Data Protection Addendum
(for Audience Town Platform Terms)

1. Introduction

This Data Protection Addendum (this "**Addendum**") sets forth the terms under State Privacy Laws pursuant to which Company (the "**Disclosing Party**") may transmit, disclose, or otherwise make available Personal Data to Audience Town (the "**Receiving Party**") for Advertising Purposes (defined below). The Disclosing Party and Receiving Party are referred to herein as a "**Party**" or "**Parties**." This Addendum supplements and forms part of the Agreement.

1.1. Audience Town's receipt of Personal Data on the Audience Town Platform

Audience Town collects or receives certain Personal Data from Company and as the Receiving Party will act as a Controller or Processor as further described in Section 3 of this DPA.

For clarity, Audience Town generally receives Personal Data from Company in the following ways:

- Company onboards Company Data to the Audience Town Platform
- Company discloses Personal Data collected by the AT Pixel on Company's digital properties

2. Definitions

For purposes of this Addendum, the following terms will have the meaning ascribed below:

2.1. "Advertising Purposes"

means all Restricted Purposes in addition to (i) activities that constitute Targeted Advertising or Cross-Context Behavioral Advertising under State Privacy Laws, including any processing that involves displaying ads to a Consumer that are selected based on the Consumer's cross-context behaviors, (ii) creating or modeling audiences, including creating or supplementing user profiles for such purposes.

2.2. "CCPA"

means the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020, and any regulations promulgated thereunder.

2.3. "Data Breach"

means "breach of the security of the system," "security breach," "breach of security," "breach of system security," and other analogous terms referenced in State Privacy Laws.

2.4. "Restricted Processing"

means Processing only for Restricted Purposes.

2.5. "Restricted Processing Signal"

means any flag or signal indicating that a Consumer has opted out of the Sale, Sharing, or Processing for purposes of Targeted Advertising of their Personal Data, including without limitation those flags or signals sent through the IAB Global Privacy Protocol, or other signaling system required by State Privacy Laws.

2.6. “Restricted Purposes”

means advertising-related Processing that qualifies as a Business Purpose, including Processing for purposes of auditing; security and integrity; debugging; short term, transient uses; analytics; providing advertising or marketing services that do not include Cross-Contextual Behavioral Advertising, Targeted Advertising, or profiling; internal research; and efforts to improve quality and safety. Restricted Purposes include as applicable, first-party advertising, contextual advertising, frequency capping, ad selection and sequencing, measurement, fraud detection and prevention, and ensuring and measuring viewability, each only to the extent such activity (i) is permissible for a Processor to perform under the applicable State Privacy Laws; and (ii) does not result in a Sale or Sharing of Personal Data or constitute Processing of Personal Data for Targeted Advertising purposes.

2.7. “State Privacy Laws”

means applicable state privacy laws in the United States including the CCPA, the Colorado Privacy Act, the Connecticut Act Concerning Personal Data Privacy and Online Monitoring of 2022, the Delaware Personal Data Privacy Act; the Iowa Consumer Data Protection Act; the Montana Consumer Data Privacy Act; the Nebraska Data Privacy Act; the New Hampshire Privacy Law; the New Jersey Privacy Act; the Oregon Consumer Privacy Act; the Tennessee Information Protection Act; the Texas Data Privacy and Security Act; the Utah Consumer Privacy Act of 2022, the Virginia Consumer Data Protection Act, and all other equivalent or similar laws and regulations relating to Personal Data , in each case as amended and including any regulations promulgated thereunder.

2.8. “Business,”

“Business,” “Business Purpose,” “Commercial Purpose,” “Consumer,” “Controller,” “Cross-Context Behavioral Advertising,” “Deidentified,” “De-identified Data,” “Personal Data,” “Personal Information,” “Process(-ing)” “Processor,” “Sale,” “Sell,” “Service Provider,” “Share,” “Targeted Advertising” and “Third Party” shall have the meanings ascribed to them in State Privacy Laws.

2.9 "Controller,"

References in this Addendum to “Controller,” “Personal Data,” and “Processor” include “Business,” “Personal Information,” and “Service Provider” respectively.

