DATA PROCESSING ADDENDUM

The parties agree to comply with the following provisions with respect to any Personal Data Processed by Bluecore for Customer in connection with the provision of the Bluecore products and services (the "Services"). References to the Agreement will be construed as including this DPA. To the extent that the terms of this DPA differ from those in the Agreement, the terms of this DPA shall control.

1. DEFINITIONS

1.1 "Agreement" means the Master Services Agreement governing the purchase of the Services from Bluecore, whether executed in writing by Customer and Bluecore, or as found at www.bluecore.com/legal and referenced thereto in the applicable SOW.

1.2 "Affiliates" means any entity which is controlled by, controls or is in common control with one of the parties.

1.3 "Bluecore" means Bluecore, Inc., a Delaware corporation, with principal offices at 116 Nassau Street, 7th Floor, New York, NY 10038.

1.4 "Customer" means the entity entering into a SOW with Bluecore, pursuant to the Agreement, for the purposes of purchasing the Bluecore Services, which is the subject of this DPA.

1.5 "Data Controller" or "Controller" means the entity which determines the purposes and means of the Processing of Personal Data; for purposes of this DPA, Customer is the Controller.

1.6 "Data Processor" or "Processor" means the entity which Processes Personal Data on behalf of the Data Controller; for purposes of this DPA, Bluecore is the Processor.

1.7 "Data Protection Laws" means all privacy and data protection laws and regulations applicable to the Processing of Personal Data under the Agreement, including, as applicable: (a) the GDPR; or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland) and applicable to the Processing of Personal Data under the Agreement.

1.8 "Data Subject" means the individual to whom Personal Data relates.

1.9 "DPA" menas this Data Processing Addendum, which applies to Customer and Bluecore.

1.10 "Effective Date" shall have the meaning ascribed to such term in Section 11.

1.11 "GDPR" means 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, and repealing Directive 95/46/EC, which shall be in force as of May 25, 2018.

1.12 "Personal Data" means any information relating to an identified or identifiable person that is subject to the Data Protection Laws as specified in Appendix 1. The types of Personal Data and categories of Data Subjects Processed under this DPA include but are not limited to the following: mobile advertising IDs, IP addresses and cookie ID's received from Customer regarding the end users of digital properties.

1.13 "Privacy Shield" means the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce.

1.14 "Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction ("Process", "Processes" and "Processed" shall have the same meaning).

1.15 "Security Breach" has the meaning set forth in Section 7 of this DPA.

1.16 "SOW" means a written order executed by Customer and Bluecore which identifies the details of the Bluecore Services being purchased by Customer.

1.17 "Sub-processor" means any sub-processor engaged by Bluecore for the Processing of Personal Data.

1.18 "Term" means the period from the Effective Date to the date the DPA is terminated in accordance with Section 10.1.

1.19 "Third Party Partner" means any entity engaged by Customer for the Processing of Personal Data.

2. PROCESSING OF PERSONAL DATA

2.1 To the extent the Services involves the Processing of Personal Data, the parties agree that Customer is the Data Controller and Bluecore is a Data Processor and that the subject matter and details of the processing of such Personal Data are described in Appendix 1. To the extent that the data protection legislation of another jurisdiction is applicable to either party's processing of data, the parties acknowledge and agree that the relevant party will comply with any obligations applicable to it under that legislation with respect to the processing of that data. Bluecore shall keep a record of all processing activities with respect to Customer's Personal Data as required under GDPR.

2.2 Each party will comply with the obligations applicable to it under the Data Protection Legislation with respect to the processing of Personal Data, including, where applicable, but not limited to providing the other party contact details for each party's Data Protection Officer which are accurate and up to date. Customer shall, in its use or receipt of the Services, Process Personal Data in accordance with the requirements of the Data Protection Laws and Customer will ensure that its instructions for the Processing of Personal Data shall comply with the Data Protection Laws. As between the parties, Customer shall have sole responsibility for determining the legal basis for processing of Personal Data and (to the extent legally required) obtain all consents from Data Subjects necessary for collection and Processing of Personal Data in the scope of the Services.

