeted threat protection and similar service which may be provided under the Agreement.

7. Duration

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: the duration is defined in the DPA.

8. Sub-processor (if applicable)

For transfers to sub-processors, specify subject matter, nature, and duration of the processing: as stipulated in the DPA, where appropriate. The Sub-processors may have access to the Personal Data for the term of this DPA or until the service contract with the respective Sub-processor is terminated or the access by the Sub-processor has been excluded as agreed between Matterport and Customer.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with clause 13 of the SCCs
Where the data exporter is established in an EU Member State: The supervisory authority of the country in which the data exporter is established is the competent authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR: The competent supervisory authority is the Member State in which the representative is established.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) without, however, having to appoint a representative pursuant to Article 27(2) of the GDPR: The competent supervisory authority is the supervisory authority in Ireland, namely the Data Protection Commission (https://www.dataprotection.ie/).

DPA SCHEDULE 3
(SCC ANNEX II & III)

ANNEX II
MATTERPORT TECHNICAL AND ORGANIZATION SECURITY MEASURES ("TOM")

Updated: April 1, 2022

Matterport's technical and organizational security measures ("TOM") describe the controls implemented by Matterport to protect personal data and ensure the ongoing security, confidentiality, integrity, and availability of Matterport's products and services as described in any customer Agreement (the "Services").

I. Overview.

This document is a high-level overview of Matterport's TOMs. More details on the measures we implement are available upon request. Matterport reserves the right to modify or revise these TOMs at any time at its discretion without notice, provided that such modification or revision does not result in a material degradation in the protection provided for personal data that Matterport processes in providing its various Services.

Evidence of the measures implemented and maintained by Matterport described below may be provided to the customer, upon written request. Matterport will provide such evidence no more than once per year, in the form of up-to-date attestations, reports or extracts from independent bodies. Customers may also request at any time Matterport's Trust Package, which includes the most recent SOC2 Type II report, and the latest penetration testing report by visiting Matterport's Trust Center located at https://matterport.com/trust.

II. Shared Responsibility.

Matterport's TOMs apply to all standard service offerings provided by Matterport, except for those areas where the customer shares the responsibility for security and privacy TOMs.

Matterport adopts a shared responsibility model where responsibility for data security is shared between Matterport and the customer. This shared model can help relieve the customer's operational burden.

Matterport is responsible for protecting the infrastructure that runs all the Services offered within Matterport's cloud Services. This infrastructure is composed of the hardware, software, networking, and facilities that run the cloud-based Services. Matterport operates, manages, and controls the components from its host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Matterport hosts all its applications with Amazon Web Services (AWS) in a multi-tenancy environment. This allows Matterport to deploy, at scale, its code base to all its infrastructure, so the Services can serve multiple customers. Matterport currently does not support single-tenancy environments.

Customer is responsible for the management of the user accounts, and visibility of its models. Customer may have additional responsibilities depending on the type of cloud Services that a customer selects. The type of cloud Services determines the amount of configuration work the customer must perform as part of its security responsibilities.

III. Technical and Organizational Measures.

Matterport maintains the following TOM to protect personal data:

1. **Information Security Program.** Matterport will maintain organizational, management and dedicated staff responsible for the development, implementation, and maintenance of Matterport's information security program.

2. **Security Policies**. Matterport will maintain information security policies and make sure that policies and measures are regularly reviewed and amend such policies as Matterport deems reasonable to maintain protection of Services and data processed therein.

3. **Risk Management.** Matterport will assess risks related to processing of personal data and create an action plan to mitigate identified risks. Matterport will maintain risk assessment procedures for the purposes of such periodic review and assessment of risks to the Matterport organization, monitoring and maintaining compliance with Matterport policies and procedures, and reporting the condition of its information security and compliance to senior internal management.

4. **Physical Security**. AWS maintains physical and environmental security of Matterport's Infrastructure containing customer confidential information designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor, and log movement of persons into and out of Matterport facilities, and (iii) guard against environmental hazards such as heat, fire, and water damage.

5. **System and Network Security.**

- **Network Security.** Matterport will maintain network security controls such as firewalls, remote access control via virtual private networks or remote access solutions, network segmentation, and detection of unauthorized or malicious network activity via security logging and monitoring, designed to protect systems from intrusion and limit the scope of any successful attack.

- **Data Security**. Matterport will maintain data security controls which include logical segregation of data, restricted (e.g., role-based) access and monitoring, and where applicable, utilization of commercially available and industry-standard encryption technologies.