3. Roles

With respect to the Processing of Personal Data, each Party acts as a Controller in its capacity as the Disclosing Party or the Receiving Party, as applicable, unless a Restricted Processing Signal is present or the Processing by the Receiving Party is otherwise solely for Restricted Purposes, in which case Receiving Party acts as a Processor and Processes the Personal Data on behalf of Disclosing Party (which may operate as either the Controller or a Processor to another Controller).

4. Mutual Processing Obligations

Each Party will:

4.1. Comply with its respective obligations under State Privacy Laws with respect to the Processing of Personal Data.

4.2. Provide Consumers with a clear and conspicuous ability to opt out of the Sale, Sharing, or Processing of their Personal Data for purposes of Targeted Advertising, in compliance with State Privacy Laws. If a Consumer opts out, Disclosing Party will (i) not Process such Consumer's Personal Data for Targeted Advertising purposes and (ii) will either (a) not disclose such Consumer's Personal Data to any Third Party; or (b) transmit a Restricted Processing Signal in conjunction with any disclosures of such Consumer's Personal Data to any Third Party.

4.3. Not modify any Restricted Processing Signal received from a Disclosing Party.

4.4. Transmit all Restricted Processing Signals received in conjunction with Personal Data to any recipients of such Personal Data.

4.5. Comply with requirements set out in State Privacy Laws for processing Deidentified Data, including by:

- 4.5.1. Not attempting to re-identify any such data;
- 4.5.2. Using reasonable administrative, technical, and organizational measures to prevent any re-identification of any such data or any inadvertent release of any such data; and
- 4.5.3. Publicly committing both to maintain and use the Deidentified Data in de-identified form and not to attempt to re-identify any such data.

4.6. To the extent acting as a Disclosing Party:

- 4.6.1. Provide all notices and obtain any consents required by State Privacy Laws necessary to permit each Party to Process Personal Data in accordance with this Addendum; and
- 4.6.2. To the extent providing Personal Data originally collected by another Controller, (i) contractually obligate such Controller to provide all notices and obtain any consents required by State Privacy Laws necessary to permit each Party to Process Personal Data in accordance with this Addendum and (ii) take reasonable steps to ensure compliance with such contractual obligations.

4.7. To the extent acting as a Receiving Party, comply with:

- 4.7.1. Section 5 (CCPA Third Party Terms) when Processing Personal Data subject to the CCPA and without a Restricted Processing Signal present.
- 4.7.2. Section 6 (Processor Obligations), when Processing Personal Data received with a Restricted Processing Signal present.

5. CCPA Third Party Terms

5.1. Applicability

This Section 5 (CCPA Third Party Terms) applies only when the Receiving Party Processes Personal Data from the Disclosing Party (i) that is subject to the CCPA; and (ii) no Restricted Processing Signal is present.

5.2. Purpose Limitations

Disclosing Party makes Personal Data available to Receiving Party only for Advertising Purposes. Receiving Party will Process Personal Data only for such Advertising Purposes, and in accordance with its obligations and any restrictions in the Agreement.

5.3. CCPA Compliance; Notification of Determination of Noncompliance

Receiving Party will comply with applicable obligations under the CCPA, including by providing an appropriate level of privacy protection as required by the CCPA, and will notify Disclosing Party without undue delay if Receiving Party determines it can no longer meet its obligations under the CCPA.

5.4. Verification of CCPA Compliance

Upon Disclosing Party's reasonable request, Receiving Party will provide the following to Disclosing Party to demonstrate Receiving Party's Processing of Personal Data consistent with Disclosing Party's obligations under the CCPA:

- 5.4.1. A copy of a certificate issued for security verification reflecting the outcome of an audit conducted by an independent third-party auditor; or
- 5.4.2. Any other information the Parties agree is reasonably necessary for Disclosing Party to verify Receiving Party's Processing is consistent with Disclosing Party's obligations under the CCPA, such as an attestation.

5.5. Unauthorized Use Remediation

If Disclosing Party reasonably believes that Receiving Party is engaged in the unauthorized use of Personal Data provided by Disclosing Party, Disclosing Party may notify Receiving Party of such belief using the contact information provided in the Agreement, and the Parties will work together in good faith to stop or remediate the allegedly unauthorized use of such Personal Data, as necessary.

