BlueSnap Data Protection Addendum

Effective date: 25 May 2018

This BlueSnap Data Protection Addendum (**"Addendum"**) is entered into by and between a BlueSnap Merchant that is currently a party to a Merchant agreement with BlueSnap (**"Merchant**") and BlueSnap, Inc. and its subsidiaries worldwide including but not limited to BlueSnap Payment Services Ltd., ("**BlueSnap**") and amends and/or supplements any Merchant agreement entered into between BlueSnap and Merchant prior to the effective date of this Addendum and any mutually-agreed upon amendments or supplements thereto (together, the **"Agreement"**). The parties agree that the EU Standard Contractual Clauses (hereafter "Standard Contractual Clauses" that shall supersede any conflicting terms in this Addendum) shall become operative as provided in this Addendum. If there is any conflict between this Addendum and the Agreement regarding BlueSnap's privacy and security obligations, the provisions of this Addendum shall control.

1. Definitions

"**Customer"** means an EEA-based customer of Merchant purchasing products and/services and in the case of an individual person is a data subject for the purposes of this Addendum.

"Customer Data" means the Personal Data that Customer provides to Merchant and which is then passed on to BlueSnap through use of the BlueSnap's payment services.

"EEA" means the European Economic Area, the European Union, plus Switzerland and, if the UK ceases to be a part of the EEA, the UK.

"EU Privacy Law" means Regulation (EU) 2106/679 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 ("GDPR") from its date of application 25 May 2018, and any legislation and/or regulation implementing or made pursuant thereto, or which amends, replaces re-enacts or consolidates.

"**Personal Data"** means any data that (a) personally identifies or may be used to personally identify a natural person, and/or (b) relates to a natural person, which either directly or indirectly, in combination with other information, is capable of identifying a natural person.

"**Merchant Party**" or "**Merchant Parties"** refers to a customer, employee, officer, director, supplier and/or contractor of Merchant or of a Merchant customer.

"**Merchant Personal Data**" means Personal Data that is disclosed to and/or shared with BlueSnap by Merchant under the Agreement;

"Processing" means any operation or set of operations that is performed on Merchant Personal Data and Customer Data whether by automatic means or otherwise, such as accessing, collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, any disclosure, including without limitation, by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Privacy Laws" means:

(i) all applicable legal requirements (federal, state, local and international laws, rules and regulations and governmental requirements) currently in effect and as they become effective, relating in any way to the privacy, confidentiality or security of Personal Data, including, but not limited to EU Privacy Law and any other laws and regulations of the EEA and their member states, applicable to the Processing of Personal Data under the Agreement;

(ii) all applicable industry standards concerning privacy, data protection, confidentiality or information security, including without limitation, the Payment Card Industry (**"PCI"**) Data Security Standard, and any other similar standards;

(iii) applicable privacy policies, statements or notices that are provided to Merchant in writing and to which Merchant has agreed to abide; and

(iv) other controls required by BlueSnap and agreed to by Merchant in writing.

"Privacy Shield" means the EU-US Privacy Shield, and the Swiss-US Privacy Shield self-certification programs operated by the U.S. Department of Commerce as approved by the European Commission and any subsequent programs updating, amending, adding to, or replacing the programs;

"Privacy Shield Principles" means the Privacy Shield Framework Principles as supplemented by the Supplemental Principles and as may be amended, superseded or replaced.

"Sub-processor" means any third party data processor engaged by BlueSnap including entities related to BlueSnap, that receive Personal Data from BlueSnap intended for processing on behalf of Merchant and in accordance with Merchant's instructions as communicated by BlueSnap and the terms of its contract with such third party.

2. With respect to EU Privacy Law:
Merchant shall be deemed to be acting as the data controller and BlueSnap as the data processor in relation to all Customer Data that is passed to or received by BlueSnap. Merchant shall be solely responsible for notifying its Customers of the use of BlueSnap for supplying payment services so as to enable Customers' payment for Merchant's goods and/or services. Merchant assumes sole responsibility for obtaining all necessary consents from its Customers for the passing of Customer Data to BlueSnap, including for the onwards transfer of Customer Data by BlueSnap to its sub-processors and transfer outside the EEA, and for ensuring that such disclosure and transfer to BlueSnap is in full accordance with EU Privacy Law.

