Data Processing Addendum

EFFECTIVE DATE: May 25, 2018

This Data Processing Addendum ("DPA") is part of Nimble's Terms of Service and Privacy Policy which together with any exhibits, form the "Master Agreement" between Nimble, Inc. ("Nimble") and the customer who entered into the Terms of Service ("Customer"). This DPA governs the manner in which Nimble shall process Customer Personal Data (as defined below) as of the Effective Date.

1. Definitions

The following capitalized terms used in this DPA shall have the meanings given to them below:

a) *"Applicable Data Protection Law(s)"* means the relevant data protection and data privacy laws, rules and regulations to which the Customer Personal Data are subject. "Applicable Data Protection Law(s)" shall include, but not be limited to, the Privacy Shield Principles and requirements and to the EU General Data Protection Regulation (2016/679), as of its effective date on May 25, 2018 (the "GDPR").

b) *"Customer Personal Data"* means Personal Data pertaining to Customer's customer lists, email addresses, phone numbers, physical addresses of Customer or others, users or employees located in the European Union and received or collected by Nimble. As required by GDPR, Customer Personal Data and the specific uses of the Customer Personal Data are detailed on Exhibit A.

c) *"Data Controller"* means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of personal data.

d) *"Data Processor"* means a natural or legal person, public authority, agency or other body which Processes Customer Personal Data subject to this DPA.

e) *"Personal Data"* shall have the meaning assigned to the terms "personal data" or "personal information" under Applicable Data Protection Law(s).

f) *"Personal Data Request(s)"* means any requests from individuals exercising their rights in Personal Data granted to them under Applicable Data Protection Law(s).

g) *"Privacy Shield"* collectively means the EU – US Privacy Shield Framework established by the US Department of Commerce and the European Commission and the Swiss – US Privacy Shield Framework established by the U.S. Department of Commerce and the Swiss Administration.

h) *"Process(es)", "Processing", "Processed"* means any operation or set of operations which is performed on data or sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

i) *"Security of Data Processing"* means technical and organizational measures designed to protect Customer Personal Data as required by Applicable Data Protection Laws

j) *"Security Breach(es)"* means the accidental loss or destruction, unauthorized access, use or disclosure of Customer Personal Data.

k) *"Sub-processor(s)"* means Nimble's authorized contractors, agents, vendors and third-party service providers that Process Customer Personal Data.

l) *"Sub-processors List"* means a list of approved Sub-processors, which may be updated, amended, modified, or supplemented at any time.

2. Processing of Personal Data

2.1. The parties agree that with regard to the Processing of Customer Personal Data, Nimble is the Data Processor and Customer is the Data Controller and that Nimble will engage Sub-processors pursuant to the requirements set forth in Section 5 below. Customer Personal Data shall be Processed in compliance with the terms of this DPA and all Applicable Data Protection Law(s).

2.2. Customer shall Process Personal Data in accordance with the requirements of Applicable Data Protection Laws and Customer will ensure that its instructions for the Processing of Personal Data shall comply with Applicable Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired such Personal Data.

2.3. Nimble shall only Process Personal Data on behalf of and in accordance with Customer's instructions. Customer instructs Nimble to Process Personal Data for the following purposes: (i) Processing in accordance with the Master Agreement; (ii) Processing to comply with other reasonable instructions provided by Customer (e.g., via a support ticket) where such instructions are consistent with the terms of the Master Agreement, and (iii) Processing of Personal Data that is required under applicable law to which Nimble is subject, including but not limited to Applicable Data Protection Laws, in which case Nimble shall to the extent permitted by applicable law, inform the Customer of such legally required Processing of Personal Data.

3. Personal Data Requests

Nimble agrees to comply with all reasonable instructions from Customer related to any Personal Data Requests. At Customer's request Nimble shall assist Customer, to the extent possible, for the fulfilment of Customer's obligation to respond to a Personal Data Request. In the event that Nimble receives a Privacy Request directly, Nimble shall, to the extent legally permitted, promptly notify Customer of receipt of a Personal Data Request. Except to the extent required by applicable law, Nimble shall not respond to any Personal Data Request without Customer's prior written consent except to confirm that the request relates to Customer.

