Data Protection Addendum

This Data Protection Addendum ("**DPA**") is incorporated into and made part of the Agreement (as defined below) referencing this DPA. This DPA governs Personal Data (as defined below) processed in connection with the Services (as defined below). This DPA sets out the terms of the Agreement governing Personal Data processing. Capitalized terms used but not defined in this DPA will have the meanings assigned to them in the Agreement.

DATA PROCESSING TERMS

1.0 Definitions

1.1 For the purpose of this DPA:

a) **"Affiliate"** has the same meaning ascribed to it in the Agreement and, if not defined in the Agreement, the term means any legal entity directly or indirectly controlling, controlled by or under common control with a party, where control means the ownership of a majority share of the stock, equity or voting interests of such entity.

b) "**Agreement**" means the contractual agreement(s), including services agreements and all related orders, between Provider and Client into which this DPA has been incorporated by reference.

c) "**Business Data**" means any Personal Data that relates to Client's business relationship with Provider, including contact information of individuals using the Services or acting as administrative or business representatives with respect to the Services and transaction data (including financial account data).

d) "**Business Data Purposes**" has the meaning given to it in Section 6.2.

e) "**Client**" means the party(ies) to the Agreement identified in the Agreement as the "Client" or "Customer".

f) "**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of processing of Personal Data.

g) "**Client Data**" means all information and data: (i) inputted or otherwise submitted by or on behalf of Client through the use of the Services; and/or (ii) collected or otherwise obtained by Provider on behalf of Client pursuant to Client's instructions in accordance with the Agreement and/or this DPA, including Third-Party Data.

h) "**Client Personal Data**" means any Personal Data included in Client Data, excluding Business Data.

i) "**Client Personal Data Purposes**" has the meaning given to it in Section 3.2.

j) "**CCBA Services**" means any Services in which Provider provides Cross-Context Behavioral Advertising.

k) "**Cross-Context Behavioral Advertising**" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications or services, other than the business, distinctly-branded website, application or service with which the consumer intentionally interacts.

l) "**Data Protection Law**" means any laws and regulations applicable to the privacy, security, protection or processing of Personal Data under the Agreement, including, where applicable and without limitation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("**GDPR**"), the GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Addendums etc.) (EU Exit) Regulations 2019 (SI 2019/419) ("**UK GDPR**"), and the California Consumer Privacy Act ("**CCPA**"), as each is amended, supplemented or replaced from time to time.

m) "**Data Subject**" means the individual to whom the applicable Personal Data relates.

n) "**Data Subject Request**" means a written request of a Data Subject received by Provider from the Data Subject or from Client by or on behalf of a Data Subject to exercise any rights conferred by Data Protection Law in relation to Client Personal Data or Business Data.

o) "**DNS Opt-Out"** means a Data Subject Request to opt out of the sale of Personal Data or the sharing of Personal Data for Cross-Context Behavioral Advertising or Targeted Advertising.

p) "**EEA**" means European Economic Area, which constitutes the member states of the European Union and Norway, Iceland and Liechtenstein.

q) "**FADP**" shall mean the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1) and Ordinances SR 235.11 and SR 235.13, as amended and applicable insofar as the data transfers are subject to the FADP and following the coming into force of FADP's revised version of 25 September 2020 on 1 January 2023 (or at the later date subject to the legislative procedure), subject to such revised version, as amended and applicable ("**Revised FADP**").

r) "**Provider**" means Mediaocean, LLC and/or its Affiliate(s) that are a direct party to the Agreement as a signatory in the capacity of "Provider".

s) "**Permitted Client Personal Data**" means Client Personal Data provided to or otherwise obtained by Provider by or on behalf of Client in compliance with Data Protection Law.

t) "**Personal Data**" means any data that relates to an identified or identifiable natural person or that otherwise meets the definition of "personal data" (or similarly defined term, such as "personal information" or "sensitive personal information") under applicable Data Protection Law.

u) "**process**", "**processed**", or "**processing**" means the collection, receipt, recording, organization, structuring, alteration, use, transmission, access, sharing, provision, disclosure, distribution, copying, transfer, storage, management, retention, deletion, combination, restriction, summarizing, aggregation, correlation, inferring, derivation, analysis, adaptation, retrieval, consultation, destruction, disposal or other handling of Personal Data or as such terms are otherwise defined under applicable Data Protection Law.

v) "**Processor**" means an entity which processes Personal Data on behalf of a Controller.

w) "**Services**" means the products and/or services provided by Provider to Client under the Agreement.

