

Matterport Data Processing Addendum

Last Updated: March 1, 2025

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 LLC (“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) Non-EU Data Protection Laws, as defined herein, applies to the processing of personal data of data subjects located outside of the EEA, UK or Switzerland.

1 DEFINITIONS

“Algorithmic Impact Assessment” means an assessment conducted to identify and mitigate the impact(s) of new technologies such as Artificial Intelligence System and analytics.

“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.

“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.

“AI Systems” means any software developed with techniques and approaches from the field of artificial intelligence, capable of generating outputs such as content, predictions, recommendations, or decisions that influence the environments they interact with, including systems that utilize machine learning approaches (supervised, unsupervised, and reinforcement learning), logic- and knowledge-based approaches, as well as statistical approaches.

“AI System Provider”, “AI System User”, “Deployer”, “Provider” “Importer” and “Low-Risk AI System”, (whether or not capitalized) have the meanings ascribed to them by EU AI Act (as defined below) and, in each case as applicable to the Services provided by Matterport under the Agreement.

“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, as amended by the California Privacy Rights Act of 2020 (**“CPRA”**).

“Conformity Assessment” means the process required to evaluate whether the specifications of an AI system comply with the standards outlined in the relevant EU legislation, ensuring that an AI system meets safety, quality, and performance standards before it is deployed, imported, or made available within the EU market.

“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 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 Non-EU Data Protection Laws are applicable, the definition of “controller” includes “Business”; and the definition of “processor” includes “Service Provider”, all as defined under Non-EU Data Protection Laws .

“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.

“CPA” means the Colorado Privacy Act

“CTDPA” means the Connecticut Data Protection Act

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

“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.

“EU AI Act” means the Regulation (EU) 2023/206 of the European Parliament and of the Council of 20 July 2023 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, aimed at ensuring the safe and lawful development, deployment, and use of artificial intelligence within the European Union.

“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.

“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.

“Matterport” means Matterport and any of its Affiliates.

“Non-EU Data Protection Law” means (i) CCPA; (ii) CPA; (iii) CTDPA; (iii) VCDPA; (iv) UCPA; (v) the Canadian Personal Information Protection and Electronic Documents Act (“PIPEDA”); (v) 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” (whether capitalized or not) (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 Non-EU Data Protection Laws in reference to residents of the United States or Canada, and (c) in reference to residents of other jurisdictions incorporates equivalent terms under other laws applicable to the Services.

“Sell” or **“Sale”** or **“Selling”** shall have the meaning assigned to it in the Applicable Data Protection Laws.

“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.

“UCPA” means the Consumer Privacy Act.

“UK” means the United Kingdom of Great Britain and Northern Ireland.

“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.

“**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.

“**VCDPA**” means the Virginia Consumer 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 Non-EU Data Protection Laws, 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 **Non-EU Data Protection Laws**, 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. This includes cooperation in implementing necessary transparency measures to comply with the EU AI Act for Limited Risk AI Systems, if applicable.

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 Non-EU Data Protection Laws. 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 Non-EU Data Protection. In accordance with Non-EU Data Protection, and with respect to personal data to which Non-EU Data Protection apply: (a) Matterport will not "sell" (as defined in the Applicable Non-EU Data Protection Laws) 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

4.2.3 Limited Risk AI Systems. In the event that Matterport processes personal data using Limited Risk AI Systems, as defined under the EU AI Act, Matterport shall ensure compliance with all applicable transparency obligations, including providing clear information to data subjects about the use of such AI systems and conducting Algorithmic Impact Assessments to identify and mitigate any potential risks associated with these systems.

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 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. For Limited Risk AI Systems, Matterport will implement additional transparency measures as required by the EU AI Act, if applicable.

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. For transfers involving Limited Risk AI Systems, Matterport shall ensure compliance with the EU AI Act and any additional transparency requirements for such transfers, including conducting Algorithmic Impact Assessments, if applicable.

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; and (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.

1.

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.

2.

7 MISCELLANEOUS.

3.

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 (b) 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: _____

MATTERPORT, LLC


Signature: _____
Printed Name: **Nicole Elmgart**
Director, Legal & Head of Privacy
Title: _____
Date: **2/28/2025**