GDPR Data Processing Addendum

This Data Processing Addendum ("DPA") supplements the Agreement between 3marketeers Advertising, Inc. (3marketeers) and Customer (jointly "the Parties"), when the GDPR applies to your use of 3marketeers' Services to Process Customer Data. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the Parties including the Agreement and this DPA, the terms of this DPA will control.

1. DEFINITIONS. Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below.

1.1 "Agreement" means any agreement between 3marketeers and a specific customer under which Services are provided by 3marketeers to that customer. Such an agreement may have various titles, including but not limited to "Order Form," "Sales Order," or "Terms of Service."

1.2 "Customer" means the entity which determines the purposes and means of Processing of Customer Data. "Customer Data" means any "personal data" (as defined in GDPR) that is provided by or on behalf of Customer and Processed by 3marketeers pursuant to the Agreement.

1.3 "Data Protection Laws" means all laws and regulations, including laws and binding regulations of the European Union, the European Economic Area ("EEA") and their member states, Switzerland and the United Kingdom, and any amending or replacement legislation from time to time, applicable to the Processing of Customer Data under the Agreement.

1.4 "GDPR" means the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC.

1.5 "Permitted Purpose" means the use of the Customer Data to the extent necessary for provision of the Services by 3marketeers to the Customer.

1.6 "Security Incident" means any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of Customer Data.

1.7 "Services" means the 3marketeers services, including the services branded as BullsEye ABM Demand Generation, eTrigue Marketing Automation, and any other related services that are ordered by the Customer from 3marketeers.

3marketeers Advertising, Inc.
6399 San Ignacio Avenue
San Jose, Ca 95119

408.293.3233
408.293.2433 fax

www.3marketeers.com

1.8 “Standard Contractual Clauses” means the agreement pursuant to the European Commission decision (C(2010)593) of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC.

1.10 “Sub-processor” means any entity engaged by 3marketeers to Process Customer Data in connection with the Services.

1.11 “Supervisory Authority” means an independent public authority which is established by an EU Member State pursuant to the GDPR.

1.12 Terms such as “Data Subject,” “Processing,” “Controller,” and “Processor” shall have the meaning ascribed to them in the GDPR.

1.13 “Third-Party Services” means connections and/or links to third party websites and/or services not included in the core Services offerings identified in the Agreement, including, without limitation, via application programming interfaces.

2. DATA PROCESSING

2.1 Details of Processing

2.1.1 Subject Matter. 3marketeers’ provision of the Services to the Customer.

2.1.2 Nature and Purpose. 3marketeers will process Customer Data for the purposes of providing the Services (including administration, operations, technical and customer support), to Customer in accordance with the Terms.

2.1.3 Data Subjects. Data Subjects include the individuals about whom data is provided to 3marketeers via the Services by or at the direction of the Customer. These include:

Natural persons who submit personal data to Customer via use of the Services (including via online websites, forms, and marketing applications and email communication hosted by 3marketeers on behalf of Customer) (“Applicants”).

Natural persons who are employees, representatives, or other business contacts of the Customer.

2.1.4 Categories of Data. Data relating to individuals provided to 3marketeers via the Services, by or at the direction of Customer. The Customer may submit Customer Data to the Services, and may request for Applicants to submit Customer Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, without limitation:

Customer Data of all types that may be submitted by Applicants to the Customer via user of the Services (such as via job applications). For example: name, geographic location, age, contact details, IP address, profession, gender, employment history, employment references, salary

- and other preferences and other personal details that the data exporter solicits or desires to collect from its Applicants.

Customer Data of all types that 3marketeers may include in forms hosted on the Services for the Customer (such as may be included in a partner application, comment or feedback forms), or may be requested by Customer via customizable fields.

Contact and billing details of the Customer's employees, authorized end users, and other business contacts. For example: name, title, employer, contact information (company, email, phone, address, etc.), payment information, and other account-related data.

The Customer's users who are authorized by the Customer to access and use the Services.

2.1.5 Special Categories. Applicants may submit special categories of Customer Data to the Customer via the Services, the extent of which is determined and controlled by the Customer. For clarity, these special categories of Customer Data may include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs.

2.2 Roles of the Parties. The Parties acknowledge and agree that 3marketeers will Process the Customer Data in the capacity of a Processor and that Customer will be the Controller of the Customer Data. Customer understands that to the extent Third-Party Services are accessed, Customer serves as the Controller and the Third-Party Services are Processors, and the Third-Party Services are not Sub-processors of 3marketeers.

