SQUARESPACE, INC. 225 VARICK STREET, 12TH FLOOR, NEW YORK, NY 10014

European Economic Area Data Processing Addendum

This European Economic Area Data Processing Addendum ("EEA Data Addendum") supplements, but does not replace, the Statement of Work ("SOW") and Vendor Master Terms and Conditions ("Master Terms") entered into by and between Squarespace, Inc. ("Squarespace") and Vendor (as defined in the applicable SOW). The SOW, Master Terms and this EEA Data Addendum are, collectively, the "Agreement". In the event of a conflict between the terms and conditions of this EEA Data Addendum and the SOW or Master Terms, the terms and conditions of this EEA Data Addendum shall supersede and control, unless the SOW specifically identifies the provision(s) of the EEA Data Addendum to be amended, in which case such amended terms shall apply only to that individual SOW and not to any other SOW. Capitalized terms used but not defined herein have the meanings set forth in the SOW or Master Terms.

1. Additional Definitions

1.1. "Applicable Laws" means any state, federal or foreign law, rule or regulation applicable to the Agreement, the Services, Squarespace, or Vendor, and applicable industry standards, including those concerning privacy, data protection, confidentiality, information security, availability and integrity, or the Processing of Squarespace Data. Applicable Laws shall include, without limitation, the EU-U.S. Privacy Shield Framework and its Principles, available here: https://www.privacyshield.gov/EU-US-Framework (the "Privacy Shield"), EU Directive 95/46/EC (the "Directive") and, when effective, the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

1.2. "Authorized Employees" means Vendor's employees who have a need to know or otherwise access Squarespace Data to enable Vendor to perform its obligations under the Agreement and who have undergone background screening by Vendor.

1.3. "Authorized Persons" means (i) Authorized Employees; and (ii) Vendor's subcontractors, agents, resellers, and auditors who have a need to know or otherwise access Squarespace Data to enable Vendor to comply with the Agreement, and who are bound in writing by confidentiality obligations sufficient to protect Squarespace Data in accordance with the terms hereof.

1.4. "Highly-Sensitive Personal Information" means an (i) individual's (including, without limitation, a Squarespace employee's) government-issued identification number (including social security number, driver's license number or state-issued identified number) or email address; (ii) financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; or (iii) biometric or health data. Squarespace's business contact information is not by itself deemed to be Highly-Sensitive Personal Information.

1.5. "Incident" means a situation whereby Squarespace Data was lost with a low risk of potential harm or damage to Squarespace or its customers, employees, contractors or agents.

1.6. "Security Breach" means (i) any act or omission that compromises either the security or confidentiality of Squarespace Data or the physical, technical, administrative or organizational safeguards put in place by Vendor (or any Authorized Persons) that relate to the protection of the security or confidentiality of Squarespace Data; or (ii) receipt of a verifiable complaint in relation to the privacy practices of Vendor (or any Authorized Persons) or a breach or alleged breach of this EEA Data Addendum relating to such privacy practices.

1.7. "Squarespace Data" means any information or data provided to Vendor by or at the direction of Squarespace, or to which Vendor has access in connection with the Agreement, including, without limitation, Highly-Sensitive Personal Information. For clarity, and without limiting any of Vendor's obligations under this EEA Data Addendum, all Squarespace Data is Squarespace Property and shall be treated as Confidential Information.

1.8. "Supervisory Authority" means the U.S. Department of Commerce or any court, tribunal, or governmental or other entity that has jurisdiction, under Applicable Laws, over the Agreement, the Services, Squarespace or Vendor, including any foreign data protection authority.

1.9. "Suspected Incident" means an interruption in Vendor's systems, logs, backups, networks, servers or other electronic devices, whether or not connected to the Internet, whereby an Incident is suspected.

1.10. "Security Measures" means those measures aimed at protecting Squarespace Data against a Security Breach or other accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, and shall include without limitation: (i) limiting access of Squarespace Data to Authorized Persons; (ii) securing business facilities, data centers, paper files, servers, back-up systems and computing equipment; (iii) implementing network, device application, database and platform security; (iv) implementing authentication and access controls within media, applications, operating systems and equipment; (v) encrypting Squarespace Data transmitted over public or wireless networks; (vi) strictly segregating Squarespace Data from information of Vendor or its other customers; and (vii) implementing appropriate personnel security and integrity procedures and practices, including, without limitation, conducting background checks consistent with Applicable Laws.

2. Standard of Care

2.1. Vendor agrees to comply with this EEA Data Addendum in its collection, receipt, transmission, accessing, storage, disposal, use, disclosure, or other operation or set of operations performed upon Squarespace Data (collectively, "Processing"). Vendor shall be responsible for any Processing, whether authorized or unauthorized, of Squarespace Data while such Squarespace Data is under Vendor's control or in its possession.

2.2. Without limiting the generality of the foregoing, Vendor shall: (i) maintain all Squarespace Data in strict confidence, through implementation of appropriate Security Measures; (ii) use and disclose Squarespace Data solely and exclusively for the purposes for which the Squarespace Data, or access thereto, is provided, and not sell, rent,

transfer, distribute, make available or otherwise Process Squarespace Data for Vendor's own purposes or for the benefit of anyone other than Squarespace, in each case, without Squarespace's prior express written consent; and (iii) not, directly or indirectly, disclose Squarespace Data to any person other than Authorized Employees without Squarespace's prior express written consent. Vendor shall be responsible for the acts and omissions of Authorized Persons and any other of its subcontractors, independent contractors, and other service providers, as if those actions were its own.

