Data Processing Agreement

Last Updated: August 20, 2020

This Data Processing Agreement ("**DPA**") forms part of the Master Subscription and Services Agreement (the "**Agreement**") between You ("**Customer**") and Validity, Inc. ("**Validity**"), and governs all Order Forms between the parties pursuant to such Agreement to reflect the parties' agreement with respect to the Processing of Personal Data, in accordance with the requirements of Applicable Data Protection Law. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

DEFINITIONS

"**Applicable Data Protection Law**" means: (i) the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"); (ii) California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq. ("**CCPA**"); (iii)) the Australian Privacy Act 1988 (Cth) ("**Privacy Act**") and the Australian Privacy Principles; and (iv) any other data protection laws which apply to the Processing of Personal Data under this DPA, including any applicable national data protection laws made under or pursuant to (i) or (ii) in the United States of America, United Kingdom, Australia or any European Union ("EU") Member State, in each case as amended or superseded from time to time.

"**CCPA Consumer**" means a "consumer" as such term is defined in the CCPA.

"**Customer Data**" means electronic data submitted to the Subscribed Offerings by Customer and its Users.

"**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.

"**Data Subject**" means an identified or identifiable natural person, including without limitation a CCPA Consumer.

"**EU Model Clauses**" means standard contractual clauses adopted or approved by the European Commission for transfers under the GDPR (and if more than one set of such clauses may apply to a transfer, the most recent such set) or any successor clauses approved for transfers by the Commission or a relevant supervisory authority under Applicable Data Protection Law.

"**Personal Data**" has the meaning assigned to it in the Applicable Data Protection Law, including without limitation "personal information" as such term is defined in the CCPA, and refers to any such data Processed by Validity on Customer's behalf in connection with the Agreement.

"**Processor**", "**Processing**" or "**Process**" (or any variation thereof) means any operation or set of operations which is performed on Personal Data or on sets of Personal 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, and "Process" will be interpreted accordingly.

"**Sensitive Data**" means data revealing a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health data, sex life or sexual orientation.

"**Sell**" and "**Sale**" have the meaning assigned to them in the CCPA.

"**Sub-processor**" means any third party appointed by Validity in accordance with the Agreement or this DPA (as applicable) to process Personal Data.

"**Subscribed Offerings**" shall mean Validity software or services and its Documentation, provided under the Agreement.

"**You**" or "**your**" means the Customer indicated in the signature block below;

INTRODUCTION

In connection with the provision of the Subscribed Offerings pursuant to the Master Subscription and Services Agreement entered into between Customer and Validity (the "Agreement"), Validity may Process Personal Data on Customer's behalf. Terms defined in the Agreement but not in this DPA shall have the same meanings in this DPA. To the extent that Validity Processes any Personal Data on behalf of Customer in connection with the Agreement, the parties agree to comply with the provisions set forth in this DPA, and with the following provisions with respect to any Personal Data Processed by Validity under the Agreement. For avoidance of doubt, Validity does not receive any Personal Data as consideration for any Subscribed Offerings or other items provided or performed by Validity. For the purposes of the CCPA, the parties acknowledge and agree that Validity will act as a "Service Provider" and not as a "Third Party," as such terms are defined in the CCPA, in its performance of its obligations pursuant to the Agreement. Customer will act as a single point of contact for its Affiliates with respect to CCPA compliance, such that if Validity gives notice to the Customer, such information or notice will be deemed received by the Customer's Affiliates.

DATA PROTECTION; COMPLIANCE WITH LAWS

Validity will Process Personal Data in accordance with Customer's documented instructions as set out in the Agreement and this DPA, except where otherwise required by applicable law. Customer instructs Validity to Process Personal Data to provide the Subscribed Offerings in accordance with the Agreement or as otherwise permitted under Applicable Data Protection Law. If applicable law requires Validity to process Personal Data for any other purpose, Validity will inform Customer of this requirement first, unless prohibited by such law(s) from doing so. Validity shall be prohibited from selling, retaining, using, or disclosing Personal Data for any purpose other than to perform the Subscribed Offerings in accordance with the Agreement and DPA (or as otherwise permitted in the Agreement or Applicable Data Protections Laws).

With regard to the Processing of Personal Data as part of the Subscribed Offerings, Customer shall be deemed the Controller and Validity shall be deemed the Processor. Customer shall ensure that it has obtained any and all authorizations and lawful bases for Processing (including verifiable consent where necessary) in accordance with Applicable Data Protection Law in order to provide Personal Data to Validity for Processing and Customer shall otherwise comply with its obligations under Applicable Data Protection Law in connection with such Personal Data. Customer acknowledges that the Subscribed Offerings are not intended or designed for the Processing of Sensitive Data, and Customer agrees not to provide any Sensitive Data through the Subscribed Offerings. The Data Subjects, categories of data, and Processing operations are specified in **Attachment A** attached hereto.

