

DATA PROCESSING ADDENDUM

[Last Updated: October 2021]

This Data Processing Addendum (“**DPA**”) forms an integral part of the Master Service Agreement (“**MSA**”) by and between Trinity including any of its affiliated companies which provides services in connection with the MSA, and the Publisher (both as defined under the MSA), and applies to the extent that Trinity Processes Publisher Data (as defined below), or has access to Publisher Data, in the course of its performance under the MSA.

This DPA forms an integral part of the MSA, and is incorporated therein by reference. Definitions used herein shall have the meaning assigned to them under the MSA.

This DPA sets forth the parties’ responsibilities and obligations regarding the Processing of Publisher Data during the engagement between the parties and under the MSA.

1. DEFINITIONS

- 1.1. “**CCPA**” means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. Seq.
- 1.2. “**Controller**,” “**Processor**,” “**Personal Data**,” “**Data Subject**,” “**Processing**” (and “**Process**”), “**Personal Data Breach**,” “**Special Categories of Personal Data**” and “**Supervisory Authority**” shall all have the meanings given to them in EU Data Protection Law. The terms “**Business**,” “**Business Purpose**,” “**Consumer**,” “**California Consumer**,” “**Service Provider**,” “**Sale**” (and “**Sell**”) shall have the same meanings as ascribed to them in the CCPA. “**Data Subject**” shall also mean and refer to a “**Consumer**,” as such term is defined in the CCPA. “**Personal Data**” shall also mean and refer to “**Personal Information**,” as such term is defined in the CCPA.
- 1.3. “**Data Protection Law**” means any and all applicable privacy and data protection laws and regulations, including, where applicable, the EU Data Protection Law and the CCPA, as may be amended or superseded from time to time.
- 1.4. “**EU Data Protection Law**” means the (i) EU General Data Protection Regulation (Regulation 2016/679) (“**GDPR**”); (ii) Regulation 2018/1725; (iii) the EU e-Privacy Directive (Directive 2002/58/EC), as amended (“**e-Privacy Law**”); (iv) any national data protection laws made under, pursuant to, replacing or succeeding (i) and (ii); (v) any legislation replacing or updating any of the foregoing; and (vi) any judicial or administrative interpretation of any of the above, including any binding guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant Supervisory Authority.
- 1.5. “**IAB TCF Policy**” means the IAB Europe Transparency & Consent Framework – Policies Version 2020-11-18.3.2a available at: https://iabeurope.eu/wp-content/uploads/2020/11/TCF_v2-0_Policy_version_2020-11-18-3.2a.docx-1.pdf.
- 1.6. “**ID**” means (i) a unique identifier stored on an end-user’s device, (ii) a unique identifier generated on the basis of a device's information, or (iii) an online identifier associated with a particular device.
- 1.7. “**Publisher Data**” means Personal Data supplied by the Publisher to Trinity pursuant to the MSA or which Trinity generates, collects, stores, transmits, or otherwise processes on behalf of the Publisher in connection with the MSA related to the Digital Asset's end users.

- 1.8. **"Security Incident"** means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Publisher Data. For the avoidance of doubt, a Personal Data Breach will be defined as a Security Incident under this DPA.
- 1.9. **"Standard Contractual Clauses"** mean the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council adopted by the European Commission Decision 2021/914 of 4 June 2021, which may be found here: [Standard Contractual Clauses](#).

