

U.S. Data Processing Addendum

[*] and Customer (as each such term is defined below) have entered into an agreement, order form, statement of work or other contract for the provision of certain services by [*] to Customer (the “**Agreement**”). This U.S. Data Processing Addendum (“**DPA**”) is entered into between [*] and the counterparty that entered into such Agreement (“**Customer**”). This DPA supplements the Agreement, inclusive of all exhibits, addenda, statements of work, work orders and similar documents entered into by the parties pursuant to such Agreement with regard to the Processing of Personal Information (as such terms are defined below) in the United States. Capitalized terms used but not defined in this DPA shall have the meanings assigned to them in the Agreement. In the event of a conflict between this DPA and the Agreement, this DPA shall prevail.

1. Definitions.

- a. “**Business**” or “**Controller**” shall mean an entity that determines the purposes and means of Processing of Personal Information.
- b. “**Consumer**” shall mean the individual to whom Personal Information relates.
- c. “**Customer Data**” means the Personal Information related to Consumers that [*] Processes on behalf of Customer as a Service Provider or Processor as set forth in Section 2 of this DPA. Customer Data is inclusive of Personal Information collected from Ads that are served or measured through Customer’s use of the Services pursuant to the Agreement.
- d. “**Data Protection Laws**” means any applicable local, state and federal laws, rules and regulations in the United States relating to the use, collection, retention, storage, security, disclosure, transfer, sale or other Processing or Personal Information, including but not limited to the California Consumer Privacy Act (the “**CCPA**”), the California Privacy Rights Act (the “**CPRA**”), the Virginia Consumer Data Protection Act (the “**VCDPA**”), the Colorado Privacy Act (the “**CPA**”), the Connecticut Data Protection Act (the “**CTDPA**”), the Utah Consumer Privacy Act, (the “**UCPA**”) and any similar laws including any amendments and any final implementing regulations to any of the foregoing that are in effect or that become effective on or after the effective date of this DPA.
- e. “**Individual Rights Request**” or “**IRR**” means a request from a Consumer for information, access or action with respect to Personal Information that, under Data Protection Laws, requires a response from either or both of the Controller and the Processor with respect to such

Personal Information, and that is reasonably attributable by the Party receiving such request to Personal Information Processed under the Agreement.

f. “Personal Information” means any information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a Consumer, or as otherwise defined by Data Protection Laws, including any equivalent terminology such as “Personal Data” or “Personally Identifiable Information”.

g. “Process” or “Processing” means any operation or set of operations performed, whether by manual or automated means, on information or on sets of information, such as the collection, use, storage, disclosure by transmission, dissemination or otherwise making available, alignment or combination, analysis, restriction, deletion, or modification of information.

h. “Service Provider” or “Processor” shall mean an entity that Processes Personal Information on behalf of a Business or Controller.

i. “Sell”, “Selling”, “Share” and “Sharing” shall have the meanings assigned to them in Data Protection Laws.

2. Role of the Parties; Compliance with Laws. With regard to Customer Data, [*] is a Service Provider and Processor, and Customer is a Business and a Controller. Each party will comply with its obligations under Data Protection Laws.

3. Customer’s Rights. Upon Customer’s reasonable request, [*] will make available such information in [*]’s possession as is reasonably necessary for Customer to conduct and document data protection assessments in accordance with Data Protection Laws. Customer will have the right to: (i) take reasonable and appropriate steps to help ensure that [*] uses Customer Data in a manner consistent with [*]’s obligations under and as required by Data Protection Laws, and (ii) upon reasonable prior written notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of such Customer Data under and as required by applicable Data Protection Laws.

4. [*] Obligations. [*] will notify Customer if it determines that it can no longer meet its obligations under applicable Data Protection Laws. [*] will Process Customer Data for the purpose of providing the Services set forth in the Agreement and in accordance with Customer’s instructions set forth in the Agreement or in writing. Without limiting the foregoing, [*] is prohibited from: (i) Selling Customer Data or otherwise making Customer Data available to any third party for monetary or other valuable

consideration; (ii) Sharing Customer Data with any third party for cross-context behavioral advertising; (iii) retaining, using, or disclosing Customer Data for any purpose other than for the business purposes specified in the Agreement or as otherwise permitted by Data Protection Laws; (iv) retaining, using, or disclosing Customer Data outside of the direct business relationship between the parties; (v) to the extent prohibited by Data Protection Laws, combining Customer Data with other information that Innovid receives from or on behalf of another person or persons, or collects from its own interaction with the Consumer. [*] hereby certifies that it understands the restrictions in the applicable Data Protection Laws and will comply with them.

5. Sub-Processors. [*] may engage a third party to act as a sub-processor for Customer Data; provided that if required under Data Protection Laws, Innovid first notifies Customer and provides Customer with the opportunity to object to the engagement, and provided in any event that: (i) [*] remains responsible for its sub-processors' compliance with this DPA, and (ii) the engagement is pursuant to a written contract that requires the sub-processor to meet the obligations of [*] under this DPA with respect to Customer Data.

6. Data Security. [*] shall implement and maintain reasonable security procedures, practices, and controls, as may be appropriate based on the nature of the information, designed to protect Customer Data from unauthorized access, disclosure or destruction. [*] will provide the notifications and assistance to Customer as required by the data breach provisions of Data Protection Laws.

7. Individual Rights Requests. If [*] receives an IRR from a Consumer to confirm whether their Personal Information is being Processed, to access their Personal Information, to correct inaccuracies in their Personal Information, to delete their Personal Information, to obtain a copy of their Personal Information, or to opt-out of the Processing of their Personal Information for the purposes of targeted advertising, sale or profiling, [*] shall promptly notify Customer of the receipt of such IRR and, subject in each case to the exceptions and limitations provided therein, comply with such IRR in accordance with and to the extent required under Data Protection Law. For the avoidance of doubt, [*] shall have no obligation to delete information that has been de-identified or aggregated or information relating to Customer's use of the Services that is not Customer Data.

8. Termination and Survival; Jurisdiction and Venue; Limitation of Liability. This DPA and all provisions herein shall survive so long as, and to the extent that, [*] Processes or retains Customer Data. The choice of law

and jurisdiction as set forth in the Agreement apply to this DPA. This DPA is subject to the limitations of liability set forth in the Agreement.