Branch Data Processing Addendum

1. Introduction

This Branch Data Processing Addendum ("**Addendum**") is an integral part of Branch Metrics, Inc.'s Terms & Conditions (or instead, where there is an existing service agreement in place between Customer and Branch prior to the effective date of this Addendum (the "**Service Agreement**"), of that Service Agreement), which together with one or more Order Forms and Exhibits, form the "**Agreement**" between Branch Metrics, Inc. ("**Branch**") and the Customer who agreed to and is party to the Terms & Conditions or Service Agreement ("**Customer**"), and is made part of the Agreement. This Addendum governs the manner in which Branch shall Process Customer Personal Data on behalf of Customer (who is Controller of the data subject to this Addendum) and only applies to the extent Branch serves as a Processor of such Customer Personal Data on behalf of Controller. This Addendum shall be effective on the date agreed to by Customer. Except for the changes made by this Addendum, the Agreement remains unchanged and in full force and effect. In the event of a conflict between the Agreement, including Order Forms and Exhibits, and this Addendum, this Addendum shall control. The parties agree that this Addendum shall replace any existing data processing addendum the parties may have previously entered into in connection with the Branch Services.

Capitalized terms have the meaning given to them in the Agreement, unless otherwise defined below.

2. Definitions

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

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 Protections Law(s)" shall include, but not be limited to, the forthcoming General Data Protection Regulation (EU 2016/679) (the "**GDPR**"), when it becomes effective on May 25, 2018, and the Privacy Shield Principles and requirements.

b) "**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.

c) "**Customer Personal Data**" means Personal Data pertaining to Customer's users located in the European Economic Area (EEA), including the United Kingdom, and Switzerland and received or collected by Branch, provided by Customer in its capacity as Controller to Branch, the Processor. The Customer Personal Data and the specific uses of the Customer Personal Data are detailed in Schedule 1 as required by the GDPR.

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

e) "**Privacy Shield**" means the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks' self-certification programs established by the U.S. Department of Commerce and the European Commission.

f) "**Privacy Shield Principles**" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended or replaced).

g) "**Process**," "**Processes**," "**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.

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

i) "**Security Incident(s)**" means the unauthorized access, use or disclosure of Customer Personal Data.

j) "**Sensitive Personal Data**" shall have the meaning assigned to the terms "special categories of personal data" under Applicable Data Protection Law(s) and shall include Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

k) "**Third Party(ies)**" means Branch-authorized contractors, agents, vendors and third-party service providers (i.e., sub-processors) that Process Customer Personal Data.

3. Data Handling, Access and Processing

a) Role of the Parties. As between Branch and Customer, Customer is the Controller of Customer Personal Data, and Branch shall Process Customer Personal Data as a Processor acting on behalf of Customer, as to the Processing identified in Schedule 1. To the extent, if at all, the Agreement provides Branch with the right to determine the purposes and means of processing Personal Data pertaining to Customer's users located in the European Economic Area (EEA) (including the United Kingdom and Switzerland), beyond the Processing identified in Schedule 1, and Branch in fact engages in any such Processing, Branch may instead be a Controller under Applicable Data Protection Law(s) as to such Processing. Where Branch is a Controller under Applicable Data Protection Law(s), Processing undertaken in its capacity as a Controller shall not be subject to this Addendum, and Branch instead shall engage in such Processing in accordance with any Applicable Data Protection Law(s) applicable to Controllers.

b) General Compliance by Branch. Customer Personal Data shall be Processed by Branch in compliance with the terms of this Addendum and all Applicable Data Protection Law(s).

c) General Compliance by Customer. Customer agrees that (i) it shall comply with its obligations as Controller under Applicable Data Protection Law(s) in respect of its Processing of Customer Personal Data and any Processing instructions it issues to Branch, and (ii) it has provided notice and obtained (or shall obtain) all necessary consents (including without limitation, verifiable consent) and rights necessary under Applicable Data Protection Law(s) for Branch to Process Customer Personal Data and provide the Branch Services pursuant to the Agreement and this Addendum.

d) Branch and Third Party Compliance. Branch agrees to (i) enter into a written agreement with Third Parties regarding such Third Parties' Processing of Customer Personal Data that imposes on such Third Parties 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 Branch's Third Parties' (and their sub-processors' if applicable) failure to perform their obligations with respect to the Processing of Customer Personal Data.

e) Authorization to Use Third Parties. To the extent necessary to fulfill Branch's contractual obligations under the Agreement or any Order Form, Customer hereby authorizes (i) Branch to engage Third Parties, including Amazon Web Services and Rollbar, and (ii) Third Parties to engage sub-processors. Any transfer of Customer Personal Data shall comply with all Applicable Data Protection Law(s).

f) Right to Object to Third Parties. Branch shall engage a new Third Party only after Branch has provided Customer with notification of a new Third Party. To receive notification via email regarding any new Third Party, Customer should email privacy@branch.io to request subscription to such notices. If Customer does not contact privacy@branch.io with any such request, Branch's posting of the name of such Third Party on its Third-Party List (available at https://branch.io/third-party-list) will be deemed to constitute notice of a new Third Party to Customer under this provision. Customer will have ten (10) calendar days to object after notice is given. In the event Customer objects within ten (10) calendar days after notice is given, Branch will make reasonable efforts to address Customer's objection. After this process, if a resolution has not been agreed to within ten (10) calendar days, Branch will proceed with engaging the Third Party. If applicable, Customer will be given the opportunity to terminate the Branch Services without penalty or another such resolution as the parties may agree.