2. PARTIES' ROLES

- 2.1. The parties acknowledge that in relation to Publisher Data, as between the parties, Publisher is the Controller of Publisher Data and that Trinity, in providing the Services is acting as a Processor on behalf of the Publisher. For the purpose of the CCPA (and to the extent applicable), the Publisher is the Business and Trinity is the Service Provider. Where applicable, Publisher Data may be collected and stored by Trinity's Advertisers as part of the Services, however, such advertisers shall not be considered to be Trinity's Sub-Processors.
- 2.2. Trinity is also a Controller of certain Personal Data related to the Publisher, such as (without limitation) Publisher's registration data, the contact details of Publisher's personnel, or the Publisher's contact information (in the event the Publisher contacts Trinity via email or through its website) ("**Trinity Data**"). Trinity Data shall be used and processed in accordance with our Privacy Policy available [here](#) and is not governed by this DPA which governs solely the processing of Publisher Data.
- 2.3. The purpose, subject matter, and duration of the Processing carried out by Trinity on behalf of the Publisher, the nature and purpose of the Processing, the types of Personal Data, and categories of Data Subjects are described in **ANNEX I** attached hereto.

3. REPRESENTATIONS AND WARRANTIES

- 3.1. The Publisher represents and warrants that: (i) its Processing instructions shall comply with applicable Data Protection Law; and (ii) it will comply with Data Protection Law, specifically with regards to the lawful basis principal for Processing Personal Data.
- 3.2. Trinity represents and warrants that: (i) it shall process Publisher Data, as set forth under Article 28(3) of the GDPR, on behalf of the Publisher, in order to provide the Service and internal operations under the Services, and for the pursuit of a Business Purpose as set forth under the CCPA, all in accordance with Publisher's written instructions including the MSA and this DPA; (ii) in the event Trinity is required under applicable laws, including Data Protection Law or any union or member state regulation, to Process Publisher Data other than as instructed by the Publisher, Trinity shall inform the Publisher of such requirement prior to Processing such Publisher Data, unless prohibited under applicable law; and (iii) it shall provide reasonable cooperation and assistance to the Publisher in ensuring compliance with its obligation to carry out data protection impact assessments with respect to the processing of Publisher Data and to consult with the Supervisory Authority (as applicable).
- 3.3. If the EU Data Protection Law or the CCPA do not apply to the Publisher, then the Publisher must abide by any other Data Protection Law and data security laws and regulations that apply to it, and at a minimum Publisher shall: (i) obtain and maintain any and all authorizations, permissions and informed consents, as may be necessary under applicable laws and regulations, in order to

allow Trinity to lawfully collect, handle, retain, process and use the processed data within the scope of the Services; (ii) substantiate the legal basis and legitimize, pursuant to applicable law, the collection of Publisher Data through the Services; (iii) have, properly publish and abide by an appropriate privacy policy that complies with all applicable Data Protection Law.

4. PROCESSING OF PERSONAL DATA AND COMPLIANCE WITH DATA PROTECTION LAW

- 4.1. The Publisher represents and warrants that Special Categories of Personal Data or Sensitive Data shall not be Processed or shared in connection with the performance of the Services unless Trinity agrees in writing for such data to be shared with it. Unless otherwise agreed to in writing by the parties, the Publisher shall not share any Personal Data with Trinity relating to children under the age of 16.
- 4.2. The Publisher acknowledges that Trinity is a "Vendor" as defined under the IAB TCF Policy. As between the parties, the Publisher undertakes, accepts and agrees that the Data Subjects (i.e., the Digital Asset's end users) do not have a direct relationship with Trinity and that Trinity relies on Publisher's lawful basis (as required under applicable Data Protection Law), including in Trinity's capacity as a Vendor. In the event that consent is needed in accordance with the Data Protection Law or under the IAB TCF Policy, the Publisher shall ensure that it obtains a proper act of consent from Data Subjects. Furthermore, the Publisher will maintain and display all necessary and appropriate notices in accordance with applicable Data Protection Law and other relevant privacy requirements in order to allow it to Process Publisher Data and enable the lawful transferring and Processing of Publisher Data to and by Trinity and Trinity's Advertisers (where applicable under the engagement between the parties). The Publisher shall also where applicable, provide the Data Subjects with the ability to opt-out of the above-mentioned Processing. In the event a Data Subject's consent is required under Data Protection Law or pursuant to the IAB TCF Policy, Publisher shall be fully responsible to support and transmit to Trinity, through the Services, the Signal (as such term is defined under the IAB TCF Policy) and the parameters of the Data Subject's consent, or the opt-out settings, as applicable. The Publisher shall maintain a record of all consents obtained from Data Subjects, which shall include: (i) the time and date that the consent was obtained; (ii) the information presented to the Data Subject in connection with their consent; (iii) details of the mechanism used to obtain consent; and (iv) a record of the same information included in (i)-(iii) above in relation to all withdrawals of consent by each Data Subject. The Publisher shall make these records available to Trinity promptly upon request. Trinity shall not be liable with respect to the obtaining of any required consent or with respect to the Signal provided by the Publisher and shall transfer the Signal "as is" and as it was provided to Trinity by the Publisher.