2.3 Customer Instructions. The Parties agree this DPA and the Agreement constitute Customer's documented instructions regarding 3marketeers' processing of Customer Data. 3marketeers will process Customer Data only in accordance with these documented instructions.

2.4 Compliance with Laws. Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR. 3marketeers is not responsible for determining the requirements of laws applicable to Customer's business or that 3marketeers' provision of the Services meet the requirements of such laws.

CUSTOMER'S OBLIGATIONS

3.1 Instructions. Customer shall warrant that the instructions it provides to 3marketeers pursuant to this DPA comply with the Data Protection Laws.

3.2 Data Subject and Supervisory Authority Requests. The Customer shall be responsible for communications and leading any efforts to comply with all requests made by Data Subjects under the Data Protection Laws, and all communications from Supervisory Authorities that relate to Customer Data, in accordance with Data Protection Laws. To the extent such requests or communications require 3marketeers' assistance, the Customer shall notify 3marketeers of the Data Subject or Supervisory Authority request.

3.3 Notice, Consent and Other Authorizations. Customer is responsible for providing the necessary notice to the Data Subjects under the Data Protection Laws. Customer is responsible for obtaining, and demonstrating evidence that it has obtained, all necessary consents, authorizations and required permissions under the Data Protection Laws in a valid manner for 3marketeers to perform the Services.

4. 3marketeers' OBLIGATIONS

4.1 Scope of Processing. 3marketeers will Process Customer Data on documented instructions from the Customer, and in such manner as is necessary for the provision of Services except as required to comply with a legal obligation to which 3marketeers is subject. If 3marketeers believes any documented instruction or additional processing instruction from Customer violates the GDPR or other Data Protection Laws, 3marketeers will inform Customer without undue delay and may suspend the performance of the Services until Customer has modified or confirmed the lawfulness of the additional processing instruction in writing. Customer acknowledges and agrees that 3marketeers is not responsible for performing legal research or for providing legal advice to Customer.

4.2 Data Subject Requests. If 3marketeers receives a request from any Data Subject made under Data Protection relating to Customer Data, 3marketeers will provide a copy of that request to the Customer within two (2) business days of receipt. 3marketeers provides Customer with tools to enable Customer to respond to a Data Subjects' requests to exercise their rights under the Data Protection Laws. To the extent Customer is unable to respond to Data Subject's request using these tools, with a manual removal link located here: https://www.3marketeers.com/html/gdpr 3marketeers will provide reasonable assistance to the Customer in responding to the request.

4.3 Supervisory Authority Requests. 3marketeers will assist Customer in addressing any communications and abiding by any advice or orders from the Supervisory Authority relating to the Customer Data.

4.4 Retention. 3marketeers will retain Customer Data only for as long as the Customer deems it necessary for the Permitted Purpose, or as required by applicable laws. At the termination of this DPA, or upon Customer's written request, 3marketeers will either destroy or return the Customer Data to the Customer, unless legal obligations require storage of the Customer Data.

4.5 Disclosure to Third Parties and Confidentiality.

4.5.1 3marketeers will not disclose the Customer Data to third parties except as permitted by this DPA or the Agreement, unless 3marketeers is required to disclose the Customer Data by applicable laws, in which case 3marketeers shall (to the extent permitted by law) notify the Customer in writing and liaise with the Customer before complying with such disclosure request.

4.5.2 3marketeers treats all Customer Data as strictly confidential and requires all employees, agents, and Sub-processors engaged in Processing the Customer Data to commit themselves

- to confidentiality, and not Process the Customer Data for any other purposes, except on instructions from Customer.

4.6 Assistance. Taking into account the nature of the Processing and the information available, 3marketeers will provide assistance to Customer in complying with its obligations under GDPR Articles 32-36 (inclusive) (which address obligations with regard to security, breach notifications, data protection impact assessments, and prior consultation). Upon request, 3marketeers will provide Customer a list of processing operations.

4.7 Security. 3marketeers will keep Customer Data confidential and implement and maintain administrative, physical, technical and organizational safeguards for the security (including protection against accidental or unlawful loss, destruction, alteration, damage, unauthorized disclosure of, or access to, Customer Data transmitted, stored or otherwise Processed), confidentiality and integrity of Customer Data as detailed in Annex 1.