x) "**Standard Contractual Clauses**" ("**SCCs**") means the standard contractual clauses for cross-border transfers to a Third Country including the standard contractual clauses (i) published by the European Commission on June 4, 2021 governing the transfer of EEA Personal Data to Third Countries as adopted by the European Commission and the Swiss Federal Data Protection and Information Commissioner ("**Swiss FDPIC**"), available at https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en ("**EU SCCs**"); and (ii) the international data transfer addendum to the EU SCCs adopted by the UK Information Commissioner as may be applicable for transfers from the UK, available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf ("**UK Addendum**").

y) "**Third-Party Data**" means Personal Data from third party sources collected or otherwise obtained by Provider on behalf of Client pursuant to Client's instructions in accordance with the Agreement and/or this DPA.

z) "**Security Incident**" means a confirmed or reasonably suspected accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to or use of Client Personal Data.

aa) "**Sub-processor**" means another Processor appointed by a Processor.

bb) "**UK**" means the United Kingdom.

cc) References to "**Business**", "**Sell**", "**Selling**", "**Share**", "**Sharing**", "**Service Provider**", "**Supervisory Authority**", "**Targeted Advertising**" and "**Third Party**" have the meanings given to them in Data Protection Laws, as applicable.

2.0 Role of Parties

2.1 Provider as Processor or Sub-processor for Client Personal Data. For all Client Personal Data processed by Provider in connection with the Services, Client is the Controller and Provider is a Processor, except if Client is a Processor, in which case Provider is a Sub-processor of Client Personal Data. If Client is a Processor or joint Controller of Client Personal Data, then Client: (a) provides instructions in accordance with this DPA on behalf of the respective Controller (or, in the case of joint Controllers, on behalf of itself and its joint Controller); and (b) represents and warrants that Client's instructions and processing of Client Personal Data, including its appointment of Provider as a Sub-processor or Processor, have been authorized by the respective Controller (or joint Controller).

2.2 Provider and Client as Independent Controllers of Business Data. Provider and Client are each independent Controllers (and not joint Controllers) of Business Data unless expressly provided otherwise in this DPA.

3.0 Data Processing for Client Personal Data

3.1 Client Instructions. The parties agree that this DPA (including the Annexes hereto) and the Agreement constitute Client's documented instructions to Provider for the processing of Client Personal Data ("**Documented Instructions**"). Any processing required outside the scope of these Documented Instructions will require prior written agreement of the parties, except where otherwise required by applicable law.

3.2 Purposes of Client Personal Data Processing. Client discloses and Provider shall process Client Personal Data solely for the following purposes ("**Client Personal Data Purposes**"):

a. To provide the Services to or on behalf of Client and to perform operations supporting such provision of Services, including collecting, analyzing, combining, parsing and organizing Client Personal Data, deidentifying or aggregating Client Personal Data, maintaining and servicing accounts, providing customer service and technical support, processing and fulfilling orders and transactions, verifying Client information, processing payments, auditing Client's account and activities performed by or on behalf of Client in connection with the Services, providing financing, providing analytic services, providing storage and providing similar services to or on behalf of Client.

b. For Provider to exercise its rights and discharge its obligations under the Agreement and this DPA.

c. For Provider to undertake internal research for technological development and demonstration and to improve and enhance the Services and Provider's and its Affiliates' other products and services; provided that, Provider (i) does not use Client Personal Data to perform services on behalf of a person other than Client or its authorized Affiliate(s); and (ii) otherwise complies with the Provider obligations in Section 3.4 with respect to such Client Personal Data.

d. To detect, investigate, prevent and respond to Security Incidents, system or network exploits or abuse, fraudulent activity or violations of this DPA or the Agreement.

e. As necessary to comply with any applicable law, including Data Protection Law.

f. To provide advertising and marketing Services, provided that, for the purposes of advertising and marketing, Provider shall not combine: (i) Personal Data of individuals for whom Provider has received a DNS Opt-Out from, or on behalf of, Client, with (ii) Personal Data that Provider receives from another source (not on behalf of Client) or collects from Provider's own interaction with individuals (not behalf of Client).

g. For CCBA Services, to provide Cross-Context Behavioral Advertising. For the avoidance of doubt Provider is not authorized to provide Cross-Context Behavioral Advertising except in connection with the CCBA Services.

h. For other purposes as agreed in writing between Client and Provider

3.3 Client Instructions for Certain Services. ***This Section 3.3 applies only to the specifically identified Services.***