   BlueSnap shall be deemed to be acting as the data controller for Merchant Personal Data supplied by Merchant to BlueSnap with respect to servicing Merchant, setting up account, performing merchant underwriting, conducting checks and reviews relating to KYC, anti-money laundering, identity, credit status, reference, financial status, beneficial interests, location, tax status and other related matters.

3. The subject matter of the Processing, type of Personal Data, duration of Processing, categories of data subject, persons or parties that shall be exposed to the data, and Sub-processors are as set out in Appendix 1.

4. BlueSnap shall ensure that all parties and persons employed or contracted to process Merchant Personal Data and/or Customer Data, shall be subject to a binding duty of confidentiality, and are adequately trained in accordance with the requirements of EU Privacy. BlueSnap shall ensure that its employees, contractors and Sub-processors are contractually bound not to wrongfully publish, disclose or divulge any Merchant Personal Data or Customer Data to any third party.

5. Ownership of Merchant Personal Data. Any Merchant Personal Data, in any reconfigured format, shall at all times be and remain the sole property of Merchant or the Merchant Parties, unless agreed otherwise in writing by Merchant. Any use of Merchant Personal Data and/or Customer Data is limited to the sole purpose expressly authorized by the Agreement and this Addendum.

6. BlueSnap Processing and Use of Merchant Personal Data and Customer Data.
   6.1. BlueSnap shall only process Merchant Personal Data and/or Customer Data on behalf of Merchant and in accordance with Merchant's written instructions including the Agreement and this Addendum. For avoidance of doubt, Merchant instructs BlueSnap to process Merchant Personal Data and/or Customer Data (i) in accordance with and to fulfill its obligations under its Agreement with Merchant and (ii) in accordance with other lawful and reasonable instructions as may be provided by Merchant from time to time. If BlueSnap is unable or refuses to comply with Merchant's instructions, for whatever reason, BlueSnap will inform Merchant promptly of its inability or refusal to comply. If BlueSnap's inability or refusal to comply with Merchant's instructions results in BlueSnap being unable to fulfill its obligations under the Agreement or this Addendum, Merchant is entitled to treat such inability or refusal as grounds for termination of the Agreement.
   6.2. BlueSnap agrees that it will not access or use Merchant Personal Data and/or Customer Data except as necessary to fulfill its obligations to Merchant under the Agreement or as necessary to carry out Merchant's lawful and reasonable instructions to BlueSnap with regard to Merchant Personal Data.

7. Compliance. Each party will comply with all laws, rules, and regulations applicable to it and binding on it in the performance of this Addendum, including all Privacy Laws.

8. Appropriate Security Safeguards. BlueSnap will implement and maintain appropriate technical, administrative, physical and organizational measures as set out in Appendix I to adequately safeguard and protect the security and confidentiality of Merchant Personal Data and/or Customer Data against, without limitation, accidental, unauthorized or unlawful destruction, alteration, modification, processing, disclosure, loss, or access. BlueSnap will

not materially decrease the overall security of its services during the term during which it processes Merchant Personal Data and/or Customer Data.

9. Audit. Subject to reasonable notice, BlueSnap shall enable Merchant to access and review up-to-date security certifications, attestations, reports or extracts thereof from independent bodies relating to compliance with the security requirements of this Addendum. BlueSnap shall provide Merchant an opportunity to conduct a security audit of BlueSnap's security program and systems and procedures that are applicable to the services provided by BlueSnap to Merchant. Audits will occur at most annually or following notice of a security incident. Alternatively Merchant may request in writing a copy of the most recent audit of such services conducted on behalf of BlueSnap by an independent third party security professional at Merchant's selection and expense. Merchant shall promptly provide a copy of such audit report to BlueSnap without charge. If any such audit reveals any vulnerability, BlueSnap shall take reasonable steps to correct such vulnerability at its sole cost and expense.

10. Notice to Merchant Regarding Third Party Inquiries. BlueSnap will, to the extent legally permitted, promptly notify Merchant of any security issue, inquiry, claim or complaint received by or affecting BlueSnap or any of its third party service providers and Sub-processors regarding the Processing of Merchant Personal Data or Customer Data within 48 hours of discovery, including but not limited to any incidences of data breach or suspected data breach, valid requests from any person for access to, correction, amendment or deletion of that person's Personal Data that constitutes Merchant Personal Data or Customer Data, and any communication from a regulator or data protection authority, or independent recourse mechanism that BlueSnap has elected to adopt under the Privacy Shield Framework. BlueSnap will not respond to any such inquiry, claim, or complaint without Merchant's prior written consent, unless legally required to do so and shall be entitled to inform the requesting party if consent has not been given. BlueSnap will provide reasonable cooperation and assistance to Merchant, upon Merchant's request, in responding to such inquiries, claims or complaints. Merchant shall agree in advance to reimburse BlueSnap for the costs arising from such assistance based on BlueSnap's standard customer work rates.