5.6. Onward Disclosure Obligations

To the extent permitted by the Advertising Purposes and the Agreement, if Receiving Party makes an onward disclosure of Personal Data provided to it by Disclosing Party, including through any Sale or Sharing of the Personal Data, Receiving Party will impose terms that are substantially similar to the terms imposed on Receiving Party by Section 4 (Mutual Processing Obligations), this Section 5 (CCPA Third Party Terms), and Attachment 2 below (DOJ Rule on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern).

6. Processor Obligations

6.1. Applicability

This Section 6 (Processor Obligations) applies only to the extent Receiving Party Processes Personal Data with a Restricted Processing Signal present that has been delivered to Receiving Party or the Processing by the Receiving Party is otherwise solely for Restricted Purposes. For avoidance of doubt, a Restricted

Processing Signal that is not passed in the bidstream or other data feed, such as in the case where a consent management platform removes or truncates such signal, may not be delivered.

6.2. Purpose Limitations

Receiving Party will Process Personal Data in accordance with its obligations in the Agreement and only for Restricted Purposes, as further described in Attachment 1. Receiving Party will not:

- 6.2.1. Process Personal Data for Targeted Advertising purposes; or
- 6.2.2. Sell or Share Personal Data.

6.3. Assistance

Receiving Party will assist Disclosing Party with State Privacy Laws compliance by:

- 6.3.1. Assisting the Disclosing Party in responding to Consumer requests made pursuant to State Privacy Laws, provided that Disclosing Party must provide to Receiving Party all information necessary for it to provide such assistance or respond to a Consumer request when required by State Privacy Laws;
- 6.3.2. Contributing to data protection impact assessments where required by State Privacy Laws;
- 6.3.3. Offering reasonable notice and assistance to Disclosing Party in the event Receiving Party experiences a Data Breach, including to help Disclosing Party satisfy its Data Breach notification obligations under State Privacy Laws; and
- 6.3.4. Implementing reasonable security procedures and practices appropriate to the nature of the Personal Data and designed to protect such Personal Data from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with State Privacy Laws.

6.4. Confidentiality

Receiving Party will treat Personal Data from Disclosing Party as confidential and subject each person that Processes such Personal Data to an appropriate obligation of confidentiality.

6.5. Further Disclosures

If Receiving Party further discloses Personal Data provided by Disclosing Party, Receiving Party will:

- 6.5.1. Ensure it has in place a written agreement with any such recipient that obligates the recipient to comply with terms at least as protective as the terms set out in this Section 6 (Processor Obligations) and Attachment 2 below (DOJ Rule on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern);
- 6.5.2. Ensure any Restricted Processing Signal is transmitted with the Personal Data to the recipient; and
- 6.5.3. To the extent required by State Privacy Laws, provide Disclosing Party notice of the planned transmission to any subcontractor and an opportunity to object.

6.6. Deletion and Return of Personal Data

Upon the earlier of any request by Disclosing Party or without undue delay following termination of the

Agreement, Data Recipient will delete, return, or de-identify in accordance with State Privacy Laws Personal Data provided to Receiving Party by Disclosing Party, unless retention of the Personal Data is required by applicable law.

6.7. Audits

Upon Disclosing Party's reasonable request, Receiving Party will provide the following to Disclosing Party to enable Disclosing Party to audit Receiving Party's compliance with this Section 6 (Processor Obligations):

- 6.7.1. A copy of a certificate issued within 12 months of the Disclosing Party's Request reflecting the outcome of an audit conducted by an independent and qualified third-party auditor using an appropriate and accepted control standard or framework and audit procedure; or
- 6.7.2. Any other information or attestation the Parties agree is reasonably necessary for Disclosing Party to verify that Receiving Party's Processing is consistent with Disclosing Party's obligations under the CCPA.