2.3 The objective of Processing of Personal Data by Bluecore is the performance of the Services pursuant to the Agreement. During the Term of the Agreement, Bluecore shall only Process Personal Data on behalf of and in accordance with the Agreement and Customer's instructions and shall treat Personal Data as Confidential Information. Customer instructs Bluecore to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement in order to provide the Services; and (ii) Processing to comply with other reasonable instructions provided by Customer where such instructions are acknowledged by Bluecore as consistent with the terms of the Agreement. Bluecore may Process Personal Data other than on the instructions of the Customer if it is mandatory under applicable law to which Bluecore is subject. In this situation Bluecore shall inform the Customer of such a requirement unless the law prohibits such notice**.**

3. RIGHTS OF DATA SUBJECTS; DATA DELETION

3.1 As the Data Controller, Customer has the primary responsibility for honoring Data Subject access requests. Bluecore shall provide reasonable and timely assistance to the Customer (at the Customer's expense) to enable the Customer to respond to: (i) any request from a Data Subject to exercise any of its rights under Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a Data Subject in connection with the processing of the Data. In the event that any such request, correspondence, enquiry or complaint is made directly to Bluecore (a "Direct Access Request"), Bluecore shall to the extent legally permitted, promptly inform the Customer providing full details of the same and, upon request, provide the Customer with contact details of the Data Subject(s). If Customer fails to respond to a Direct Access Request within 30 days, Bluecore reserves the right to take appropriate steps in its reasonable judgement to respond to such request(s).

4. BLUECORE PERSONNEL

4.1 Bluecore shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data as well as any security obligations with respect to such Data.

4.2 Bluecore will take appropriate steps to ensure compliance with the Security Measures outlined in Appendix 2 by its personnel to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that any such obligations survive the termination of that individual's engagement with Bluecore.

4.3 Bluecore shall ensure that access to Personal Data is limited to those personnel who require such access to perform the Services.

5. SUB-PROCESSORS

5.1 Customer acknowledges and agrees that Bluecore may engage third-party Sub-processors in connection with the provision of the Services. Any such Sub-processors will be permitted to obtain Personal Data only to deliver the services Bluecore has retained them to provide, and are prohibited from using Personal Data for any other purpose. Bluecore will have a written agreement with each Sub-processor and agrees that any agreement with a Sub-processor will include substantially the same data protection obligations as set out in this DPA. All data

collected by Bluecore from the front end of the website is processed by Bluecore via Google Cloud Platform.

5.2 Bluecore shall be liable for the acts and omissions of its Sub-processors to the same extent Bluecore would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

5.3 Customer acknowledges and agrees that Third Party Partners are not Sub-processors and Bluecore assumes no responsibility or liability for the acts or omissions of such Third Party Partners.

6. SECURITY; AUDIT RIGHTS; PRIVACY IMPACT ASSESSMENTS

6.1 Bluecore shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Customer's Personal Data. Bluecore will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the "Security Measures"). As described in Appendix 2, the Security Measures include measures to encrypt Personal Data; to help ensure ongoing confidentiality, integrity, availability and resilience of Bluecore's systems and services; to help restore timely access to Personal Data following an incident; and for regular testing of effectiveness. Bluecore may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

6.2 Bluecore will (taking into account the nature of the processing of Customer Personal Data and the information available to Bluecore) assist Customer in ensuring compliance with any of Customer's obligations with respect to the security of Personal Data and Personal Data breaches, including (if applicable) Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by: (a) implementing and maintaining the Security Measures in accordance with Appendix 2; and (b) complying with the terms of Section 7 of this DPA.