5. RIGHTS OF DATA SUBJECTS AND THE PARTIES' COOPERATION OBLIGATIONS

It is agreed that where Trinity receives a request from a Data Subject or an applicable authority in respect of Publisher Data Processed by Trinity, where relevant, Trinity will direct the Data Subject or the applicable authority to the Publisher in order to allow the Publisher to respond directly to the Data Subject's or the applicable authority's request unless otherwise required under applicable laws. Both parties shall provide each other with commercially reasonable cooperation and assistance in relation to the handling of a Data Subject's or applicable authority's request, to the extent permitted under Data Protection Law.

6. TRINITY'S PERSONNEL

Trinity shall take reasonable steps to ensure: (i) the reliability of its staff and any other person acting under its supervision who may come into contact with, or otherwise have access to and Process Publisher Data; (ii) that persons authorized to process the Publisher Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and (iii) that such personnel are aware of their responsibilities under this DPA and any applicable Data Protection Laws.

7. DO NOT SELL PERSONAL INFORMATION

- 7.1. It is hereby agreed that any sharing of Publisher Data between the parties is made solely in order to fulfill a Business Purpose and Trinity does not receive or process any of Publisher Data as consideration for the Services. Thus, such Processing of Publisher Data shall not be considered as a "Sale" under the CCPA.
- 7.2. Notwithstanding the above, the process of sharing Publisher Data by Trinity with Trinity's Advertisers (where applicable to the engagement between the parties) may be considered a Sale under the CCPA. The Publisher is therefore solely liable for its compliance with the CCPA with respect to its use of the Services. It is the Publisher's sole responsibility and liability to determine whether the sharing or transferring of Publisher Data during the course of the Services constitutes a Sale of Publisher Data and it is also the Publisher's responsibility to comply with the applicable CCPA requirements in this regard, including providing a "**Do Not Sell My Personal Information**" signal for end-users who have exercised their right to opt-out, where applicable.

8. SUB-PROCESSOR

- 8.1. The Publisher acknowledges that Trinity may transfer Publisher Data to and otherwise interact with third party data processors ("**Sub-Processor**"). Publisher hereby, authorizes Trinity to engage and appoint such Sub-Processors to Process Publisher Data, as well as permits each Sub-Processor to appoint a Sub-Processor on its behalf. Trinity may continue to use those Sub-Processors already engaged by the Trinity, as listed in **ANNEX III** (and as amended from time to time), and Trinity may engage an additional or replace an existing Sub-Processor to process Publisher Data, subject to providing prior notice to the Publisher. In case the Publisher has not objected to the adding or replacing of a Sub-Processor within up to five (5) days as of Trinity's notice, such Sub-Processor shall be considered as approved by the Publisher. In the event the Publisher objects to the adding or replacing of a Sub-Processor, Trinity may, under Trinity's sole discretion, suggest the engagement of a different Sub-Processor for the same course of services, or otherwise terminate the MSA. Notwithstanding the above, it is hereby agreed that Publisher may object to the replacement or addition of any particular Sub-Processor solely on reasonable grounds related to noncompliance with applicable Data Protection Law, and shall be entitled to terminate the MSA, solely in the event that Trinity failed to offer an applicable alternative Sub-Processor.
- 8.2. Trinity shall, where it engages any Sub-Processor, impose, through a legally binding contract between Trinity and the Sub-Processor, data protection obligations similar to those set out in this DPA. Trinity shall ensure that such agreement with the Sub-Processor will require the Sub-

Processor to provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of Data Protection Law. Trinity shall, upon written request by the Publisher, provide the Publisher with the applicable contract and any subsequent amendments thereto. To the extent necessary to protect trade secrets or other confidential information, as shall be determined by Trinity in its sole discretion, Trinity may redact the text of the agreement before sharing the copy with the Publisher.