RIGHTS OF DATA SUBJECTS

If a Data Subject contacts Validity in relation to its Processing of Personal Data for Customer, Validity will promptly redirect the Data Subject to Customer. Customer, as the Controller, shall be solely responsible

for responding to any Data Subject rights requests or complaints and/or any regulatory or supervisory authority inquiries or communications related to Personal Data, Processed by Validity on Customer's behalf. Validity will not disclose any such Personal Data to a Data Subject or a third party unless required to do so by law. If required by Applicable Data Protection Law, and required and requested by the Customer, Validity will (at the Customer's expense) provide commercially reasonable assistance to Customer in Customer's response to Data Subjects, as it relates to their Personal Data; and provide Customer with the ability to ensure that the data subject can exercise their right to data portability and the right to delete, correct, block, access, or copy their Personal Data, and/or promptly delete, correct, block, access or copy their Personal Data within the Subscribed Offerings, in each case at the request of the Customer and at the Customer's expense.

COOPERATION TO CUSTOMER

Validity shall, without undue delay, notify Customer if it receives a demand from any court, government agency, supervisory authority, or law enforcement agency for Customer Data, including demands for Personal Data that Validity Processes on Customer's behalf, unless prohibited by law from notifying Customer, and Validity will use its best efforts to direct the court, government agency, supervisory authority, or law enforcement agency to request such information directly from Customer. As part of this effort, Validity may provide Customer's basic contact information to the requester. If compelled to disclose Customer Data to any court, government agency, supervisory authority, or law enforcement agency, Validity will first promptly, and without any undue delay, notify Customer of the request (except where Validity is legally prohibited from doing so).

Validity shall also provide reasonable cooperation to Customer (at Customer's expense) in connection with any data protection impact assessment that Customer may be required to undertake under Applicable Data Protection Law.

SUBPROCESSING

Customer agrees that Validity may appoint Sub-processors to assist it in providing the Subscribed Offerings by processing Personal Data solely for the purpose of providing the Subscribed Offerings, provided that such Sub-processors: (i) agree to act only on Validity's instructions when processing the Personal Data (which instructions shall be consistent with Customer's processing instructions); and (ii) agree to protect the Personal Data to a standard consistent with the requirements of this DPA. Validity will maintain a list of such Sub-processors in **Attachment B** attached hereto, which we may update from time to time. Before authorizing any new Sub-processor, we shall provide notification. You may object to the change without penalty by notifying us within 14 days after the notice, provided such objection is based on reasonable grounds relating to data protection. In such event, Validity will either not appoint or replace the relevant Sub-processor or, if this is not possible, Customer may suspend or terminate the Master Services Agreement (without prejudice to any fees or other obligations incurred by Customer prior to suspension or termination).

PERSONNEL; SECURITY CONTROLS

Validity shall ensure that (i) access to Personal Data that Validity Processes on Customer's behalf is strictly limited to those personnel who require such access as strictly necessary for the purposes of the Agreement, and to comply with Applicable Data Protection Law; (ii) ensure that personnel who have access to such Personal Data are informed of the confidential nature of such information, and are subject to confidentiality undertakings or professional or statutory obligations of confidentiality, with such confidentiality obligations surviving the termination of such personnel's work with Validity; and (iii) take commercially reasonable steps to ensure the reliability of any personnel who have access to such Personal Data. Validity will implement and maintain appropriate technical and organizational security measures to prevent accidental

or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by Validity on Customer's behalf ("**Security Incidents**"), and to preserve appropriately the security, availability, integrity and confidentiality of Personal Data ("**Information Security Controls**"). Customer agrees that Validity's implementation of the Information Security Controls identified available at https://www.validity.com/resources/Information-Security-Controls.pdf shall be deemed to sufficient for the purposes of complying with its obligations under this Section. Validity may update its Information Security Controls from time to time, provided that this does not result in a reduction in the general level of protection provided by Validity's security measures.

TRANSFERS

Validity shall not transfer Personal Data outside of the European Economic Area ("EEA") unless it has taken such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include (without limitation) transfers to any country or territory that is at the time subject to a current finding by the European Commission of adequate protection, to a recipient that has achieved binding corporate rules authorisation in accordance with Applicable Data Protection Law, or under any derogation permitted by Applicable Data Protection Law. To the extent any transfer by Validity outside the EEA in connection with the Agreement is not covered by the above mechanisms, the relevant transfer will be governed by the appropriate EU Model Clauses of which the body is incorporated by reference to this DPA, with the data exporter being Customer (on behalf of itself and its Affiliates), the data importer being Validity, and the remaining details on data subjects etc. being deemed completed as appropriate with the information set out in this DPA (including without limitation Attachment A) and the Agreement. In the event of any conflict or inconsistency among or between the terms and conditions of such EU Model Clauses and this DPA and/or the Agreement, the terms of the EU Model Clauses shall prevail.