6.3 No more than once per year, Customer may audit Bluecore solely for the purposes of meeting its audit requirements pursuant to Article 28, Section 3(h) of the General Data Protection Regulation ("GDPR"). Any such audit may be conducted by Customer or a Customer-designated third party reasonably acceptable to Bluecore, provided that Customer shall be liable for any misappropriation or breach of confidentiality, by Customer or any such third party, of Bluecore's corporate headquarters, corporate networks or Bluecore's production systsms, in relation to the audit. Bluecore shall not be required to disclose any information, or provide access to any systems, to the extent that such disclosure or access may cause Bluecore to breach its confidentiality, violate obligations to third parties, violate regulatory requirements, or violate an order from a law enforcement agency. To request an audit, Customer must submit a detailed audit plan at least four (4) weeks in advance of the proposed audit date describing the proposed scope, duration, and start date of the audit. Audit requests must be sent to security@Bluecore.com. The auditor must execute a written confidentiality agreement acceptable to Bluecore before conducting the audit. The audit must be conducted during regular business hours, subject to Bluecore's policies, and may not unreasonably interfere with Bluecore's business activities. Any audits are at Customer's expense.

6.4 Any request for Bluecore to provide assistance with an audit is considered a separate service if such audit assistance requires the use of resources different from or in addition to those required by law. Customer shall reimburse Bluecore for any time spent for any such audit at the rates agreed to by the parties. Before the commencement of any such audit, Customer and Bluecore shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Bluecore.

6.5 All audit results are to be treated as Confidential Information under the Agreement. Customer will provide Bluecore a letter of attestation stating that all audit results have been permanently deleted or destroyed within thirty (30) days of completion of the audit. Customer shall promptly notify Bluecore with information regarding any non-compliance discovered during the course of an audit.

6.6 Data Protection Impact Assessment. Customer will provide Bluecore with reasonable cooperation and assistance needed with any Data Protection Impact Assessments, and prior consultations with Supervising Authorities, which Bluecore reasonably considers to be required for Bluecore to fulfill its legal obligations. If Customer believes or becomes aware that its Processing of Personal Data is likely to result in a high risk to the data protection rights and freedoms of any persons, it will promptly inform Bluecore and provide Bluecore with all such reasonable and timely assistance as Bluecore may require in order to conduct a Data Protection Impact Assessment and, if necessary, consult with the relevant supervisory authority.

7. SECURITY BREACH MANAGEMENT AND NOTIFICATION

7.1 If Bluecore becomes aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to any Customer Personal Data transmitted, stored or otherwise Processed on Bluecore's equipment or facilities ("Security Breach"), Bluecore will promptly notify Customer of the Security Breach. Notifications made pursuant to this section will describe, to the extent possible, details of the Security Breach, including steps taken to mitigate the potential risks and steps Bluecore recommends Customer take to address the Security Breach.

7.2 Customer agrees that an unsuccessful Security Breach attempt will not be subject to this Section. An unsuccessful Security Breach attempt is one that results in no unauthorized access to Customer Personal Data or to any of Bluecore's equipment or facilities storing Customer 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, or similar incidents.

7.3 Notification(s) of Security Breaches, if any, will be delivered to one or more of Customer's business, technical or administrative contacts by any means Bluecore selects, including via email. It is Customer's sole responsibility to ensure it maintains accurate contact information on Bluecore's support systems at all times.

7.4 Bluecore's notification of or response to a Security Breach under this Section 7 will not be construed as an acknowledgement by Bluecore of any fault or liability with respect to the Security Breach.

7.5 Bluecore shall implement reasonable technical and organizational Security Measures to provide a level of security appropriate to the risk in respect to the Customer Personal Data. As technical and organizational measures are subject to technological development, Bluecore is entitled to implement alternative measures provided they do not fall short of the level of data protection set out by Data Protection Law.

8. RETURN AND DELETION OF CUSTOMER DATA

8.1 Bluecore will enable Customer to delete Customer Data during the Term in a manner consistent with the functionality of the Services.

8.2 Bluecore will comply with written requests from the Customer to delete certain Personal Data as soon as reasonably practicable and within a maximum period of 30 days, unless Data Protection Law (or, in the case the data is not subject to Data Protection Law, applicable law) requires further storage.

