DATA PROTECTION ADDENDUM

This Data Protection Addendum ("DPA"), is entered into as of December 10, 2020, (the "DPA Effective Date") by and between Bright Market, LLC, d/b/a FastSpring ("FastSpring") and Gemmeus d.o.o. ("Vendor"), and is subject to and incorporated into the Reseller Agreement by and between FastSpring and Vendor dated October 17, 2019, (the "Agreement"). Unless otherwise defined in this DPA, all capitalized terms shall have the meaning given to them in the Agreement.

RECITALS

WHEREAS, FastSpring and Vendor entered into the Agreement pursuant to which FastSpring agreed to act as the reseller of Vendor's Products to the general public;

WHEREAS, Vendor is providing Personal Data (as defined below) to FastSpring in order for FastSpring to sell Vendor's Products to Purchasers; and

WHEREAS, the Parties wish to set forth their obligations with respect to Personal Data.

NOW, THEREFORE, for and in consideration of the promises and mutual agreements herein, and intending to be legally bound, the parties hereby agree as follows:

1. **Definitions**

"Applicable Privacy Laws" means all privacy, security, data protection, direct marketing, and consumer protection laws, rules, requirements and regulations of any applicable jurisdiction, including without limitation EU Data Protection Laws.

"Controller" means any person or organization that alone or jointly with others determines the purposes and means of the processing of Personal Data. For the avoidance of doubt, as the reseller of Vendor's Products, FastSpring is a Controller of the Personal Data, and FastSpring is the sole Controller of any personal information FastSpring collects from a Purchaser in the process of reselling Vendor's Products.

"EU Data Protection Laws" means EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as it may be amended or replaced (including without limitation by the General Data Protection Regulation defined below) from time to time, and any applicable national laws, rules and regulations implementing the foregoing.

"General Data Protection Regulation" means 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 as of May 25, 2018.

"Permitted Purposes" means the following purposes: (a) for FastSpring to provide the FastSpring Service; (b) for FastSpring's payment and tax processes; (c) to prevent fraud; (d) for Product fulfillment; (e) to investigate and remediate Security Incidents (as defined below); (f) to enforce FastSpring's rights or perform its obligations under the Agreement; (g) to fulfill legal, regulatory, and compliance

requirements

applicable to FastSpring; (h) for FastSpring to conduct its business relationship with Vendor; and (i) any other purpose described in FastSpring's privacy statement posted at http://www.fastspring.com/privacy.php, which may be updated from time to time.

"Personal Data" means any information that can be used, directly or indirectly, alone in combination with other information, to identify a natural person, which is provided directly to FastSpring by Vendor.

"Privacy Shield" means the EU-U.S. Privacy Shield framework.

2. **Transfers of Personal Data**

2.1 Vendor represents and warrants that Vendor has obtained all applicable consents required by Applicable Privacy Laws to transfer the relevant Personal Data to FastSpring in the United States so that FastSpring may lawfully use, process, and transfer the Personal Data under Applicable Privacy Laws in connection with the Agreement.

2.2 Vendor expressly acknowledges and agrees that any Personal Data transferred from Vendor to FastSpring will be processed in the United States. For so long as Privacy Shield is recognized by the European Union as a legitimate basis for transfer of Personal Data to an entity located in the United States, FastSpring shall maintain a current Privacy Shield certification with the U.S. Department of Commerce.

2.3 Vendor expressly acknowledges and agrees that FastSpring is a Controller in relation to Personal Data of Purchasers who purchase Vendor's Products via the FastSpring Service.

3. **Processing of Personal Data**

FastSpring shall process Personal Data solely for the Permitted Purposes and in compliance with Applicable Privacy Laws. FastSpring shall treat Personal Data as confidential.

4. **Personal Data Safeguards**

4.1 FastSpring shall, at its sole expense, establish and maintain a comprehensive data security program, which will include reasonable and appropriate environmental, security, and other safeguards against the destruction, loss, alteration of, and unauthorized access to Personal Data in the possession of FastSpring and during the electronic use, transmission, storage, and destruction thereof ("Security Program"). The Security Program will include written policies and practices, including without limitation appropriate system access controls, to protect Personal Data from destruction, loss, alteration of, and unauthorized access, and restrict access to Personal Data to only those FastSpring employees needing such access to provide the FastSpring Service.

4.2 Without limiting the generality of the foregoing, the Security Program will include: (i) an organizational structure and appropriate security controls to identify and protect Personal Data in

accordance with this DPA; (ii) employee controls, such as communication of all applicable security policies, background checks, security awareness training, disciplinary processes; (iii) controls to ensure the physical safety and security of FastSpring's facilities; (iv) controls to ensure

FastSpring's security posture is maintained over time, such as patch management, backups, and incident management; (v) controls to protect access to FastSpring's systems and Personal Data, and ensure appropriate levels of access are restricted to authorized individuals, and that authentication mechanisms are appropriately protected, such as key management and access rights auditing; and (vi) controls to ensure, if applicable, that its software is securely developed, including engaging in design reviews, secure separation of development and production environments, code reviews, and quality assurance testing.

4.3 During the term of this DPA, FastSpring will use Amazon Web Services ("AWS") as its hosting provider. Although FastSpring is not permitted to directly audit or to inspect AWS' physical server location(s), AWS is ISO 27001 certified and supplies an annual SOC 2 Type II report to FastSpring.

4.4 FastSpring shall encrypt all Personal Data while in motion, including on portable devices or on portable media, consistent with industry standards and at a minimum of 256-bit encryption.

4.5 In addition to complying with any notification requirements under Applicable Privacy Laws, if FastSpring discovers or is notified of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data of data subjects from the European Union (a "Security Incident"), upon confirmation of such Security Incident, FastSpring will: (i) notify Vendor of the Security Incident; and (ii) take commercially reasonable steps to investigate and mitigate the adverse effects of the Security Incident. In addition, FastSpring will promptly (and in any event as soon as reasonably practical) (i) perform a root cause analysis and prepare a corrective action plan, (ii) provide Vendor with written reports and detailed information regarding any Security Incident, including how and when such Security Incident occurred and what actions FastSpring has taken, or intends to take to remedy such Security Incident.

5. **Audit**

FastSpring will comply with the Payment Card Industry Data Security Standard ("PCI-DSS") in providing the FastSpring Service. Upon written request from Vendor, FastSpring will provide to Vendor a PCI-DSS v3.0 Attestation of Compliance facilitated and signed by a Qualified Security Assessor firm and signed by an executive officer of FastSpring with oversight responsibility.

6. **Term and Termination**

The term of this DPA commences on the DPA Effective Date and continues until the Agreement terminates or expires. Upon termination of this DPA or the Agreement, FastSpring will retain

Personal Data in accordance with consumer disclosures (particularly with regard to any software or other subscriptions automatically renewed on an annual basis, or to comply with FastSpring's business processes and/or as necessary for FastSpring in its discretion to comply with any applicable law(s)). In the event that FastSpring does not return to Vendor the Personal Data furnished hereunder, FastSpring agrees to apply the same privacy and security protections as are required in this DPA for as long as FastSpring retains the Personal Data.

IN WITNESS WHEREOF, the parties have read this DPA and agree to be bound by it and therefore have caused it to be signed by their duly authorized representatives.

AGREED TO AND ACCEPTED BY:

BRIGHT MARKET LLC, d/b/a FASTSPRING VENDOR:

_____ By:

_____ By: _____ Beth Thorpe

Name: _____ Name: _____ Customer Support Specialist

Title:_____ Title:_____