Data Processing Agreement

This Data Processing Addendum ("**DPA**") sets forth the terms and conditions under which Processor may receive and process Personal Data from Customer. This DPA takes into account the nature of the processing pursuant to the Agreement and describes the appropriate technical and organizational measures undertaken by Processor in the processing of Personal Data. The Parties to this DPA hereby agree to be bound by the terms and conditions in the attached Schedules 1 (Data Processing Terms), the Appendices thereto, and 2 (Cross Border Data Transfer Mechanisms). This DPA is appended to the Agreement between the Parties.

For purposes of this DPA, the following definitions shall apply:

"**Affiliate**" means any entity controlled by, controlling, or under common control with, a Party.

"**Agreement**" means the Master Services Agreement governing the purchase of Bluecore's Services, whether executed by the Parties or the online version found at www.bluecore.com/legal, as referenced within an SOW executed by the Parties.

"**Bluecore**" means Bluecore, Inc., a Delaware corporation with offices at 44 West 18th Street, New York, NY 10011.

"**Controller**" means Customer.

"**Customer**" means the entity entering into an SOW with Bluecore, pursuant to the Agreement, for the purchase of Bluecore's Services.

"**Party**" means each of Bluecore and Customer; "**Parties**" means collectively, Bluecore and Customer.

"**Processor**" means Bluecore.

"**Services**" means Bluecore's products and services made available to Customer pursuant to an SOW.

"**SOW**" means the Statement of Work executed by the Parties for Customer's purchase of the Services.

In addition to Bluecore's obligations set out in this DPA, Bluecore will comply with the obligations of a Data Importer as set out in applicable EU Standard Contractual Clauses and UK International Data Transfer Agreement. Any reference to **Data Importer** shall be deemed to be a reference to **Bluecore, Inc. or the Processor** and any reference to **Data Exporter** or **Data Controller** shall be deemed to be a reference to **Customer** and its Affiliates. Customer hereby covenants and warrants that it has the right and authority to enter into this DPA on behalf of itself and its affiliated companies.

SCHEDULE 1
DATA PROCESSING TERMS

1. Definitions.

a. All terms used without definition in this DPA have the meanings ascribed to them: first, in the Applicable Data Protection Law; second, as applicable in Schedule 3 (Jurisdiction Specific Terms); and third, in the Agreement.

b. "**Applicable Data Protection Law**" means all applicable laws and regulations regarding the Processing of Personal Data to the extent in connection of the provision of Bluecore Services under the Agreement.

c. "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

d. "**Personal Data**" has the meaning as set forth in Applicable Data Protection Law, as it relates to data provided by Customer.

e. "**Security Breach**" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed by Bluecore.

f. "**Subprocessor**" means any processor engaged by Bluecore to process Personal Data.

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

2. Processing of Personal Data.

a. It is the intent of the Parties that, with respect to the activities described in Appendix 1, Customer and its Affiliates (or their Affiliates or clients) may act either as a controller or processor (data exporter) and Processor will be the data processor / data importer to the extent it processes such Personal Data. Customer agrees and warrants that its instructions to Processor regarding the processing of Personal Data are and shall be in accordance with the relevant provisions of Applicable Data Protection Law.

b. The subject matter and duration of the Processing of Personal Data are set out in the Agreement, which describes the provision of the Services to Customer. The nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are set forth in Appendix 1 to this DPA.

c. Customer is responsible for the accuracy, quality, and legality of the Personal Data, and the means by which Customer acquired the Personal Data.

d. The Agreement and this DPA hereby form Customer's instructions to Processor regarding: (1) the Processing of Personal Data, and (2) the transfer of such Personal Data to any country or territory, when reasonably necessary for the provision of the Services.

3. Data Protection Impact Assessment

Taking into account the nature of the Processing, Processor may provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under Applicable Data Protection Law to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Processor. Processor shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 3 of this DPA, to the extent required under Applicable Data Protection Law.

4. Rights of Data Subjects. Processor will, to the extent legally permitted, promptly notify Customer if Processor receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of processing, right to be forgotten, data portability, objection to the processing, right to opt out of the sale of their personal information, or right not to be subject to an automated individual decision making. Taking into account the nature of the Processing, Processor shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to the Data Subject's request.