4. Personnel

4.1. Any person authorized to Process Customer Personal Data is informed of the confidential nature of the Customer Personal Data, has received appropriate training on his/her responsibilities and is subject to obligations of confidentiality and such obligations survive the termination of that persons' engagement with Nimble.

4.2. Nimble shall ensure that access to Customer Personal Data is limited to those personnel who require such access to perform under the Master Agreement.

5. Sub-processors

5.1. Customer authorizes and agrees, that to the extent necessary to fulfill Nimble's obligations under the Master Agreement, Nimble may (i) engage Sub-processors and (ii) Sub-processors may engage other sub-processors. Any transfer of Customer Personal Data shall comply with all Applicable Data Protection Law(s). Any such Sub-processors will be permitted to obtain Customer Personal Data only to deliver the services Nimble has retained them to provide, and they are prohibited from using Customer Personal Data for any other purpose.

5.2. Nimble agrees to (i) enter into a written agreement with third parties ("Sub-processor(s)") regarding such Sub-processors' Processing of Customer Personal Data that imposes on such Sub-processors' data protection and security requirements for Customer Personal Data that are compliant with Applicable Data Protection Law(s); and (ii) remain responsible to Customer for Nimble's Sub-processors' (and their sub-processors if applicable) failure to perform their obligations with respect to the Processing of Customer Personal Data.

5.3. Nimble has included a list of approved Sub-processors as of the effective date of this DPA on Exhibit B. In the event Nimble makes any changes to the list of Sub-processors, Customer may access the current list of Sub-processors at the following link, Sub-processors List.

5.4. Customer may object to any new Sub-processor in writing within thirty (30) days after any updates are made by Nimble to the Sub-processors List. In the event of such objection by Customer, Nimble will take commercially reasonable steps to address the objections raised by Customer. Legitimate objections must contain reasonable and documented grounds relating to a Sub-processor's non-compliance with Applicable Data Protection Laws. If Nimble is unable to resolve Customer's objection, Nimble will either (a) instruct the Third Party to cease any further processing of Customer Personal Data, or (b) allow Customer to terminate the part of the service, or the service in its entirety, performed under the Master Agreement that cannot be performed by Nimble without use of the objectionable Sub-processor. If Customer does not object, the new Sub-processor shall be deemed accepted and Nimble may continue to use such Sub-processor.

6. Data Transfers

6.1. Nimble will process Customer Personal Data only as necessary for the limited and specified purposes identified in this DPA and/or Master Agreement. In the event that Customer Personal Data is transferred outside the European Economic Area or Switzerland to any country not deemed by the European Commission as providing an adequate level of protection for personal data, Nimble complies with the provisions of Section 6.2 with respect to such transfers.

6.2. Nimble has certified its compliance with Privacy Shield and Nimble and Customer will use Privacy Shield as the adequacy mechanism supporting the transfer and Processing of Customer Personal Data.

7. Security and Compliance

7.1. Nimble agrees to implement appropriate measures to ensure Security of Data Processing. Nimble regularly monitors compliance with these safeguards, and further agrees to regularly test, assess and evaluate the effectiveness of its Security of Data Processing.

7.2. Nimble shall provide Customer with reasonable assistance at Customer's expense, where Customer believes the type of Processing performed by Nimble is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, Processing sensitive Personal Data on a large scale and systematic monitoring on a large scale), and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities. Nimble shall provide such assistance upon Customer's reasonable request and to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Nimble.

7.3. Nimble agrees to keep records of its Processing in compliance with Applicable Data Protection Laws and provide such records to Customer upon Customer's reasonable request to assist Customer with complying with supervisory authorities' requests. Upon request from Customer and at Customer's expense, Nimble agrees to reasonably cooperate with Customer for the purpose of verifying Nimble's compliance with Applicable Data Protection Laws.