g) Following Instructions. Branch shall Process Customer Personal Data only in accordance with the written instructions of Customer as specifically authorized by the Agreement. Branch will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer's instructions and applicable law or otherwise seeks to Process Customer Personal Data in a manner that is inconsistent with Customer's instructions.

h) Confidentiality. Any person authorized to Process Customer Personal Data must agree to maintain the confidentiality of such information or be under an appropriate statutory or contractual obligation of confidentiality.

i) Personal Data Inquiries and Requests. Branch agrees to comply with all reasonable instructions from Customer related to any requests from individuals exercising their rights in Personal Data granted to them under Applicable Data Protection Law(s) ("**Privacy Request**"). At Customer's request and without undue delay, Branch agrees to assist Customer in answering or complying with any Privacy Request.

j) Prior Consultation. Branch agrees to provide reasonable assistance to Customer where, in Customer's judgement, the type of Processing performed by Branch is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, or where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

k) Demonstrable Compliance. Branch agrees to keep records of its Processing in compliance with Applicable Data Protection Law(s) and provide such records to Customer upon reasonable request to assist Customer with complying with supervisory authorities' requests.

l) Processing of Certain Types of Personal Data. Customer agrees that it shall not use the Branch Services to Process Sensitive Personal Data without Branch's explicit and prior written consent.

4. International Transfers

a) Cross-Border Data Transfer Mechanism. The parties acknowledge and agree that to the extent Branch Processes any Customer Personal Data under the Agreement, any related Order Forms, or Exhibits, outside the EEA in a country that has not been designated as providing an adequate level of protection for Personal Data, including the United States, Branch shall be deemed to provide adequate protection under Applicable Data Protection Law(s) for any such Customer Personal Data due to Branch's Privacy Shield certification. Customer will operate as a Controller and Branch will operate as a Processor Processing Customer Personal Data only as necessary for the limited and specified purposes identified in this Addendum and/or the Agreement, and in accordance with at least the same level of protection as is required under the applicable Privacy Shield Principles. Additionally, Branch hereby expressly agrees to assist Customer with any request from the U.S. Department of Commerce to provide the relevant privacy provisions of this Addendum and the Agreement. Branch will provide Customer with reasonable prior written notice if it can no longer meet its obligations under the Privacy Shield or if it plans not to renew its certification under the Privacy Shield, at which time, as the parties' sole remedy, the parties will negotiate entry into an alternative data transfer solution, including entering into the European Commission Standard Contractual Clauses for Data Processors (2010/87/EU) (the "**Standard Contractual Clauses**"), or any replacement thereof. The foregoing will not entitle Customer to any termination or cancellation right with respect to the Agreement.

5. Information Security Program

Branch agrees to implement appropriate technical and organizational measures designed to protect Customer Personal Data as required by Applicable Data Protection Law(s) (the "**Information Security Program**"). Further, Branch agrees to regularly test, assess and evaluate the effectiveness of its Information Security Program to ensure the security of the Processing.

6. Audits

Upon request from Customer, Branch agrees to reasonably cooperate with Customer for the purpose of verifying Branch's compliance with Applicable Data Protection Law(s).

7. Return or Deletion of Data

After notification from Customer that Customer seeks to terminate use of all Branch Services, Branch shall delete or provide to Customer all Customer Personal Data in its possession or control, save that this requirement shall not apply to the extent Branch is required by applicable law to retain some or all of the Customer Personal Data, or to Customer Personal Data it has archived on back-up systems, which Customer Personal Data Branch shall securely isolate and protect from any further processing, except to the extent required by applicable law.

8. Security Incident

a) Security Incident Procedure. Branch will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to suspected or known Security Incidents, mitigate harmful effects of Security Incidents, document Security Incidents and their outcomes, and (ii) restore the availability or access to Customer Personal Data in a timely manner.

b) Notice. Branch agrees to provide prompt written notice without undue delay and within the time frame required under Applicable Data Protection Law(s) to Customer if it knows or suspects that a Security Incident has taken place. Such notice will include all available details required under Applicable Data Protection Law(s) for Customer to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

IN WITNESS WHEREOF, the parties have caused this Addendum to be signed by their duly authorized representatives effective as of the last date of execution below:

Customer Name:____________________	**BRANCH METRICS, INC.:** DocuSigned by:
Signature:____________________	Signature: Michael Molinet AC69E839BB3B430...
Name:____________________	Name: Michael Molinet
Title:____________________	Title: Chief Operating Officer
Date:____________________	Date: April 30, 2018

Schedule 1 to the Branch Privacy and Security Addendum

1.1 Subject Matter of Processing	The subject matter of Processing is the Branch Services pursuant to the Agreement.
1.2 Duration of Processing	The Processing will continue until Branch's receipt of notification from Customer of termination of use of all Branch Services.
1.3 Categories of Data Subjects	Includes the end users of Customer's app(s) and/or websites into which the Branch SDK is integrated, and/or end users who click on Branch deep links.
1.4 Nature and Purpose of Processing	The purpose of Processing of Customer Personal Data by Branch is the performance of the Branch Services pursuant to the Agreement.
1.5 Types of Personal Data	The data collected via Branch's SDK and Branch links includes the following types of Personal Data: iOS Identifier for Advertising (IDFA) iOS Identifier for Vendors (IDFV) Android Advertising ID (GAAID) Android ID IP Address Developer ID Local IP address Cookie Phone number (only used with "Text Me the App" feature)