5. Limited use of Personal Data & personnel. Except as otherwise set forth in the Agreement, (i) Processor will not acquire any rights in or to the Personal Data; and (ii) Processor and its Affiliates shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any

contracted Subprocessor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with applicable data protection and privacy laws, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

6. Subprocessors.

a. Bluecore shall not engage third-party Subprocessors in connection with the provision of the Services except in accordance with this Section 6. Any such Subprocessors 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 Subprocessor and agrees that any agreement with a Subprocessor will include data protection obligations no less protective than those set out in this DPA

b. Bluecore shall be liable for the acts and omissions of its Subprocessors and compliance with all the obligations of this DPA by such Subprocessors to the same extent Bluecore would be liable if performing the services of each Subprocessor directly under the terms of this DPA. To this end, Bluecore will conduct proper due diligence on all Subprocessors to ensure each Subprocess can comply with Data Protection Laws and all applicable terms and conditions of this DPA.

c. Customer acknowledges and agrees that Third Party Partners are not Subprocessors and Bluecore assumes no responsibility or liability for the acts or omissions of such Third Party Partners. Subprocessors retained by Bluecore to provide Services for Customer will at all times be deemed Subprocessors of Bluecore and shall not under any circumstance be construed or deemed to be employees or Subprocessors of Customer.

d. A list of Bluecore's authorized Subprocessors is available upon Customer's request. Bluecore may add additional Subprocessors to this list provided that it gives thirty (30) days' prior written notification of the identity of the Subprocessor to Customer and Customer does not object to the appointment within that period. In the event Customer objects to a new Subprocessor, Bluecore will use reasonable efforts to make available to Customer a change in the affected Services or recommend a commercially reasonable change to Customer's use of the affected Services to avoid Processing of Personal Data by the objected-to new Subprocessor without unreasonably burdening Customer. If Bluecore is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the Agreement and applicable SOW(s) in respect to those Services which cannot be provided by Bluecore without the use of the objected-to new Subprocessor, by providing written notice to Bluecore, without Bluecore imposing a penalty for such termination on Customer. Customer shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated Services.

7. Special categories of Personal Data. Customer (and its Affiliates) shall be solely responsible for compliance with data protection and privacy laws, as applicable to Customer (and its Affiliates), including any Personal Data that requires special handling or special categories of Personal Data such as, without limitation, that which relates to an individual's race or ethnicity, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life, or personal finances.

8. Security of Personal Data.

a. The Processor shall at a minimum implement the technical and organizational measures specified in Appendix 2 to ensure the security of the Personal Data. This includes protecting the Personal Data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the Personal Data. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the Data Subjects.

b. 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 Applicable Data Protection Law.

c. The Processor shall grant access to the Personal Data undergoing processing to members of its personnel only to the extent necessary for implementing, managing and monitoring of the Agreement. The Processor shall ensure that persons authorized to process the Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

9. Cooperation with Supervisory Authorities.

Upon Customer's request, Processor shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under Applicable Data Protection Law to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Processor. Processor shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 8 of this DPA, to the extent required under Applicable Data Protection Law. Additionally, in connection with the Supervisory Authority's request, at Customer's expense, Processor shall make reasonable efforts to acquire the reasonable cooperation and assistance of Subprocessors in providing access to relevant information needed to fulfill Customer's obligations under Applicable Data Protection Law.

10. Personal Data Breach.

a. Bluecore will notify Customer without undue delay after detecting a Security Breach.

b. Such notification shall contain, at least
   (i) a description of the nature of the Security Breach (including, where possible, the categories and approximate number of Data Subjects and data records concerned);
   (ii) the details of a contact point where more information concerning the Personal Data breach can be obtained; and
   (iii) its likely consequences and the measures taken or proposed to be taken to address the Security Breach, including to mitigate its possible adverse effects.

c. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. 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.

e. Bluecore's notification of or response to a Security Breach under this Section 10 will not be construed as an acknowledgement by Bluecore of any fault or liability with respect to the Security Breach.

11. International Transfer of Data

a. **General**. Processor will abide by the requirements of Applicable Data Protection Law regarding the international transfer of Personal Data to Processor. Solely for the provision of Services to Customer under the Agreement, Personal Data may be transferred to and stored and/or Processed in any country in which Processor or its Subprocessors operate. All applicable transfers of Personal Data shall be governed by the applicable Cross Border Data Transfer Mechanisms which the Parties hereby enter into and incorporate into this DPA as referenced in Schedule 2 (Cross Border Data Transfer Mechanisms).