- **Encryption**. Matterport employs encrypted and authenticated remote connectivity to Matterport computing environments and customer systems. Matterport maintains a

cryptographic standard that aligns with recommendations from industry groups, government publications and other reputable standards groups. This standard is periodically reviewed, and selected technologies and ciphers may be updated in accordance with the assessed risk and market acceptance of new standards.

In-Transit Encryption. All network traffic flowing in and out of the Services data centers, including customer data, is encrypted in transit.

At-Rest Encryption. Customer data created by the customer, is encrypted at rest with 256-bit AES encryption.

6. **User Access Management**. Matterport will maintain logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review, and revoking/changing access promptly when employment terminates or changes in job functions occur).

- Password Management. Matterport will maintain password controls designed to manage and control password strength, expiration, and usage including prohibiting users from sharing passwords. Matterport shall ensure password hardening standards are in place that align with accepted industry security frameworks to ensure sufficient controls.

- Workstation Protection. Matterport will implement protections on end-user devices and monitor those devices to be in compliance with the security standard requiring screen lock timeout, malware software, firewall software, remote administration, unauthenticated file sharing, hard disk encryption and appropriate patch levels. Controls are implemented to detect and remediate workstation compliance deviations. Matterport will securely sanitize physical media intended for reuse prior to such reuse and will destroy physical media not intended for reuse.

- Media Handling. Matterport will implement protections to secure portable storage media from damage, destruction, theft or unauthorized copying and the personal data stored on portable media through encryption and secure removal of data when it is no longer needed. Additional similar measures will be implemented for mobile computing devices to protect personal data.

7. **Auditing and Logging.** Matterport will maintain system audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review. Matterport will create, protect and retain such log records to the extent needed to enable monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate information system activity, including successful and unsuccessful account logon events, account management, events, security events, object access, policy change, privileged functions, administrator account creation/deletion and other administrator activity, data deletions, data access and changes, firewall logs, and permission changes.

8. **Change Management.** Matterport will maintain change management procedures and tracking mechanisms designed to test, approve, and monitor all changes to Matterport technology and information assets. Any modifications to applications by Matterport (or a third party) that will create a major change or discontinuity – other than modifications linked to corrective maintenance – will be communicated to customers before being put into production so that customer may take the necessary measures to address any such discontinuity.

9. **Threat and Vulnerability Management.** Matterport will maintain measures meant to regularly identify, manage, assess, mitigate and/or remediate vulnerabilities within the Matterport computing environments. Measures include:

- Patch management
- Anti-virus / anti-malware
- Threat notification advisories
- Vulnerability scanning (all internal systems)
- Annual penetration testing (Internet facing systems) within remediation of identified vulnerabilities by a third-party security firm.

10. **Security Incidents**. Matterport will maintain incident response procedures designed to allow Matterport to investigate, respond to, mitigate, and notify of events related to Matterport technology and information assets. Matterport will follow documented incident response procedures to comply with applicable laws and regulations including data breach notification to any Data Controller, without undue delay, but in any event within forty-eight (48) hours, after Matterport's validation of a personal data breach known or reasonably suspected to affect customers' personal data.

11. **Business Continuity Plans.** Matterport will maintain defined business resiliency/continuity and disaster recovery procedures, as appropriate, designed to maintain service and recovery from foreseeable emergency situations or disasters, consistent with industry standard practices.

12. **Vendor Management.** Matterport maintains a formal vendor management program, including vendor security reviews for critical vendors, to ensure compliance with Matterport's information security policies. Matterport may engage and use vendors, acting as sub-processors, that access, store, or process certain customer data. Matterport maintains updated information on its sub-processors on its website at https://matterport.com/matterport-subprocessors

13. **Privacy by Design.** Matterport will incorporate Privacy by Design principles for systems and enhancements at the earliest stage of development as well as educate all employees on security and privacy annually.

14. **Security of Disposed and Retained Data.** Matterport retains operational procedures and controls for the secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Matterport possession. Matterport retains back-up data in cloud storage for seven (7) days and may retain other data in accordance with applicable laws pursuant to Matterport's internal retention policies.