3. Law; Information Security

3.1. Vendor represents and warrants that its Processing of Squarespace Data does and will comply with all Applicable Laws.

3.2. Without limiting the generality of the foregoing, Vendor represents and warrants that during the term of the Agreement, it: (i)(a) shall remain Privacy Shield certified; or (b) has read and understands, and will adhere to, all applicable provisions of the Privacy Shield in connection with Vendor's Processing of Squarespace Data; and (ii) will implement, maintain and regularly review the Security Measures in place with respect to all Squarespace Data.

3.3. Vendor represents and warrants that Vendor has previously informed Squarespace and obtained its prior express written consent to any Processing of Squarespace Data by third parties other than Authorized Employees. Upon Squarespace's request, Vendor shall promptly provide Squarespace copies of any agreements regarding the Processing of Squarespace Data.

4. Actions and Access Requests

4.1. Vendor shall assist Squarespace in the event of any action by any Supervisory Authority and in any certification or re-certification efforts by Squarespace with respect to the Privacy Shield.

4.2. Upon Squarespace's request, Vendor shall provide Squarespace with: (i) a designated contact for all privacy-related queries; and (ii) all necessary assistance in responding to any individual's claims or requests relating to Squarespace Data (including, without limitation, for correction, deletion or blocking thereof).

4.3. In the event Vendor determines that its Processing of Squarespace Data violates Applicable Laws or the Agreement, it will immediately inform Squarespace, and shall follow Squarespace's directions or instructions for immediately stopping the Processing and/or remediating such violation. Without limiting the generality of the foregoing, in the event of a change in Applicable Laws affecting the Agreement, Vendor agrees to work with Squarespace to make any amendments to Vendor's Security Measures or the Agreement as are reasonably necessary to ensure continued compliance with Applicable Laws.

5. Security Breach Procedures

5.1. In the event of a Security Breach, Vendor shall:

5.1.1. send notice of a Suspected Incident to Squarespace as soon as reasonably practical, but in any event, not more than forty-eight (48) hours after becoming aware of a Suspected Incident;

5.1.2. notify Squarespace if the Suspected Incident becomes an Incident or a Security Breach and shall describe in detail the circumstances of the Incident or Security Breach as investigated by Vendor in a written report, providing: (i) initial findings and regular updates as soon as practicable; and (ii) a final report;

5.1.3. update Squarespace of any additional discoveries regarding the Incident or Security Breach within a reasonable period of time;

5.1.4. not publicly disclose any information regarding the Suspected Incident, Incident or Security Breach without Squarespace's prior express written consent; provided that Vendor may disclose any Suspected Incident, Incident or Security Breach solely as necessary to comply with Applicable Laws; and

5.1.5. fully cooperate with Squarespace, at Vendor's expense, to draft disclosures, press releases and other communication for Squarespace to use with its customers, the public or government entities.

5.2. Vendor shall, at Vendor's expense and in accordance with Applicable Laws, use best efforts to immediately mitigate and remedy any Security Breach, and prevent any further Security Breach or recurrence thereof.

6. Audit Rights

Vendor shall maintain complete and accurate books and records consistent with generally accepted accounting practices in connection with Vendor's performance under this EEA Data Addendum. Such books and records shall include, without limitation, records relevant to any charges by Vendor, all papers, correspondence, data, information, reports, records, receipts, files and other sources of relevant information relating to the work performed by Vendor under this EEA Data Addendum. Squarespace's duly authorized representatives shall have access during regular business hours upon reasonable notice, to examine, review, audit and copy, at Squarespace's expense, all of Vendor's books and records pertaining to Vendor's provision of Services. These records shall be retained by Vendor for a period of three (3) years after the termination or expiration of the Agreement. Squarespace also reserves the right to actively test Vendor's compliance with Squarespace's security requirements, including, without limitation, security configuration (e.g., server parameters, security settings and control environment) and network perimeter controls; provided that such tests are not unreasonably disruptive to Vendor's business. Squarespace shall be responsible for

SQUARESPACE, INC. 225 VARICK STREET, 12TH FLOOR, NEW YORK, NY 10014

the costs of such tests unless Vendor is found to have inadequate security. Vendor agrees, at its expense, to make any changes requested by Squarespace to correct inadequacies discovered in such audits or tests.

7. Deletion of Squarespace Data

At any time during the term of the Agreement, at Squarespace's written request or upon the termination or expiration of the Agreement for any reason, Vendor shall, and shall instruct all Authorized Persons to, promptly and securely return to Squarespace or dispose of all copies of Squarespace Data and certify in writing to Squarespace that such actions have been taken securely. Vendor shall comply with all directions provided by Squarespace with respect to the return or disposal of Squarespace Data.

8. Termination for Convenience and Material Breach

Vendor's failure to comply with any requirement under this EEA Data Addendum is a material breach of the Agreement and in such event, Squarespace may terminate the Agreement, in whole or in part, effective immediately upon written notice to Vendor and shall receive a prorated refund of any fees paid to Vendor for Services not received.