12. Governmental queries. Bluecore will not disclose to any third party, any Personal Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends Bluecore a demand for sensitive Personal Data, Bluecore will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, Bluecore may provide Customer's basic contact information to the governmental body. If compelled to disclose sensitive Personal Data to a governmental body, then Bluecore will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Bluecore is legally prohibited from doing so.

13. Verification and audit. The Parties acknowledge that Customer must be able to assess Bluecore' compliance with its obligations under Applicable Data Protection Law and this DPA, insofar as Bluecore is acting as a processor on behalf of Customer**.**

a. 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 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 systems, 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. 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, if any. All reimbursement rates shall be reasonable, taking into account the resources anticipated to be expended by Bluecore.

b. 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, unless required to maintain a copy in order to comply with applicable Data Protection Laws. Customer shall promptly notify Bluecore with information regarding any non-compliance discovered during the course of an audit.

14. Return and deletion of Personal Data

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

b. 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 thirty (30) days, unless Data Protection Law (or, in the case the data is not subject to Data Protection Law, applicable law) requires further storage.

c. Within thirty (30) days of expiration of the Agreement, Bluecore shall, at Customer's option, return or delete all Personal Data (including existing copies thereof) from Bluecore's systems and discontinue processing of such Personal Data in accordance with Data Protection Law. Bluecore will comply with this instruction as soon as reasonably practicable and within a maximum period of thirty (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 Personal 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 Personal Data it wishes to retain afterwards. Notwithstanding the foregoing, the provisions of this DPA will survive the termination of the Agreement for as long as Bluecore retains any of the Customer Personal Data.

15. Liability

a. 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.

b. Notwithstanding anything to the contrary in the Agreement, in no event shall either Party's liability under this DPA exceed, in the aggregate, the total fees paid or payable by Customer to Bluecore under the Agreement during the twelve (12) months preceding the date on which the claim arose.

16. Miscellaneous

a. Nothing in this DPA shall confer any benefits or rights on any person or entity other than the Parties to this DPA, except as provided in this DPA or pursuant to Applicable Data Protection Law.

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

c. 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 TO THE DPA – DETAILS OF PROCESSING

This Appendix 1 includes details of the Processing of Controller's Personal Data

- **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 Personal 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.

- **Sensitive Information:** No sensitive 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 and for no other purposes whatsoever, except as expressly provided for in the Agreement.

- **Period of Personal Data Retention:** Provider processes Personal Data for the duration described in the Agreement.

- **Subprocessors:** A current list of Subprocessors will be provided on request.

APPENDIX 2 TO THE DPA –
TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall implement the measures outlined below to ensure an appropriate level of security for the provision of the Services.

Where applicable, this Appendix 2 will serve as Annex II to the EU Standard Contractual Clauses and UK International Data Transfer Agreement

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 encrypts all Personal Data in transit and at rest, and 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 systems 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 minimum 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 five (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 records 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 deployment. 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.

SCHEDULE 2

CROSS BORDER DATA TRANSFER MECHANISMS

1. Definitions

- "**EC**" means the European Commission
- "**EEA**" means the European Economic Area
- "**EU Standard Contractual Clauses**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.
- "**UK International Data Transfer Agreement**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.

2. Cross Border Data Transfer Mechanisms.

2.1 Order of Precedence. In the event the Services are covered by more than one Transfer Mechanism, the transfer of Personal Data will be subject to a single Transfer Mechanism in accordance with the following order of precedence: (a) the EU Standard Contractual Clauses as set forth in Section 2.2 (EU Standard Contractual Clauses) of this Schedule 2; (b) the UK International Data Transfer Agreement as set forth in Section 2.3 (UK International Data Transfer Agreement) of this Schedule 2; and, if neither (a) nor (b) is applicable, then (c) other applicable data Transfer Mechanisms permitted under Applicable Data Protection Law.

2.2 EU Standard Contractual Clauses. The Parties agree that the EU Standard Contractual Clauses will apply to Personal Data that is transferred via the Services from the EEA or Switzerland, either directly or via onward transfer, to any country or recipient outside the EEA or Switzerland that is: (a) not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for Personal Data. For data transfers from the EEA Area that are subject to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will be deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

(a) Module Two (Controller to Processor) of the EU Standard Contractual Clauses will apply where Customer is a controller of Personal Data and Bluecore is processing Personal Data.