5. CONTRACTING WITH SUB-PROCESSORS

5.1 General Consent. Customer agrees that 3marketeers may engage third-party Sub-processors in connection with the provision of Services, subject to compliance with the requirements below. As a condition to permitting a Sub-processor to Process Customer Data, 3marketeers will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Customer Data as those in this DPA, to the extent applicable to the nature of the Services provided by such Sub-processor. 3marketeers will provide copies of any Sub-processor agreements to Customer pursuant only upon reasonable request by Customer.

5.2 Current Sub-processor List. Customer acknowledges and agrees that 3marketeers may engage its current Sub-processors which include printers, LinkedIn validation and mail processors including the USPS.

5.3 Written Notice Via Mailing List. 3marketeers will provide Customer with notice ("New Sub-processor Notice") of the addition of any new Sub-processor to the Sub- processor List at any time during the term of the Agreement. 3marketeers will provide Customer with additional information about any Sub-processor on the Sub-processor List that Customer may reasonably request upon receipt of a New Sub-processor Notice

5.4 Customer Objection. If Customer has a reasonable basis to object to 3marketeers' use of a new Sub-processor, Customer will notify 3marketeers promptly in writing within 15 days after receipt of a New Sub-processor Notice. 3marketeers will use reasonable efforts to make available to Customer a change in the affected Services or recommend a commercially reasonable change to Customer's configuration or use of the affected Services to avoid processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If 3marketeers is unable to make available such change within a reasonable period of time, which will not exceed 30 days, Customer may terminate the portion of any Agreement relating to the Services that cannot be reasonably provided without the objected-to new Sub-processor by providing written notice to 3marketeers.

5.5 Responsibility. 3marketeers will remain responsible for its compliance with the obligations of this DPA and for any acts and omissions of its Sub-processors that cause 3marketeers to breach any of 3marketeers' obligations under this DPA.

6. SECURITY INCIDENT MANAGEMENT

6.1 Notification. 3marketeers shall, to the extent permitted by law, notify Customer without undue delay, but no later than 48 hours after becoming aware of any Security Incident.

6.2 Security Incident. 3marketeers' notification of a Security Incident to the Customer to the extent known should include: (a) the nature of the incident; (b) the date and time upon which the incident took place and was discovered; (c) the number of data subjects affected by the incident; (d) the categories of Customer Data involved; (e) the measures – such as encryption, or other technical or organizational measures – that were taken to address the incident, including measures to mitigate the possible adverse effects; (f) whether such proposed measures would result in a disproportionate effort given the nature of the incident; (g) the name and contact details of the data protection officer or other contact; and (h) a description of the likely consequences of the incident. The Customer alone may notify any public authority.

7. TRANSFERS OUTSIDE THE EUROPEAN ECONOMIC AREA

7.1 Privacy Shield. 3marketeers complies with the terms of the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, and is Privacy Shield self-certified. That certification will serve as the transfer mechanisms for any Customer transfers of Customer Data under this DPA to 3marketeers from the EEA, Switzerland or the United Kingdom to the United States. The Parties acknowledge and agree that on the request of the United States Department of Commerce (or any successor body) or a competent supervisory authority, enforcement or other public or regulatory authority, court or tribunal, 3marketeers may make available to them a summary or representative copy of this DPA or any relevant provisions in the Agreement.

7.2 Standard Contractual Clauses. To the extent Privacy Shield is nullified or no longer is recognized by the European Commission as a valid transfer mechanism, the Parties agree the Standard Contractual Clauses (as evidence by each party's authorized signature on the Agreement), will apply to Customer Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing as adequate level of protection for personal data (as described by the GDPR.

7.2.1 Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees 3marketeers may engage new Sub-processors as described in Section 5 of this DPA.

7.2.2 The Parties agree the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out as described in Section 8 of this DPA.

7.2.3 The Parties agree that the certification of deletion of Customer Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by 3marketeers to Customer only upon Customer's request.

8. THIRD PARTY CERTIFICATIONS AND AUDITS

8.1 Certification. In addition to the information contained in this DPA, upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement place, 3marketeers will make available documents and information describing the controls implemented by 3marketeers so that Customer can reasonably verify 3marketeers' compliance with its obligations under this DPA.