Audience Marketplace Services

a) With respect to the **Audience Marketplace Services**, Client instructs Provider to perform the following operations on Client Personal Data:

i. License, purchase or otherwise obtain Third-Party Data on behalf of Client from the third-party sources selected by Client in the Services. In taking such actions, Provider is acting on behalf of Client and not independently or as a data broker.

ii. On behalf of Client, pay all applicable fees (including for both inclusion and exclusion audience targeting segments) for Third-Party Data licensed, purchased or otherwise obtained by or on behalf of Client, and bill Client for such fees. Provider does not charge, earn or otherwise receive any fees for licensing or purchasing Third-Party Data on behalf of Client. Any fees paid to Provider in connection with licensing, purchasing or otherwise obtaining Third-Party Data on behalf of Client are for Provider's services (including platform services, API services, and processing services).

iii. Process Third-Party Data obtained on behalf of Client in accordance with Client's instructions, including Client's instructions made via the Services.

iv. Provide Client Data to the third-party sources selected by Client as necessary for such third-party sources to provide the Third-Party Data ordered by Client.

Flashtalking Social Ads Manager Audience Hub Services and/or Audience HQ

b) With respect to the **Flashtalking Social Ads Manager Audience Hub Services and/or Audience HQ**, Client instructs Provider to perform the following operations on Client Personal Data:

i. License, purchase or otherwise obtain Third-Party Data on behalf of Client, including from TransUnion ("**TU**"). In taking such actions, Provider is acting on behalf of Client and not independently or as a data broker. Third-Party Data from TU includes pseudo-anonymous IDs ("**PELs**") for the adult US population along with associated digital identifiers, such as, hashed emails, mobile ad IDs (IDFA and AAID/GAID) and IP address.

ii. On behalf of Client, pay all applicable fees for Third-Party data licensed, purchased or otherwise obtained by or on behalf of Client, and bill Client for such fees. Provider does not charge, earn or otherwise receive any fees for licensing or purchasing Third-Party Data on behalf of Client. Any fees paid to Provider in connection with licensing, purchasing or otherwise obtaining Third-Party Data on behalf of Client are for Provider's services (including platform services, API services and processing services).

iii. Ingest Client Data (including Third-Party Data) from platforms and sources selected by Client.

iv. Combine and match ingested Client Data and Third-Party Data obtained on behalf of Client and translate it into identifiers appropriate for distribution to social publishers and other distribution platforms selected by Client for activation.

v. Distribute audience segments to endpoints selected by Client.

vi. Automatically refresh/update distributed audiences based on newly ingested Client Data.

vii. Display to Client's users the size of the audience as matched by each applicable social publisher(s) or distribution platform(s) selected by Client.

viii. Display the aggregate characteristics of seed files across dimensions mentioned above.

ix. Perform lookalike modeling and distribute expanded audiences to social publishers or distribution platforms selected by Client.

x. Combine, match and/or supress Client Data and generate subsets of Client Data in accordance with Client's selections within the Services, to identify real-time audiences and segments for targeting.

xi. Conduct auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions and auditing compliance with this specification and other standards.

xii. Use Third-Party Data obtained on behalf of Client to improve and enhance Provider's products and services, provided that Provider shall not use such data to perform services on behalf of a third party.

xiii. Provide Client Data to TU and any additional third-party sources selected by Client as necessary for TU and such third-party sources to provide the Third-Party Data ordered by Client and to assist Provider in carrying out any of the activities in this Section 3.3(b).

Flashtalking FTrack Services

c) With respect to the **Flashtalking FTrack Services** (including Household IDs), Client instructs Provider to perform the following operations on Client Personal Data:

i. Collect signals from Client Data and from Data Subjects on behalf of Client, including IP address, device type, user agent, screen size and pixel size. Such collected signals constitute "Client Data" and not "Business Data".

ii. Combine signals collected to generate a unique signature which is logged and assigned a unique identifier, called an "**unique FTrack ID**". Unique Ftrack IDs constitute "Client Data" and not "Business Data". Provider may generate a "**master FTrack ID**" in the same manner it generates unique FTrack IDs, which master FTrack IDs may be used by Provider to improve and enhance its products and services, provided that Provider shall not use any master FTrack IDs to perform services on behalf of a third party. Master FTrack IDs constitute "Business Data" and not "Client Data" and Provider is the sole independent Controller of master FTrack IDs.

iii. Collect cookie identifiers ("**cookie IDs**"), from Client Data and from Data Subjects on behalf of Client. Cookie IDs constitute "Client Data" and not "Business Data".