8.3 On expiry of the Agreement, Customer instructs Bluecore to delete all Customer Data (including existing copies) from Bluecore's systems and discontinue processing of such Customer Data in accordance with Data Protection Law. Bluecore will comply with this instruction as soon as reasonably practicable and within a maximum period of 30 days, unless Data Protection Law (or, in the case the data is not subject to Data Protection Law, applicable law) or Google Cloud Platform publicly-posted policies and procedures require further storage or a longer deletion cycle. This requirement shall not apply to the extent that Bluecore has archived Customer Data on back-up systems so long as Bluecore securely isolates and protect such data from any further processing except to the extent required by applicable law. Without prejudice to this Section, Customer acknowledges and agrees that Customer will be responsible for exporting, before the Agreement expires, any Customer Data it wishes to retain afterwards. Notwithstanding the foregoing, the provisions of this DPA will survive the termination of this Agreement for as long as the Bluecore retains any of the Customer Personal Data.

9. CROSS-BORDER DATA TRANSFERS, PRIVACY SHIELD

9.1 Bluecore may, subject to this Section 9, store and process the relevant Customer Data in the European Economic Area and/or the United Kingdom and the United States.

9.2 Bluecore self-certified to and complies with the Privacy Shield, and Bluecore shall maintain its self-certification to and compliance with the Privacy Shield with respect to the Processing of Personal Data that is transferred from the European Economic Area, the United Kingdom or Switzerland to the United States.

10. LIABILITY

10.1 Both parties agree that their respective liability under this DPA shall be apportioned according to each parties' respective responsibility for the harm (if any) caused by each respective party.

10.2 Nothing in this Section 10 will affect the remaining terms of the Agreement relating to liability (including any specific exclusions from any limitation of liability).

11. MISCELLANEOUS

11.1 This DPA will take effect on the date it is executed by Customer and Bluecore at the bottom of this Agreement (the "Effective Date") and will remain in effect until, and automatically expire upon, the deletion of all Customer

Data by Bluecore or Customer as described in this DPA

11.2 Nothing in this DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA.

11.3 Where Customer's Affiliates are Data Controllers of the Personal Data, they may enforce the terms of this DPA against Bluecore directly.

This DPA may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one Agreement.

Appendix 1: Subject matter and details of the processing

Data importer: The data importer is Bluecore, Inc.

Data exporter: The data exporter is the Customer.

Data subjects: The Personal Data concern the following categories of Data Subjects:

The users of the data exporter's websites, mobile applications and other digital mediums and any data received from Third Party Partners as described in the MSA.

Categories of data: The Personal Data concern the following categories of data:

Data on user behavior collected through an SDK or pixels placed on the data exporter's websites, mobile applications or digital mediums, including email addresses, telephone numbers, mobile advertising identifiers, and pseudonymous identifiers of the users of the data exporter's websites, mobile applications, or digital mediums as outlined in the Agreement.

Special categories of data (if appropriate):

No special categories of data are contemplated under this DPA.

Processing operations:

The personal data transferred will be subject to the following basic processing activities:

The data importer will access, reproduce, display and store the relevant personal data in order to provide the services as set out in the Agreement made between (1) Customer and (2) Bluecore Inc. effective as of the date of execution by both parties and for no other purposes whatsoever, except as expressly provided in the Agreement.

Appendix 2: Security Measures

Bluecore Security Organization:

The Bluecore Security Organization consists of a CISO/Director of Information Security that is supported by various members of the organization including Information Technology, the Software and Production Engineering teams, the CTO, the VP of Engineering, Head of Legal, and Human Resources. Additionally, external expertise is enlisted from qualified firms as needed to bolster the capabilities of the organization. Primary responsibilities of the Bluecore Security Team include incident response, vulnerability management, architecture guidance, configuration oversight, policy management, compliance support and support of the legal, sales and customer success departments.

Security and Privacy Training Program:

Bluecore has put in place an annual security and privacy training program that includes information security basics, GDPR training and incident response training. In addition to the annual training courses that all employees must complete, the Security Team also delivers periodic educational documentation on a range of topics designed to be timely within the news and the context of Bluecore's business. Training is also completed by all new employees within two weeks of the hire date.

Ongoing Risk Assessments:

Bluecore has executed a comprehensive risk assessment that is updated on a quarterly basis, communicated with the Bluecore leadership team and drives the security budget planning and security initiatives of the organization. Frameworks employed in whole or in part as the underlying foundation of the risk assessment include ISO 27001, Risk IT (Cobit 5) and NIST 800-53a Rev 4. Additionally, while not a credit card processor, Bluecore utilize the PCI DSS standard as a reference framework for security and compliance controls as the industry in which Bluecore primarily functions adheres closely to this standard.