8.2 Audits. To the extent the reports provided in Section 8.1 do not verify 3marketeers' compliance with its obligations under this DPA, Customer may audit 3marketeers' compliance with this DPA up to once per year, unless requested by a Supervisory Authority or in the event of a Security Incident. Such audit will be conducted by an independent third party ("Auditor") reasonably acceptable to 3marketeers. Before the commencement of any such on-site audit, Customer must submit a detailed proposed audit plan to 3marketeers at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration and state date of the audit. 3marketeers will review the proposed audit plan and provide Customer with any concerns or questions. 3marketeers will work cooperatively with Customer to agree on a final audit plan. The results of the inspection and all information reviewed during such inspection will be deemed 3marketeers' confidential information and shall be protected by Auditor in accordance with the confidentiality provisions noted above. Notwithstanding any other terms, the Auditor may only disclose to the Customer specific violations of the DPA, if any, and the basis for such findings, and shall not disclose to Customer any of the records or information reviewed during the inspection.

9. MISCELLANEOUS

9.1 Obligations Post-termination. Termination or expiration of this DPA shall not discharge the Parties from their obligations meant to survive the termination or expiration of this DPA.

9.2 Severability. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invaliding the remaining provisions hereof, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. The Parties will attempt to agree upon a valid and enforceable provision that is a reasonable substitute and shall incorporate such substitute provision into this DPA.

Annex 1
Security Policies, Procedures, Controls

3marketeers implements the following security measures with respect to the Customer Data:

1. Access Control of Processing Areas. Processes to prevent unauthorized persons from gaining access to the 3marketeers data processing equipment (namely telephones, database and application servers and related hardware) where the Customer Data are processed or used, to include:

a. establishing security areas;

b. protection and restriction of access paths;

c. securing the data processing equipment and personal computers;

d. establishing access authorization for employees and third parties, including respective authorization;

e. all access to the data centers where Customer Data are hosted is logged, monitored, and tracked; and

f. the data centers where Customer Data are hosted is secured by a security alarm system, and other appropriate security measures.

2. Access Control to Data Processing Systems. Processes to prevent 3marketeers data processing systems from being used by unauthorized persons, to include:

a. identification of the terminal and/or the terminal user to the data processor systems;

b. automatic time-out of user terminal if left idle, identification and password required to reopen;

c. regular examination of security risks by internal personnel and qualified third-parties;

d. issuing and safeguarding of identification codes;

e. password complexity requirements (minimum length, expiry of passwords, etc.); and

f. protection against external access by means of firewall and network access controls.

3. Access Control to Use Specific Areas of Data Processing Systems. Measures to ensure that persons entitled to use 3marketeers data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that Customer Data cannot be read, copied or modified or removed without authorization, to include by:

a. implementing binding employee policies and providing training in respect of each employee's access rights to the Customer Data;

b. assignment of unique user identifiers with permissions appropriate to the role;

c. effective and measured disciplinary action against individuals who access Personal Data without authorization;

d. release of data to only authorized persons; and

f. policies controlling the retention of back-up copies.

4. Transmission Control. Procedures to prevent Customer Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media and to ensure that it is possible to check and establish to which bodies the transfer of Customer Data by means of data transmission facilities is envisaged, to include:

a. use of firewall and encryption technologies to protect the gateways and pipelines through which the data travels;

b. implementation of encrypted connections to safeguard the connection to 3marketeers systems;

c. constant monitoring of infrastructure (e.g. McAfee Secure scanning at network level, disk space examination at system level, successful delivery of specified test pages and 3rd party independent penetration testing at application level); and

d. monitoring of the completeness and correctness of the transfer of data (end-to-end check).

5. Input Control. Measures to ensure that it is possible to check and establish whether and by whom Customer Data has been input into data processing systems or removed, to include:

a. authentication of the authorized personnel;

b. protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;

c. Segregation and protection of stored data via database schemas and logical access controls;

d. utilization of user codes (passwords);

e. proof established within data importer's organization of the input authorization; and

f. providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked.

6. Availability Control. Measures to ensure that Customer Data are protected from accidental destruction or loss, to include:

a. automatic failover between sites;

b. infrastructure redundancy; and

c. regular back-ups performed on database servers.

7. Segregation of Processing. Procedures to ensure that data collected for different purposes can be processed separately, to include:

- a. separating data through application security for the appropriate users;

  b. storing data, at the database level, in different tables, separated by the module or function they support; and

  c. designing interfaces, batch processes and reports for only specific purposes and functions, so data collected for specific purposes is processed separately.