iv. Collect activity from Client Data and from Data Subjects on behalf of Client and combine and match such activity with unique FTrack IDs. Such collected activity data constitute "Client Data" and not "Business Data".

v. Combine and match unique FTrack IDs with rejected cookie IDs, other Client Data (such as impressions, clicks and spots), and Third-Party Data (including PELS) for campaign reporting, personalization and analysis.

vi. Collect and process DNS Opt-Outs from Data Subject devices and apply such DNS Opt-Outs to all unique FTrack IDs, master FTrack IDs and cookie IDs associated with such Data Subject devices.

vii. Combine and match unique FTrack IDs with other Client Data to measure accuracy of reporting and analysis

viii. License, purchase or otherwise obtain Third-Party Data on behalf of Client, including from TU. In taking such actions, Provider is acting on behalf of Client and not independently or as a data broker. Third -Party Data from TU includes PELS for the adult US population along with associated digital identifiers, such as, hashed emails, mobile ad IDs (IDFA and AAID/GAID) and IP address.

ix. On behalf of Client, pay all applicable fees for Third-Party Data licensed, purchased or otherwise obtained by or on behalf of Client, and bill Client for such fees. Provider does not charge, earn or otherwise receive any fees for licensing or purchasing Third-Party Data on behalf of Client. Any fees paid to Provider in connection with licensing, purchasing or otherwise obtaining Third-Party Data on behalf of Client are for Provider's services (including platform services, API services, and processing services).

x. Conduct auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions and auditing compliance with this specification and other standards.

xi. Use Third-Party Data obtained on behalf of Client to improve and enhance Provider's products and services, provided that Provider shall not use such data to perform services on behalf of a third party.

xii. Provide Client Data to TU and any additional third-party sources selected by Client as necessary for TU and such third-party sources to provide the Third-Party Data ordered by Client and to assist Provider in carrying out any of the activities in this Section 3.3(c).

3.4 Provider Obligations: In connection with Provider's processing of Client Personal Data.

a) Provider is prohibited from Selling the Client Personal Data.

b) Provider is prohibited from Sharing (as such term is defined in the CCPA) Client Personal Data with third parties for Cross-Context Behavioral Advertising purposes, except as instructed by Client in connection with the CCBA Services (if any).

c) Provider is prohibited from retaining, using or disclosing Client Personal Data for any purposes other than for the Client Personal Data Purposes or as otherwise permitted by Data Protection Law.

d) Provider is prohibited from retaining, using or disclosing Client Personal Data for any commercial purposes other than for the Client Personal Data Purposes, unless expressly permitted by Data Protection Law.

e) Provider is prohibited from retaining, using or disclosing Client Personal Data outside the direct business relationship between Provider and Client, including combining or updating Client Personal Data with Personal Data received by Provider from another source (not on behalf of Client) or Provider's own independent interaction with the consumer (not on behalf of Client), unless expressly permitted by Data Protection Law.

f) Provider will comply with all Data Protection Law applicable to its role as a Processor or a Service Provider for Client Personal Data in connection with its performance under the Agreement, including providing the same level of privacy protection as required of a Business (as defined in the CCPA) by the CCPA.

g) Provider will notify Client no later than five (5) business days after it makes a determination that it can no longer meet its obligations under Data Protection Law with respect to Client Personal Data.

h) Provider shall notify Client as soon as reasonably practical if, in its opinion, any Document Instruction infringes any Data Protection Laws.

i) Client may take the reasonable and appropriate steps set forth in Section 9 to ensure that Provider uses Client Personal Data in a manner consistent with Client's obligations under Data Protection Law, including the CCPA.

j) In the event of Provider's unauthorized use of Client Personal Data or a Security Incident resulting from an act or omission of Provider, Client may, upon reasonable notice to Provider, take, or require Provider to take, reasonable and appropriate steps, as provided in Section 5.4, to stop and remediate such unauthorized use of Client Personal Data or Security Incident.

3.5 Client Compliance. Client will comply with Data Protection Law applicable to Client's role as a Controller and/or a Processor for Client Personal Data. Client, as Controller and/or Processor, represents and warrants that, in connection with Client Personal Data:

a. Client has complied, and will continue to comply, with all applicable laws relating to privacy and data protection, including the Data Protection Laws, and the provision of Client Personal Data to Provider is in strict compliance with Data Protection Laws;

b. Client has, and will continue to have, the right and all necessary permissions to transfer, or provide access to, Client Personal Data to Provider for processing in accordance with the terms of the Agreement and this DPA;

c. Client only processes Client Personal Data that has been collected in accordance with Data Protection Laws;

d. