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

1.2 "**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.

1.3 "**Bluecore**" means Bluecore, Inc., a Delaware corporation, with principal offices at 228 Park Avenue South, PMB 24329, New York, NY 10003-1502.

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 without limitation: (a) the GDPR; (b) the Federal Data Protection Act of 19 June 1992 (Switzerland) (c) the California Consumer Privacy Act ("**CCPA**"); and (d) any any other laws, rules, or regulations applicable to the Processing of Personal Data under the Agreement.

1.8 "**Data Subject**" means an identified or identifiable natural person about whom Personal Data relates.

1.9 "**DPA**" means 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 "personal data", "personal information", and "personally identifiable information", including without limitation the types of data specified in Appendix 1, and such terms shall have the same meaning as defined by the applicable Data Protection Laws. 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**" means any accidental or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

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

1.17 "**Standard Contractual Clauses**" means the agreement attached hereto as Appendix 3 pursuant to the European Commission's decision of 5 February 2020 on Standard Contractual Clauses for the transfer of Personal Data to Processors established in third countries which do not ensure an adequate level of data protection.

1.18 "**Sub-processor**" means any sub-processor engaged by Bluecore for the Processing of Personal Data.
1.19 "**Term**" means the period from the Effective Date to the date the DPA is terminated in accordance with Section 10.1.
1.20 "**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 the Data Processor and that the subject matter and details of the processing of such Personal Data are described in Appendix 1. For purposes of the CCPA, Bluecore is a "service provider" (as such term is defined under the CCPA). The parties acknowledge and agree that each will comply with any obligations applicable to it under Data Protection Laws with respect to the processing of Personal Data. Bluecore shall keep a record of all Processing activities with respect to Customer's Personal Data in a format as required under applicable Data Protection Laws.

2.2 Each party will comply with the obligations applicable to it under the Data Protection Laws 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. However, Bluecore shall immediately inform Customer if, in its opinion, an instruction from Customer infringes Data Protection Laws. Customer shall have sole responsibility for obtaining all consents from Data Subjects where necessary under applicable Data Protection Laws for collection and Processing of Personal Data in the scope of the Services where Customer is the Controller.

2.3 During the Term of the Agreement, Bluecore shall only Process Personal Data to perform the Services to Customer and in accordance with the Agreement and Customer's instructions, and for no other purpose, and shall treat Personal Data as Confidential Information and not disclose Personal Data to any third party except as provided under this DPA. Customer instructs Bluecore to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement solely in order to provide the Services to Customer; 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, before processing such Personal Data, inform the Customer of such a requirement unless applicable law prohibits such notice**.** Under no circumstances shall Bluecore process Personal Data for its own purposes or for purposes of any third party, or create any profiles reflecting a Dataa Subject's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes, except as necessary to provide the Services solely to Customer.

2.4 Bluecore shall take no action or process any Personal Data in any way that could lead to: (i) Bluecore exceeding its role as a processor under the GDPR; (ii) Bluecore exceeding its role or losing its status as a "service provider" under CCPA; or (iii) any "sale" of Personal Information by Bluecore or Customer under the CCPA.

2.5 In the event that Bluecore will provide any Bluecore Personal Data to Customer in connection with the Services, Bluecore warrants that: (i) Bluecore's transfer of such Bluecore Personal Data is lawful under Data Protection Laws; (ii) Customer's processing of such Blueore Personal Data as contemplated by the Agreement will not violate Data Protection Laws; and 3) Bluecore has obtained all necessary consents from Data Subjects to transfer such Bluecore Personal Data to Customer.

2.6 Notwithstanding anything to the contrary in this DPA, (i) due to the nature of the Personal Data that Customer provides to Bluecore, together with all data transfers to the United States being TLS-encrypted, Bluecore believes the risk of government surveillance to the privacy of Personal Data to be very low; and (ii) Bluecore will only provide Personal Data to applicable law enforcement authorities when under strict legal compulsion.

3. RIGHTS OF DATA SUBJECTS; DATA DELETION

3.1 Bluecore shall provide reasonable and timely assistance to the Customer 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 without limitation 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 or governmental authority or regulator 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, not act directly on the Direct Access Request, and promptly inform the Customer providing full details of the same and provide the Customer with contact details of the Data Subject(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, including but not limited to the obligations in this DPA.

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 Bluecore shall not engage third-party Sub-processors in connection with the provision of the Services except in accordance with this Section 5. 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 data protection obligations no less protective than those set out in this DPA.

5.2 Bluecore shall be liable for the acts and omissions of its Sub-processors and compliance with all the obligations of this DPA by such 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. To this end, Bluecore will conduct proper due diligence on all Sub-processors to ensure each Sub-process can comply with Data Protection Laws and all applicable terms and conditions of this DPA.

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. Sub-processors retained by Bluecore to provide Services for Customer will at all times be deemed Sub-processors of Bluecore and shall not under any circumstance be construed or deemed to be employees or Sub-processors of Customer.

5.4 A list of Bluecore's authorized Sub-processors is available upon Customer's request. Bluecore may add additional Sub-processors to this list provided that it gives 30 days' prior written notification of the identity of the Sub-processor to Customer and Customer does not object to the appointment within that period. In the event Customer objects to a new Sub-processor, 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 Sub-processor 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 Sub-processor, 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.

6. SECURITY; AUDIT RIGHTS; PRIVACY IMPACT ASSESSMENTS

6.1 Bluecore shall maintain administrative, physical and technical safeguards sufficient for protection of the security, confidentiality and integrity of Customer's Personal Data. Bluecore will implement and maintain technical and organizational measures ("**Security Measures**") to protect Personal Data against a Security Breach. The Security Measures shall include, at a minimum, measures to encrypt Personal Data; to help ensure ongoing confidentiality,

integrity, availability and resilience of Bluecore's systems and services; to 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 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.

6.4 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.

6.5 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 a 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 the Data Protection Laws.

8. RETURN AND DELETION OF PERSONAL DATA

8.1 Bluecore will enable Customer to delete Personal 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 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 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 this Agreement for as long as the Bluecore retains any of the Customer Personal Data.

9. CROSS-BORDER DATA TRANSFERS; PRIVACY SHIELD; STANDARD CONTRACTUAL CLAUSES

9.1 Bluecore may, subject to this Section 9, store and process the relevant Personal 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.

9.3 The Standard Contractual Clauses set forth in Appendix 3 to this DPA apply to the Services. Bluecore enters into the Standard Contractual Clauses as data importer; Customer enters into the Standard Contractual Clauses as data exporter.

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 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.

11. MISCELLANEOUS

11.1 This DPA will take effect on the last date the applicable SOW is signed by the parties (the "**Effective Date**") and will remain in effect until, and automatically expire upon, the deletion of all Personal 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, except as provided in this DPA or pursuant to the Data Protection Laws.

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

11.4 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.

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 and for no other purposes whatsoever, except as expressly provided for 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 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 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.

Appendix 3

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

The data exporter

AND

The data importer

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) '*personal data', 'special categories of data', 'process/processing*', *'controller', 'processor', 'data subject'* and *'supervisory authority*' shall have the same meaning as in 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;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *‘the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other

unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11; and

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.