11. Sub-processing. Merchant agrees that BlueSnap may continue to use those Sub-processors already engaged by BlueSnap as at the effective data of this Addendum, subject to the provisions of sub-sections (i) to (iv) of this clause, and that BlueSnap may appoint Sub-processors to assist it in providing Processing, provided that such Sub-processors:
    (i) agree to act only on BlueSnap's instructions (which shall be consistent with Merchant's instructions to BlueSnap); and
    (ii) are engaged under a written agreement consistent with this Addendum; and
    (iii) agree to protect the Personal Data to a standard consistent with the requirements of this Addendum, including by implementing and maintaining appropriate technical and organizational measures to protect the Personal Data consistent with those required by the Privacy Shield Principles if appropriate and this Addendum.
    (iv) BlueSnap agrees and warrants to remain liable to Merchant for the subcontracted services of any of its direct or indirect Sub-processors under this Agreement.
    (v) BlueSnap shall maintain a list of its current Sub-processors used for Processing under this Agreement and shall update such list as necessary with details of any changes and additions. BlueSnap shall notify Merchant of any additions or changes within 7 days prior to such changes taking effect by email to the email registered to Merchant in the BlueSnap console. Merchant shall have the opportunity to object to the engagement of new Sub-processors within 30 days of the issue of such notice.The objection must be based on reasonable grounds such as Merchant establishes significant risk for the protection of Merchant Personal Data and/or Customer Data. If the parties are unable to resolve such objection then either party may terminate the Agreement on providing 30 days' written notice without penalty.

12. Return or Destruction of Merchant Personal Data, Retention of Copies
Upon Merchant's request or upon termination or expiration of the Agreement, and subject to all relevant legal requirements or credit card association requirements, BlueSnap agrees, at Merchant's option, to either deliver to Merchant or destroy in a manner that prevents Merchant Personal Data from being reconstructed, any Merchant Personal Data in BlueSnap's control or possession. Such delivery or destruction shall occur as soon as practicable

and in any event within thirty (30) business days after the effective date of such termination or the date of Merchant's request. Upon reasonable notice and if requested by Merchant, BlueSnap shall provide Merchant a certificate by an officer of compliance with this Section or written reasons why such data cannot or should not be delivered or destroyed.

BlueSnap and each Sub-processor may however retain Merchant Personal Data and/or Customer Data to the extent required by applicable laws only to the extent and for such period as required by such laws and always provided that BlueSnap shall ensure the confidentiality of all such Merchant Personal Data/Customer Data and shall ensure that such data is only processed as necessary for the purpose(s) specified in such laws and for no other purpose.

Merchant agrees that after the termination or expiration of the Agreement, Merchant Personal Data and/or Customer Data may be stored as a backup for the time needed to secure (establish, investigate or defend) Merchant's and BlueSnap's claims that may arise due to the performance of the services (for the time it takes for the claims to be barred).

13. If required under EU Privacy Law, BlueSnap shall take steps to appoint a Data Protection Officer and a representative in the European Union, and shall notify Merchant in writing within 7 days of any such appointment. BlueSnap's current representative in the European Union is BlueSnap Payment Services Limited, a company based in the UK and regulated by the Financial Conduct Authority as an authorized payments institution.

14. BlueSnap shall keep records of its processing activities in accordance with EU Privacy Law, including but not limited to Article 30 of the GDPR.

15. Nothing in this Addendum shall relieve BlueSnap or Merchant of their respective individual responsibilities and liabilities under international and/or EU Privacy Law.

16. <u>Cross-Border Transfers of Merchant Personal Data</u>.