(b) Module Three (Processor to Processor) of the EU Standard Contractual Clauses will apply where Customer is a processor of Personal Data and Bluecore is processing Personal Data.

(c) For each Module, where applicable:

(i) in Clause 7 of the EU Standard Contractual Clauses, the optional docking clause will not apply;

(ii) in Clause 9 of the EU Standard Contractual Clauses, Option 2 will apply and the time period for prior notice of Subprocessor changes will be as set forth in Section 6 (Subprocessors) of this DPA;

(iii) in Clause 11 of the EU Standard Contractual Clauses, the optional language will not apply;

(iv) in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by Irish law;

(v) in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Ireland;

(vi) in Annex I, Part A of the EU Standard Contractual Clauses:

- Data Exporter: Customer.

- Contact Details: The email address(es) designated by Customer in Customer's account via its notification preferences.

- Data Exporter Role: The Data Exporter's role is set forth in Section 2 (Processing of Personal Data) of this DPA.

- Signature and Date: By entering into the Agreement, Data Exporter is deemed to have signed these EU Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

- Data Importer: Bluecore, Inc.

- Contact details: Bluecore Privacy Team – privacy@bluecore.com.

- Data Importer Role: Data Processor.

- Signature and Date: By entering into the Agreement, Data Importer is deemed to have signed these EU Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

(vii) in Annex I, Part B of the EU Standard Contractual Clauses:

- The categories of data subjects are described in Appendix 1 (Details of Processing) of this DPA.

- The Sensitive Information transferred is described in Appendix 1 (Details of Processing) of this DPA.

- The frequency of the transfer is a continuous basis for the duration of the Agreement.

- The nature of the processing is described in Appendix 1 (Details of Processing) of this DPA.

- The purpose of the processing is described in Appendix 1 (Details of Processing) of this DPA.

- The period for which the Personal Data will be retained is described in Appendix 1 (Details of Processing) of this DPA.

- For transfers to Subprocessors, the subject matter, nature, and duration of the processing remains unchanged, and the Subprocessors are as set forth at https://bluecore.com/legal.

(viii) in Annex I, Part C of the EU Standard Contractual Clauses: The Irish Data Protection Commission will be the competent supervisory authority.

(ix) Schedule 2 (Technical and Organizational Security Measures) of this DPA serves as Annex II of the EU Standard Contractual Clauses.

2.3 UK International Data Transfer Agreement. The Parties agree that the UK International Data Transfer Agreement will apply to Personal Data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for Personal Data. For data transfers from the United Kingdom that are subject to the UK International Data Transfer Agreement, the UK International Data Transfer Agreement will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

(a) In Table 1 of the UK International Data Transfer Agreement, the Parties' details and key contact information are located in Section 2.2 (c)(vi) of this Schedule 2.

(b) In Table 2 of the UK International Data Transfer Agreement, information about the version of the Approved EU SCCs, modules and selected clauses which this UK International Data Transfer Agreement is appended to is located in Section 2.2 (EU Standard Contractual Clauses) of this Schedule 2.

(c) In Table 3 of the UK International Data Transfer Agreement:

1. The list of Parties is located in Section 2.2(c)(vi) of this Schedule 2.
2. The description of the transfer is set forth in Appendix 1 (Details of Processing) of this DPA.
3. Annex II is located in Appendix 2 (Technical and Organizational Security Measures) of this DPA.
4. The list of Subprocessors is available upon request.

(d) In Table 4 of the UK International Data Transfer Agreement, both the Importer and the exporter may end the UK International Data Transfer Agreement in accordance with the terms of the UK International Data Transfer Agreement.

2.4 Conflict. To the extent there is any conflict or inconsistency between the EU Standard Contractual Clauses or UK International Data Transfer Agreement and any other terms in this Addendum, including Schedule 3 (Jurisdiction Specific Terms), or the Agreement, the provisions of the EU Standard Contractual Clauses or UK International Data Transfer Agreement, as applicable, will prevail.

SCHEDULE 3

JURISDICTION SPECIFIC TERMS

1. Australia:

1.1 The definition of "Applicable Data Protection Law" includes the Australian Privacy Principles and the Australian Privacy Act (1988).

1.2 The definition of "Personal Data" includes "Personal Information" as defined under Applicable Data Protection Law.

1.3 The definition of "Sensitive Information" includes "Sensitive Information" as defined under Applicable Data Protection Law.