- 8.3. Trinity shall remain responsible to the Publisher for the performance of the Sub-Processor's obligations in accordance with this DPA. Trinity shall notify the Publisher of any failure by the Sub-Processor to fulfill its contractual obligations.

9. TECHNICAL AND ORGANIZATIONAL MEASURES

- 9.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and without prejudice to any other security standards agreed upon by the parties, Trinity shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and in accordance with industry practices to protect data from a Security Incident. The parties acknowledge that security requirements are constantly changing and that effective security requires the frequent evaluation and regular improvement of outdated security measures.
- 9.2. The security measures are further detailed in **ANNEX II**.

10. SECURITY INCIDENT

- 10.1. Trinity will notify the Publisher upon becoming aware of any confirmed Security Incident involving the Publisher Data in Trinity's possession or control, as determined by Trinity in its sole discretion. Trinity will, in connection with a confirmed Security Incident affecting the Publisher Data: (i) take such steps as are necessary to contain, remediate, minimize any effects of and investigate any Security Incident and to identify its cause; (ii) reasonably co-operate with the Publisher and provide the Publisher with such assistance and information as it may reasonably require in connection with the containment, investigation, remediation or mitigation of the Security Incident; (iii) notify the Publisher in writing of any request, inspection, audit or investigation by a Supervisory Authority or other authority related to the Publisher Data; (iv) keep the Publisher informed of all material developments in connection with the Security Incident and execute a response plan to address the Security Incident; and (v) co-operate with the Publisher and assist Publisher with its obligation to notify the affected individuals in the case of a Security Incident.
- 10.2. Trinity's notification or response regarding a Security Incident under this Section 10 shall not be construed as an acknowledgment by Trinity of any fault or liability with respect to the Security Incident.

11. AUDIT RIGHTS

- 11.1. Trinity shall respond adequately with respect to reasonable inquiries from the Publisher regarding the Processing of Publisher Data in accordance with this DPA. Trinity shall make

available to the Publisher reasonable information necessary to demonstrate compliance with the obligations under the EU Data Protection Law.

- 11.2. Trinity shall make available, solely upon prior written notice and no more than once per year (except for in the case of a Security Incident), information necessary to reasonably demonstrate compliance with this DPA to a reputable auditor nominated by the Publisher, and shall allow for audits, including inspections, by such reputable auditor solely concerning the Processing of the Publisher Data ("**Audit**") in accordance with the terms and conditions hereunder. The Audit shall be subject to the terms of this DPA and standard confidentiality obligations (including towards third parties). Trinity may object to an auditor appointed by the Publisher in the event Trinity reasonably believes that the auditor is not suitably qualified or independent, is a competitor of Trinity, or is otherwise unsuitable ("**Objection Notice**"). The Publisher will appoint a different auditor or conduct the Audit itself upon its receipt of an Objection Notice from Trinity. Publisher shall bear all expenses related to the Audit and shall (and ensure that each of its auditors shall) throughout such Audit, avoid causing any damage, injury, or disruption to Trinity. Any and all conclusions of such Audit shall be confidential and reported back to Trinity immediately.