16.1. If, in fulfilling its obligations under the Agreement or pursuant to other lawful instructions from Merchant, Merchant Personal Data and/or Customer Data must be transferred, directly or via an onward transfer, from the European Economic Area to any country that has not been recognized by the European Commission as providing an adequate level of protection for Personal Data (as described under EU Privacy Law), BlueSnap agrees to comply with either of the following in 16.2.1 or 16.2.2:

16.2.1 Execute, as an annex hereto as Appendix 2, at the written request of the Merchant, the Standard Contractual Clauses deemed by the European Commission, on the basis of Article 26(4) of the Directive, as amended or superceded, to offer adequate data protection and safeguards in relation to any transfer of Personal Data out of the European Economic Area (EEA). BlueSnap will comply with such terms of Standard Contractual Clauses as though it were the named data importer therein with respect to the Processing of Personal Data. BlueSnap agrees that the Standard Contractual Clauses shall be binding on BlueSnap as between BlueSnap and Merchant:

(a) whether Merchant is acting as a data exporter or data importer under any set of Standard Contractual Clauses, with respect to Personal Data that BlueSnap is then Processing during the course of providing Merchant services;

(b) that each affiliate of Merchant established in the EEA and Switzerland that has purchased or benefitted from BlueSnap's services or on whose behalf BlueSnap may Process Personal Data shall be covered; and

(c) that each data subject whose Personal Data is Processed by BlueSnap under the Agreement and who is entitled to make a claim against Merchant or any of its affiliates pursuant to clause 3 of the Standard Contractual Clauses shall be covered.

The Standard Contractual Clauses will prevail over this Addendum to the extent there is any conflict or inconsistency between the two; or

16.2.2 Where BlueSnap has itself self-certified to the Privacy Shield Framework, BlueSnap warrants and undertakes:

(a) to provide at least the same level of protection to the Personal Data as is required by the Privacy Shield Principles;

(b) to promptly notify Merchant if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles and in such event, to work with Merchant to promptly take reasonable and appropriate steps to stop and remediate any processing until such time as the processing meets the level of protection as is required by the Privacy Shield Principles; and

(c) at Merchant's sole election, to cease processing the Personal Data immediately if in Merchant's reasonable discretion, BlueSnap is not providing the same level of protection to the Personal Data as is required by the Privacy Shield Principles.

Notwithstanding the foregoing, BlueSnap shall not be required to carry out Section 16.2.1 or 16.2.2 above if it has adopted an alternative recognized compliance standard for the lawful transfer of personal data (as defined by the EU Privacy Law) outside the European Economic Area, such as Binding Corporate Rules.

17. **Privacy Policy.** BlueSnap shall publish on its web site and adhere to a Privacy Policy that fully conforms with all relevant requirements of EU Privacy Law.

18. **Disclosure of Addendum and Agreement**. The parties acknowledge that they may each disclose this Addendum, and any relevant privacy provisions in the agreement to the US Department of Commerce, the Federal Trade Commission, European or Swiss data protection authority, or any other judicial or regulatory body upon their request. Where BlueSnap's services are related to the processing of payment transactions, BlueSnap may also make such disclosure to relevant credit card associations and acquiring banks.

19. **Jurisdication and Law.** The parties to this Addendum submit to the choice of jurisdiction and choice of law stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity.

20. BlueSnap may propose variations to this Addendum which it reasonably considers to be necessary to address the requirements of any international or EU Privacy Law.

21. **Severance.** Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

Appendix 1

Section A:

Reason for Processing: The underwriting and due diligence reviews of Merchant and prospective affiliates in accordance with payment/financial industry standards, legal requirements relating to Know Your Customer, Anti-Money Laundering, Counter Terrorist Financing checks, and in order to provide safe secure payment transaction services to individuals, customers and businesses.

Legal Basis for Processing:
Compliance with a legal obligation
Performance of a contract
Legitimate Interest

Subject Matter of Processing: Contact information, identity documents, financial records, references, payment and payment account data

Type of Personal Data:
Including but not limited to the following:
1. Contact details (name, address, e-mail address, phone and fax contact details and associated local time zone information);
2. IT systems information (user ID and password, computer name, domain name, IP address, location, and software usage pattern tracking information i.e. cookies);
3. Where applicable financial, payment data
4. Other data: ID documents, passport data, financial records, security certificates, professional qualifications, bank/credit/personal references

Duration of Processing:
Data to be retained until cessation of BlueSnap's due diligence processes. If Merchant is retained then until cessation of contract with data subject or following Merchant's request to delete Merchant Data in respect of individual data subjects

Categories of Data Subject:
Customers, potential customers, affiliates, and personnel of Merchant

Persons or Parties Exposed to Merchant Personal Data:
Merchant's and BlueSnap's personnel, employees, contractors

List of BlueSnap Sub-processors (including relevant cloud server services):
See list at: https://home.bluesnap.com/legal/BlueSnapDPASubprocessors

Section B:

Description of the technical and organizational security measures implemented by BlueSnap February 2018

1. Information Security Program

(a) BlueSnap maintains an information security program focused on the security and integrity of Customer Data. BlueSnap's information security program includes administrative, technical and operational controls appropriate for the size of its business, the types of information it processes and the relative level of risk such information poses.