2. Brazil:

2.1 The definition of "Applicable Data Protection Law" includes the Lei Geral de Proteção de Dados (LGPD).

2.2 The definition of "Security Breach" includes a security incident that may result in any relevant risk or damage to data subjects.

2.3 The definition of "processor" includes "operator" as defined under Applicable Data Protection Law.

3. California:

3.1 The definition of "Applicable Data Protection Law" includes the California Consumer Privacy Act (CCPA) and, beginning January 1, 2023, the California Privacy Rights Act (CPRA).

3.2 The definition of "Personal Data" includes "Personal Information" as defined under Applicable Data Protection Law.

3.3 The definition of "Data Subject" includes "Consumer" as defined under Applicable Data Protection Law. Any data subject rights, as described in Section 4 (Rights of Data Subjects) of this DPA, include any Consumer rights. In regards to data subject requests, Bluecore can only verify a request from Customer and not from Customer's end user or any third party.

3.4 The definition of "controller" includes "Business" as defined under Applicable Data Protection Law.

3.5 The definition of "processor" includes "Service Provider" as defined under Applicable Data Protection Law.

3.6 Bluecore will process, retain, use, and disclose Personal Data only as necessary to provide the Services under the Agreement, which constitutes a business purpose. Bluecore agrees not to (a) sell (as defined by the CCPA) Customer's Personal Data or Customer end users' Personal Data; (b) retain, use, or disclose Customer's Personal Data for any commercial purpose (as defined by the CCPA) or other purpose other than for the specific purpose of providing the Services; or (c) retain, use, or disclose Customer's Personal Data outside of the direct business relationship between the Parties as set forth in the Agreement. Additionally, beginning January 1, 2023, Bluecore: (a) shall not share (as defined in the CPRA) Customer's Personal Data; (b) shall not combine Customer's Personal Data with other Personal Information (as defined in the CPRA) received from any other source, except as otherwise permitted by the CPRA or its regulations; (c) shall provide the same level of privacy protection as is required by the CPRA; (d) shall notify Customer promptly in writing if Bluecore makes a

determination that it can no longer meet its obligations under the CPRA; (e) grants Customer the right, upon notice, to take reasonable and appropriate steps to stop and remediate Bluecore' unauthorized use of Customer's Personal Data and to take reasonable and appropriate steps to ensure that Bluecore uses the Customer's Personal Data in a manner consistent with Customer's CPRA obligations. Bluecore certifies that it understands its obligations under Applicable Data Protection Law and this Section 3.6 and will comply with them.

3.7 Bluecore certifies that its Subprocessors, as described in Section 6 (Subprocessors) of this DPA, are Service Providers under Applicable Data Protection Law, with whom Bluecore has entered into a written contract that includes terms substantially similar to this DPA. Bluecore conducts appropriate due diligence on its Subprocessors.

3.8 Bluecore will implement and maintain reasonable security procedures and practices appropriate to the nature of the Personal Data it processes to protect the Personal Data from unauthorized or illegal access, destruction, use, modification, or disclosure as set forth in Section 8 (Security of Personal Data) of this DPA.

4. Canada:

4.1 The definition of "Applicable Data Protection Law" includes the Federal Personal Information Protection and Electronic Documents Act (PIPEDA).

4.2 Bluecore's Subprocessors, as described in Section 6 (Subprocessors) of this DPA, are third parties under Applicable Data Protection Law, with whom Bluecore has entered into a written contract that includes terms substantially similar to this DPA. Bluecore has conducted appropriate due diligence on its Subprocessors.

4.3 Bluecore will implement technical and organizational measures as set forth in Section 8 (Security of Personal Data) of this DPA.

5. European Economic Area (EEA):

5.1 The definition of "Applicable Data Protection Law" includes the General Data Protection Regulation (EU 2016/679) ("*GDPR*").

5.2 When Bluecore engages a Subprocessor under Section 6 (Subprocessors) of this DPA, it will:

(a) require any appointed Subprocessor to protect the Personal Data to the standard required by Applicable Data Protection Law, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR, and

(b) require any appointed Subprocessor to (i) agree in writing to only process Personal Data in a country that the European Union has declared to have an "adequate" level of protection or (ii) only process Personal Data on terms equivalent to the EU Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent European Union data protection authorities.

5.3 Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either Party's indemnification obligations), neither Party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other Party by a regulatory authority or governmental body in connection with such other Party's violation of the GDPR.