12. DATA TRANSFER

- 12.1. The Publisher acknowledges and agrees that in order to be provided with the Services, Trinity may access and Process the Publisher Data from territories that are not part of the EEA. Moreover, the Publisher further agrees that Trinity may engage a Sub-Processor which is not established in the EEA, in accordance with Section 8. In the event the Processing includes transferring of Publisher Data to a country that has not received the adequacy decision from the European Commission or is not exempt under Article 49 of the GDPR ("**Restricted Transfer**"), the following shall apply:
- 12.1.1. In order to maintain the integrity, security, and confidentiality of the Publisher Data, a Restricted Transfer shall be subject, in addition to the terms of this DPA, to the terms and obligations of **Module II** of the [Standard Contractual Clauses](#) in which event Trinity shall be deemed as the Data Importer and the Publisher shall be deemed as the Data Exporter.
- 12.1.2. The purpose and description of the transfer shall be detailed in **ANNEX I**.
- 12.2. **Specifically, EU-US Transfers:** Following Schrems II, Case No. C-311/18, and related guidance from Supervisory Authorities, the parties acknowledge that supplemental measures may be needed with respect to EU-U.S. data transfers where Publisher Data may be Processed in the US. The Publisher acknowledges and warrants that Publisher's EU operations involve merely ordinary commercial services, and any EU-U.S. transfers of Publisher Data contemplated by this DPA involve ordinary commercial information, which is not the type of data that is of interest to, or generally subject to, surveillance by U.S. intelligence agencies. Accordingly, Trinity acknowledges that it will not provide access to Publisher Data to any US government or intelligence agency, except where under Trinity's sole discretion and legal counsels advice it is necessary under the US law or valid and binding order of government authority (such as pursuant to a court order). In any such case, Trinity will attempt to redirect the law enforcement agency to request the data directly from the Publisher. Unless Trinity is legally prohibited from doing so, in any such case Trinity will: (1) provide the Publisher notice of the

demand no later than ten (10) days after such demand is received to allow the Publisher to seek recourse or another appropriate remedy to adequately protect the privacy of EEA Data Subjects; and (2) in any event, provide access only to such Publisher Data as is strictly required by the applicable law or binding order (having used reasonable efforts to minimize and limit the scope of any such access), as determined solely by Trinity's legal advisors.

13. CONFLICT

In the event of a conflict between the terms and conditions of this DPA and the MSA or IO, this DPA shall prevail.

14. TERM & TERMINATION

- 14.1. This DPA shall be effective as of the Effective Date and shall remain in force until the MSA terminates.
- 14.2. Trinity shall be entitled to terminate this DPA or terminate the Processing of Publisher Data in the event that Processing of Publisher Data under the Publisher's instructions or this DPA infringe applicable legal requirements.

ANNEX I

DETAILS OF PROCESSING AND TRANSFERRING OF PUBLISHER DATA

This Annex I include certain details of the Processing and transferring of Publisher Data as required by Article 28(3) GDPR and the Standard Contractual Clauses.

Categories of data subjects whose personal data is processed or transferred:

- End users of Publisher's Digital Assets, interacting with Trinity's Streaming Feature.

Categories of personal data processed and transferred:

- IDs - such as the end-user's IP address and IDFA.

Sensitive data processed or transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measure:

NA

Nature of the processing and transfer:

Analytics and optimization

Purpose(s) for which the Publisher Data is processed or transferred on behalf of the Publisher:

The Publisher Data is processed by Trinity on behalf of the Publisher to provide the Services under the MSA and for internal operations.

Duration of the processing:

Processing shall be carried out in connection with the provision of the Services. The duration shall be for the duration of the Term.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

The processing occurs on a continuous basis.

For transfers to (sub-) processors, also specify the subject matter, nature, and duration of the processing

Sub-Processors are used to provide hosting services and enable the provision of the Services by the Company.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

The security objectives of the Company are identified and managed to maintain a high level of security and consists of the following (concerning all data assets and systems):

- **Availability** - information and associated assets should be accessible to authorized users when required. The computer network must be resilient. The Company must detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems, and information.
- **Confidentiality** - ensuring that information is only accessible to those authorized to access it, on a need-to-know-basis.
- **Integrity** - safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorized modification, of electronic data.