6.8. Additional CCPA Processing Obligations

If Personal Data provided to Receiving Party by Disclosing Party is subject to the CCPA, in addition to the obligations set out in Sections 6.1 - 6.7 above, Receiving Party will:

- 6.8.1. Not retain, use, or disclose the Personal Data outside of the direct business relationship with Disclosing Party or for any purpose, including Commercial Purposes, other than the Restricted Purposes, unless otherwise permitted by the CCPA.
- 6.8.2. Upon notice from Disclosing Party of its reasonable belief that Receiving Party is Processing Personal Data in an unauthorized manner, cooperate with Disclosing Party in good faith to stop or remediate the allegedly unauthorized use of such Personal Data, as necessary, such as by providing documentation verifying certain practices.
- 6.8.3. Notify the Disclosing Party without undue delay if Receiving Party determines it can no longer meet its obligations under the CCPA.
- 6.8.4. Except to Process for the Restricted Purposes or as otherwise permitted by the CCPA, not combine the Personal Data provided to Receiving Party by Disclosing Party with Personal Data received from or on behalf of another person or source or that Receiving Party collects from its own interactions with Consumers.

7. Miscellaneous

7.1. Conflicts

Except as provided in Section 5.2, if there is any inconsistency or conflict between this Addendum and the Agreement, then this Addendum will govern, regardless of whether any language in the Agreement purports to state that the Agreement is the controlling document. The provisions of this Addendum may not be amended, except by an agreement to specifically amend this Addendum in writing signed by the Parties.

7.2. Counterparts

This Addendum may be executed in several counterparts (including delivery via facsimile or electronic mail), each of which will be deemed to be an original but all of which together will constitute one and the same instrument.

7.3. Amendment

This Addendum may not be amended except in a writing executed by both Parties

7.4. Survival

This Addendum will survive any expiration or termination of the Agreement.

7.5 Data Security

When Audience Town acts as a Processor, the technical and organizational measures to protect the security of Company Data as set forth in Attachment 3 will apply.

Attachment 1: Description of Processing (Processing for Restricted Purposes)

1.1. Nature and Purpose of Processing

Data Recipient Processes the Personal Data it receives for the Restricted Purposes, as further described in Section 2.6 of the DPA.

1.2. Types of Personal Data Processed.

- Offline identifiers such as name, email addresses, postal addresses
- Online identifiers such as cookie IDs, mobile ad identifiers, hashed emails
- Information based on consumer's browsing activity such as behavioral or interest data
- Information about browsers and devices used
- Non-precise geolocation information such as IP addresses or zip code information
- Real estate transactions information such as mortgage type or property tax information
- Demographic information such as a age, gender, occupation

Attachment 2: DOJ Rule on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern

The Disclosing Party provides the Receiving Party access to Personal Data for the purposes set forth in the Agreement, including the DPA. The Receiving Party is prohibited from engaging or attempting to engage in, or permitting others to engage or attempt to engage in the following: (a) selling, licensing of access to, or other similar commercial transactions, such as reselling, sub-licensing, leasing, or transferring in return for valuable consideration, the Personal Data or any part thereof, to countries of concern or covered persons, as defined in 28 CFR part 202; and

Where the Receiving Party knows or suspects that a country of concern or covered person has gained access to Personal Data through a data brokerage transaction, the Receiving Party will immediately inform the Disclosing Party. Failure to comply with the above will constitute a breach of the Agreement and may constitute a violation of 28 CFR part 202.

Attachment 3: Audience Town's Data Security Measures (Processing for Restricted Purposes)

Audience Town shall implement reasonable and appropriate technical, physical, and organizational measures designed to adequately safeguard and protect against a Security Incident (each, a "Security Measure"). Such Security Measures shall require Audience Town to have regard to industry standards and costs of implementation as well as taking into account the nature, scope, context, and purposes of the Processing as well as the risk of harm that may result from a Security Incident to Company. Audience Town will allow and cooperate with Company to conduct reasonable assessments or Audience Town may arrange for a qualified and independent assessor to conduct an assessment of Audience Town's policies and technical and organisational measures, at least annually and at Audience Town's expense. Audience Town shall provide a report of such assessment to Company upon request.

Audience Town will promptly and without undue delay and in any case no later than seventy-two (72) hours of becoming aware, inform Company in the event of: (i) any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosures of, or access to, Personal Information (altogether, a "Security Incident"), or (ii) any reasonable suspicion of a Security Incident, regardless of its cause. At Company's direction, Audience Town will provide all relevant information and assistance required by Company to investigate, mitigate and respond to a Security Incident, including at a minimum, any information or assistance required by applicable privacy and data security laws, rules and regulations.