6. Israel:

6.1 The definition of "Applicable Data Protection Law" includes the Protection of Privacy Law (PPL).

6.2 The definition of “controller” includes “Database Owner” as defined under Applicable Data Protection Law.

6.3 The definition of “processor” includes “Holder” as defined under Applicable Data Protection Law.

6.4 Bluecore will require that any personnel authorized to process Personal Data comply with the principle of data secrecy and have been duly instructed about Applicable Data Protection Law. Such personnel sign confidentiality agreements with Bluecore in accordance with Section 5 (Limited use of Personal Data & personnel) of this DPA.

6.5 Bluecore must take sufficient steps to ensure the privacy of data subjects by implementing and maintaining the security measures as specified in Section 8 (Security of Personal Data) of this DPA and complying with the terms of the Agreement.

6.6 Bluecore must ensure that the Personal Data will not be transferred to a Subprocessor unless such Subprocessor has executed an agreement with Bluecore pursuant to Section 6 (Processors) of this DPA.

7. Japan:

7.1 The definition of “Applicable Data Protection Law” includes the Act on the Protection of Personal Information (APPI).

7.2 The definition of “Personal Data” includes “Personal Information” as defined under Applicable Data Protection Law.

7.3 The definition of “controller” includes “Business Operator” as defined under Applicable Data Protection Law. As a Business Operator, Bluecore is responsible for the handling of Personal Data in its possession.

7.4 The definition of “processor” includes a business operator entrusted by the Business Operator with the handling of Personal Data in whole or in part (also a “trustee”), as described under Applicable Data Protection Law. As a trustee, Bluecore will ensure that the use of the entrusted Personal Data is securely controlled.

8. Mexico:

8.1 The definition of “Applicable Data Protection Law” includes the Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations (FLPPIPPE).

8.2 When acting as a processor, Bluecore will:

(a) treat Personal Data in accordance with Customer’s instructions set forth in Section 2 (Processing of Personal Data) of this DPA;

(b) process Personal Data only to the extent necessary to provide the Services;

(c) implement security measures in accordance with Applicable Data Protection Law and Section 8 (Security of Personal Data) of this DPA;

(d) keep confidentiality regarding the Personal Data processed in accordance with the Agreement;

(e) delete all Personal Data in accordance with the Agreement; and

(f) only transfer Personal Data to Subprocessors in accordance with Section 6 (Subprocessors) of this DPA.

9. Singapore:

9.1 The definition of "Applicable Data Protection Law" includes the Personal Data Protection Act 2012 (PDPA).

9.2 Bluecore will process Personal Data to a standard of protection in accordance with the PDPA by implementing adequate technical and organizational measures as set forth in Section 8 (Security of Personal Data) of this DPA and complying with the terms of the Agreement.

10. Switzerland:

10.1 The definition of "Applicable Data Protection Law" includes the Swiss Federal Act on Data Protection.

10.2 When Bluecore engages a Subprocessor under Section 6 (Subprocessors) of this DPA, it will:

(a) require any appointed Subprocessor to protect the Personal Data to the standard required by Applicable Data Protection Law, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR, and

(b) require any appointed Subprocessor to (i) agree in writing to only process Personal Data in a country that the European Union has declared to have an "adequate" level of protection or (ii) only process Personal Data on terms equivalent to the EU Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent European Union data protection authorities.

11. United Kingdom (UK):

11.1 References in this DPA to GDPR will to that extent be deemed to be references to the corresponding laws of the United Kingdom (including the UK GDPR and Data Protection Act 2018).

11.2 When Bluecore engages a Subprocessor under Section 6 (Subprocessors) of this DPA, it will:

(a) require any appointed Subprocessor to protect the Personal Data to the standard required by Applicable Data Protection Law, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR; and

(b) require any appointed Subprocessor to (i) agree in writing to only process Personal Data in a country that the United Kingdom has declared to have an "adequate" level of protection or (ii) only process Personal Data on terms equivalent to the UK International Data Transfer Agreement or pursuant to a Binding Corporate Rules approval granted by competent United Kingdom data protection authorities.

11.3 Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either Party's indemnification obligations), neither Party will be responsible for any UK GDPR fines issued or levied under Article 83 of the UK GDPR against the other Party by a regulatory authority or governmental body in connection with such other Party's violation of the UK GDPR.