Physical Access Control

The Company ensures the protection of the physical access to the data servers which store the Personal Data. The Personal Data processed by the Company is stored on Amazon Web Services (AWS). Further, the Company secures the physical access to its offices (i.e., - alarm systems, code locks) and maintain records of any physical access to the protected Personal Data in order to ensure that solely authorized individuals such as employees and authorized external parties (maintenance staff, visitor, etc.) can access the Company's offices.

Security Risk Analysis and Management.

The Company conducting an assessment of the potential risks and vulnerabilities of the Company's Personal Data to ensure the confidentiality, integrity, and availability of electronic Personal Data. The Company's servers include an automated back-up procedure.

System Control

Access to the Company's database is highly restricted in order to ensure that solely the appropriate prior approved personnel can access the Company's Personal Data. Safeguards related to remote access and wireless computing capabilities are in implemented therein. Employee are required to comply with the Company's password policy when composing a password in order to allow strict access or use related to Personal Data all in accordance with position, and solely to the extent such access or use is required. Electronic procedures in order to terminate an inactive session are also in use by the Company.

Data Access Control

There are restrictions in place to ensure that the access to the Personal Data is restricted to employees which have a permission to access it. The Personal Data information shall not be accessed, modified, copied, used, transferred or deleted without specific authorization. The access to the Personal Data information, as well as any action performed involving the use of the Personal Data requires a password and user name, which is routinely changed, as well as blocked when applicable. Each employee is able to perform actions solely according to the permissions determined by the Company. Further, the Company has ongoing review of which employees' have authorizations, to assess whether access is still required.

Company revokes access immediately upon termination of employment. Authorized individuals can solely access Personal Data that is established in their individual profiles.

Organizational and Operational Security

The Company invests efforts and resources in order to ensure compliance with the Company's security practices, as well as continuously provides employees on-going training and periodic updates regarding Company's security procedures. The Company strives to raise awareness to the risk involved in the processing of Personal Data. In addition, the Company implemented applicable safeguards for its hardware and software, including web content filtering, firewalls and anti-virus software ("**Protection Measures**") on applicable Company hardware, software or employee's computer, in order to protect against virus, worms, Trojan identifications or any other malicious software.

Transfer Control

All transfer of Personal Data between the client side and the Company's servers is protected using encryption safeguards. The Company's servers are protected by industry best standards. In addition, to the extent applicable, the Company's business partners execute an applicable Data Processing Agreement, all in accordance with applicable laws.

International Transfer

On July 16, 2020, Europe's highest court ("**CJEU**") invalidated the EU-US Privacy Shield. Additionally, on September 8, 2020, the Swiss Data Protection Authority announced in a position statement that it no longer considers the Swiss-U.S. Privacy Shield adequate for the purposes of transfers of personal data from Switzerland to the U.S.

We ensure any data transfer is done in a secure manner, in compliance with the latest EDPB recommendations concerning data transfer as well as contractually sign a Data Processing Agreement which incorporate the Standard Contractual Clauses which remain a valid data export mechanism and which automatically apply in accordance our Data Processing Agreement.

Data Retention

Personal Data is retained for as long as needed to provide the services or as required under applicable laws. Individuals may request data deletion; however, this request is not absolute and is limited, all as detailed in the Company Privacy Policy.

Job Control and Third-Party Contractors and Service Providers

All of the Company's employees are required to execute an employment agreement which includes confidentiality provisions as well as applicable provisions binding them to comply with applicable data security practices. In the event of a breach of an employee's obligation or non-compliance with the Company's policies, the Company implements certain repercussions in order to ensure compliance with the Company's policies. The Company ensures that it enters into data protection agreements with all of its clients and service providers.

ANNEX III

List of Sub-Processors

Name	Address	Server location	Description of the processing
Amazon Web Services	Amazon Web Services, Inc., 410 Terry Avenue North, Seattle, WA 98109-5210, ATT	US	Cloud Storage Server