2. Personnel Security.

(a) As part of the hiring process, all employees undergo criminal background (US) and reference checks, sign NDAs committing them to protecting confidential information (including Customer Data), agree to reasonable use policies for Customer Data, and sign off on the BlueSnap Information Security Policy.
(b) During employment, continued security awareness training and education are provided annually.
(c) Following any severing of the work relationship, the employee must surrender all assets and all access is revoked.

3. Physical Security and Hosting Environment

(a) All customer data is secured and access is limited to only the systems and employees that need access to facilitate providing services to the customer.

(b) The production servers are hosted at SSAE16-audited facilities. Visual confirmation and strict sign-in procedures are executed by trained security personnel that have passed criminal background checks. Data center access is also restricted with key cards, photo ID verification and is staffed 24/7/365. The site is also monitored and recorded via color, high-resolution digital video cameras. Neither the lessor of the servers nor the facility managers have login access to the servers.
(c) The BlueSnap corporate headquarters in USA is protected by badge access and staffed by security personnel 24/7.

4. Application Security and Access Control

(a) System Administration: All access is authenticated via userID/password, sensitive systems/services are also protected with an additional 2FA authentication. All access is logged and those logs are replicated and preserved.
(b) Customer Data
Employees that need to access customer data to do their jobs may only do so under the following conditions:
There is no other way to accomplish the task
Only the minimal amount of data required is accessed
Any captured information is destroyed once no longer needed
Access is granted on a per-user basis, based on job role and requirements, and only to the appropriate level of customer data in accordance with least privilege. User authentication is controlled using multiple security factors including username, password, and 2 Factor authentication. Passwords are safeguarded and never stored in plain text, either at rest or in transit.

5. Information Security / Incident Management

(a) For Production systems, the operating system is CentOS Linux with all ports but 443 are closed to the internet at large. Critical patches are applied with urgency commensurate with the vulnerability severity. Vulnerability digests are monitored daily for new issues in any software BlueSnap relies on.
(b) Surfaces are minimized by locking down all ports accessible outside of the private network.
(c) In the event of an incident, there is an on-call engineer at all times. The process for triage, escalation, and communication are clear and documented internally.
(d) BlueSnap maintains security incident management policies and procedures. BlueSnap will promptly notify Customer in the event Company becomes aware of an actual or reasonably suspected unauthorized disclosure of Personal Data.
(e) In addition, periodic penetration tests are performed against the Production and Corporate environment to minimize the risk of exposure. Internal security reviews are conducted for all new features. A particular emphasis is placed on the OWASP Top 10.

6. Data Protection and Encryption

Https is required for all access to production services and applications that have access to customer data

7. Corporate Infrastructure Security

(a) Anti-Virus/Anti-Malware: All workstations are equipped with centrally-managed anti-malware and anti-virus software
(b) Next Generation Security agent is deployed on every desktop/laptop
(c) Wireless Networks: Wi-Fi networks is completely segregated from the corporate network.
(d) Automatic Updates: All Windows workstations are configured using Active Directory based Group Policies to automatically download and install security and related updates released by Microsoft.
(e) User Account Password Complexity: Passwords used for common login services such as Active Directory and Google Apps for Work are required to meet complexity requirements, where available, required to be changed on a regular basis.
(f) An Intrusion Prevention System is deployed in production and corporate networks
(g) Web Application Firewall is deployed in Production to defend against application attacks
(h) Host Intrusion Detection Software is deployed on every production server to alert on system file changes
(i) Data Leak Detection is deployed in email and SharePoint sites
(j) 2 Facto Authentication is deployed to protect every sensitive server/IT asset

(k) The Production network is segmented into VLANs for further isolation and protection of data and servers
(l) BlueSnap is level 1 PCI compliant which requires the following:

- Annual Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")
- Annual onsite audit and assessment by the QSA
- Quarterly network scan by an Approved Scan Vendor ("ASV")
- Proper encryption of card data at rest and in transmission

Appendix 2
EU Standard Contractual Clauses Controller to Processor (set II) or as subsequently updated or superceded

To be activated by BlueSnap in accordance with clause 16.2.1 above.