Validity shall not Sell any Personal Data that Validity processes on Customer's behalf to another business or third party without the prior written consent of the Customer unless and only to the extent that any sharing or disclosure of Personal Data is made to a Sub-processor. VALIDITY HEREBY CERTIFIES THAT VALIDITY UNDERSTANDS THE REQUIREMENT IN THE PRECEDING SENTENCE AND AGREES TO COMPLY WITH IT. Notwithstanding the foregoing two sentences, nothing in this DPA or the Agreement shall restrict Validity's ability to disclose Personal Data to comply with applicable laws or as otherwise permitted by Applicable Data Protection Law.

SECURITY INCIDENT MANAGEMENT

If Validity becomes aware of a confirmed Security Incident, Validity shall inform Customer without undue delay and shall provide reasonable information and cooperation to Customer so that Customer can fulfil any data breach reporting obligations it may have under (and in accordance with the timescales required by) Applicable Data Protection Law. Validity shall further take any such reasonably necessary measures and actions to remedy or mitigate the effects of the Security Incident and shall keep Customer informed of all material developments in connection with the Security Incident.

DELETION AND RETURN

Subject to this Section, Customer may , upon any termination of the Agreement, require (in writing)Validity to return (at Customer's expense) or delete and procure the deletion of all copies of Personal Data Processed by Validity or any Sub-processors on Customer's behalf. Validity shall comply with any such written deletion request within a maximum of 90 days after the date of termination of the Agreement (or within such shorter timeframe as may be required by the Agreement).

This requirement shall not apply to the extent that Validity is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, in which event Validity shall securely isolate and protect such Personal Data from any further processing except to the extent required by applicable law until deletion is possible.

AUDIT REPORTS

Upon Customer's request, Validity will make available to Customer, up to once per year, a copy of a third-party audit or assessment reports, such as a Service Organization Controls No. 2 (SOC2) in accordance with auditing standards in the Statements on Standards for Attestation Engagements No. 16 (SSAE16)) or such other alternative standards that are substantially equivalent to ISO 27001 ("**Audit Reports**"); or (b) if Validity has not obtained a Report, Validity shall, at the Customer's expense, provide responses to any questions that Customer may reasonably submit for purposes of verifying Validity's compliance with this DPA ("**Questionnaires**"). Any such Audit Reports and completed Questionnaires will constitute Confidential Information and may not be disclosed without Validity or applicable third party prior written consent, except as required by law.

GENERAL

In the event of any conflict or inconsistency among or between the terms and conditions of the Agreement (including any existing data processing addendum to the Agreement) and this DPA, this DPA shall prevail. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA 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. This DPA may not be modified except by a subsequent written instrument agreed by both parties.

ATTACHMENT A

DESCRIPTION OF PROCESSING

1. Subject Matter, Nature and Purpose

Validity Processes Personal Data for the purposes set forth in the Agreement.

2. Duration

Validity shall possess Personal Data for as long as necessary to carry out its obligations under the terms of the Agreement with Controller.

3. Categories of Individuals

The Personal Data Processed relates to Customer's employees (Users of the Subscribed Offerings) or other individuals, current or prospective Customer's customer, identified by Customer.

4. Type of Personal Data

Customer's current or prospect customer e-mail addresses; for certain BriteVerify features phone numbers and addresses; and for Customer using Return Path tacking pixels, IP addresses.

5. Sensitive Data

N/A

ATTACHMENT B

VALIDITY SUB-PROCESSORS

Vendor Name	Services Provided	Location
Melissa Data, Inc.	Phone and street address verification vendor for BriteVerify	United States
TowerData, Inc.	Email address verification vendor for 250ok	United States
Amazon Web Services, Inc.	Infrastructure hosting for all services	United States
Recurly, Inc.	Payment processor for DemandTools SMB site	United States
Braintree	Payment processor for BriteVerify SMB site	United States
Auth0, Inc.	Identity management provider	United States
LightBound	Data center power/connectivity for 250ok (Validity owns/operates all hardware)	United States
Expedient	Data center power/connectivity for 250ok (Validity owns/operates all hardware)	United States
Pendo.io	Customer engagement and website analytics	United States
ChurnZero, Inc.	Customer engagement and website analytics	United States