Security Incident Response Plan:

Bluecore has a comprehensive security incident response plan that outlines responsibilities and actions to be performed in the event of a breach of security, both physical and informational. The plan, which is closely modeled after Bluecore's non-security incident triage process, includes step-by-step procedures for denial of service situations, malicious code exposure, unauthorized access and inappropriate usage. Guidance for incident participants, based on company role, is detailed within the plan. The plan includes an incident runback, documentation requirements and guidance on forensic matters as well as communication plans.

Background Checks:

Bluecore requires extensive background checks for all employees. Background checks are outsourced to a reputable third party and managed internally by the Human Resources team. Bluecore requires all contract or temporary workers to undergo a background check sourced by the firm by which they are employed.

Encryption Policy:

Bluecore maintains a detailed encryption policy coupled with an encryption technology guide defining acceptable technologies. Encryption key access is restricted to the fewest number of custodians needed to operate. Key storage is limited to secure locations, with as little duplication or key storage instances as possible. Systems have fully implemented and documented key generation processes, key distribution processes, key storage details, periodic key change processes and key destruction processes. All new development efforts are required to use encryption technologies from the Strategic or Emerging Columns. New code implementing obsolete or transitional technologies will not be approved for deployment. All Bluecore systems use TLS for data transmission, or secured RPC connectivity between system within the Google Cloud fabric. Data is also encrypted at rest within the Google environment under the AES 256 algorithm.

System Privileges:

Each Bluecore associate is granted the minim set of systems privileges to perform their assigned job function ("Least Privilege Access"). Least Privileged Access is also employed for any privileged data, as determined by assigned responsibilities. When an associate changes roles within the company or is terminated, privileges are reassessed and modified appropriately. The HR

team is responsible for coordinating timely cancellation of privileges in the event of the termination of an employee. All privileges are reviewed on the Bluecore platforms and related tools on a quarterly basis.

Data Retention:

Bluecore maintains a detailed data retention policy for all categories of corporate data and production data stored within Bluecore's processing facilities. Business data related to Bluecore's clients and the personal data of Bluecore's clients' customers is stored for the term of the business relationship. Data for active clients is stored for 5 years prior to being purged unless an alternative retention period has been arranged with the client.

Destruction Policies:

Bluecore has strict data and device destruction policies. Before a decommissioned storage device can physically leave custody of the datacenter, it is cleaned using a multi-step process that includes two independent verifications. Devices that do not pass this wiping procedure are physically destroyed (e.g. shredded) on-premises.

Anti-Malware Software:

Bluecore uses properly configured anti-malware software as a key tool in protecting information security against evolving threats. Anti-malware detection software is constantly operating, and continually updated for all Bluecore owned or operated workstations, servers, or other computing resources that connect to Bluecore resources. Anti-malware software is configured to receive automatic updates to ensure the latest version of the signature files is installed, if applicable. All anti-malware scans are scheduled to occur automatically on at least a weekly basis. Anti-malware generates alerts to the IT team and logs detailing the occurrence of a scan as well as any findings.

Vulnerability Management Program:

Bluecore maintains a vulnerability management program aiming to identify and remediate security vulnerabilities within computing systems. This includes regular testing and record of system remediation. Toolsets used to identify vulnerabilities are maintained with up-to-date vulnerability signatures. Results of vulnerability testing are utilized to craft an annual penetration test of systems and networks perceived as high risk, high value, or demonstrating a need for further scrutiny. All newly deployed systems or systems that have experienced a high level of change will be scanned for vulnerabilities prior to production deploy. Highly orchestrated environments with appropriate change control may be exempt from pre-deployment scanning.

Intrusion Detection:

Bluecore's intrusion detection capabilities include sophisticated data processing pipelines which integrate host-based signals on individual devices, network-based signals from various monitoring points in the infrastructure, and signals from infrastructure services. Rules and machine intelligence built on top of these pipelines give operational security and operational personnel warnings of possible incidents.