ANNEX III

LIST OF SUBPROCESSORS

Data exporter authorizes the Sub-processors disclosed via the applicable hyperlink(s) below (also available in Matterport's Trust Center at http://www.matterport.com/trust) to process customer data and to provide and operate the Matterport's Services to which they have subscribed under their Agreement:

https://matterport.com/matterport-subprocessors

DPA SCHEDULE 4
UK AND SWISS ADDENDUM

1. UK ADDENDUM

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

1.1. Part 1: Tables

Table 1: Parties. DPA Schedule 2 is hereby incorporated.

Table 2: Selected SCCs, Modules and Selected Clauses. DPA Schedule 1 is hereby incorporated.

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 is set forth in DPA Schedule 2.
Annex 1B: Description of Transfer is set forth in DPA Schedule 2.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data is set forth in DPA Schedule 3.
Annex III: List of Sub processors (Modules 2 and 3 only) is as set forth in DPA Schedule 3.

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: ☐ Importer ☐x Exporter ☐ neither Party

1.2. 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, and defined in the DPA. In addition, the following terms have the following meanings:

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.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.

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 may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

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.

2. **SWISS ADDENDUM**

As stipulated in the DPA, this Swiss Addendum shall apply to any processing of Customer Personal Data subject to Swiss data protection law or to both Swiss data protection law and the GDPR.

2.1. Interpretation of this Addendum

(a) Where this Addendum uses terms that are defined in the Standard Contractual Clauses as further specified in Schedule 1 of this DPA, those terms shall have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:
– "This Addendum" means This Addendum to the Clauses.
– "Clauses" means The Standard Contractual Clauses as further specified in Schedule 1 of this DPA.
– "Swiss Data Protection Laws" means The Swiss Federal Act on Data Protection of 19 June 1992 and the Swiss Ordinance to the Swiss Federal Act on Data Protection of 14 June 1993, and any new or revised version of these laws that may enter into force from time to time.
(b) This Addendum shall be read and interpreted in the light of the provisions of Swiss Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.
(c) This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.
(d) 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.

2.2. Hierarchy. In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

2.3. Incorporation of the Clauses

(a) In relation to any processing of personal data subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the GDPR, this Addendum amends the DPA including as further specified in Schedule 1 of this DPA to the extent necessary, so they operate:

(i) for transfers made by the data exporter to the data importer, to the extent that Swiss Data Protection Laws or Swiss Data Protection Laws and the GDPR apply to the data exporter's processing when making that transfer; and

(ii) to provide appropriate safeguards for the transfers in accordance with Article 46 of the GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

(b) To the extent that any processing of personal data is exclusively subject to Swiss Data Protection Laws, the amendments to the DPA including the SCCs, as further specified in Schedule 1 of this DPA and as required by clause 2.1 of this Swiss Addendum, include (without limitation):

(i) References to the "Clauses" or the "SCCs" means this Swiss Addendum as it amends the SCCs and

(ii) Clause 6 Description of the transfer(s) is replaced with:

"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 those specified in Schedule 1 of this DPA where Swiss Data Protection Laws apply to the data exporter's processing when making that transfer."

(iii) References to "Regulation (EU) 2016/679" or "that Regulation" or ""GDPR" are replaced by "Swiss Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" or "GDPR" are replaced with the equivalent Article or Section of Swiss Data Protection Laws extent applicable.

(iv) References to Regulation (EU) 2018/1725 are removed.

(v) References to the "European Union", "Union", "EU" and "EU Member State" are all replaced with "Switzerland".

(vi) Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the Federal Data Protection and Information Commissioner (the "FDPIC") insofar as the transfers are governed by Swiss Data Protection Laws.

(vii) Clause 17 is replaced to state:

"These Clauses are governed by the laws of Switzerland insofar as the transfers are governed by Swiss Data Protection Laws".

(viii) Clause 18 is replaced to state:

"Any dispute arising from these Clauses relating to Swiss Data Protection Laws shall be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts."

Until the entry into force of the revised Swiss Data Protection Laws, the Clauses shall also protect personal data of legal entities and legal entities shall receive the same protection under the Clauses as natural persons.

2.4. To the extent that any processing of personal data is subject to both Swiss Data Protection Laws and the GDPR, the DPA including the Clauses as further specified in Schedule 1 of this DPA will apply (i) as is and (ii) additionally, to the extent that a transfer is subject to Swiss Data Protection Laws, as amended by clauses 2.1 and 2.3 of this Swiss Addendum, with the sole exception that Clause 17 of the SCCs shall not be replaced as stipulated under clause 2.3(b)(vii) of this Swiss Addendum.

Customer warrants that it has made any notifications to the FDPIC which are