7.4. Nimble will promptly notify Customer, without undue delay, after Nimble becomes aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unlawful access to any Customer's Personal Data that is transmitted, stored or otherwise Processed by Nimble or

its Sub-processors of which Nimble becomes aware. Nimble will use reasonable efforts to identify the cause of such Security Breach and shall promptly and without undue delay: (a) investigate the Security Breach and provide Customer with information about the Security Breach, including if applicable, such information a Data Processor must provide to a Data Controller under Applicable Data Protection Laws to the extent such information is reasonably available; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Breach to the extent the remediation is within Nimble's reasonable control. The obligations herein shall not apply to any breach that is caused by Customer.

7.5. Nimble shall notify Customer of Security Breaches, if any, via email It is Customer's sole responsibility to ensure it maintains accurate contact information with Nimble at all times.

7.6. Nimble's obligation to report or respond to a Security Breach under this Section will not be construed as an acknowledgement by Nimble of any fault or liability with respect to any Security Breach.

8. Data Retention and Deletion upon Termination

Upon termination of the Master Agreement, Customer may delete the Customer Personal Data in Nimble's possession or control by deleting its account. At Customer's discretion, Customer may export all Customer Personal Data before deleting its account. The foregoing requirement will not apply to the extent Nimble is required by applicable law to retain some or all of the Customer Personal Data, or to Customer Personal Data that is archived on Nimble's back-up systems. With regards to such Customer Personal Data on Nimble's back-up systems, Nimble will stop Processing and destroy or deidentify such data according to its data retention policies, except to the extent required by applicable law.

Exhibit A

Details of Processing of Customer Personal Data

Subject matter and duration of the Processing of Customer Personal Data:

The subject matter and duration of the Processing of the Customer Personal Data are set out in the Master Agreement.

The nature and purpose of the Processing of Customer Personal Data:

Customer Personal Data is used to provide services as set out in the Master Agreement.

The types of Customer Personal Data to be Processed:

Customer Personal Data to be processed may be any Personal Data stored by Customer as permitted under the Master Agreement, including, but not limited to, Personal Data of natural persons, Personal Data of companies / organizations, Personal Data of employees.

The categories of Data Subject to whom the Customer Personal Data relates:

Data Subjects to whom the Customer Personal Data relates may be customers, vendors, employees, friends, agents, partners, advisors, investors of Customer.

Exhibit B

Third-Party Sub-Processors

EFFECTIVE DATE: May 25, 2018

Third-Party Service Provider	Purpose	Entity Country	Entity Website
Act-On	Email service provider	USA	http://www.act-on.com/
Amazon AWS	Data Hosting	USA	http://aws.amazon.com/
Atlassian	Bug Reporting and Tracking	Australia	https://www.atlassian.com/
Braintree	Payment Processor	USA	http://www.braintreepayments.com/
CircleBack	Data Enrichment	USA	https://www.circleback.com/
Clearbit	Data Enrichment	USA	http://clearbit.com/
FullContact	Data Enrichment	USA	https://www.fullcontact.com/
Google Inc.	Email service provider	USA	http://www.google.com/
Google Analytics	Analytics Platform	USA	http://www.google.com/
Google Search API	Data Enrichment	USA	http://www.google.com/
Hunter	Data Enrichment	France	https://hunter.io/
Intercom	Email service provider	USA	http://www.intercom.com/
Klout	Data Enrichment	USA	http://klout.com/
Microsoft Azure	Data Hosting	USA	https://azure.microsoft.com/
Microsoft PowerBI	Analytics Platform	USA	https://powerbi.microsoft.com/
Mixpanel	Analytics Platform	USA	http://www.mixpanel.com/
OneSignal	Notifications Engine	USA	https://onesignal.com/
Owler	Data Enrichment	USA	http://www.owler.com/
PayPal	Payment Processor	USA	https://www.paypal.com
SendGrid	Email service provider	USA	http://www.sendgrid.com/
VWO	Analytics Platform	USA	https://vwo.com/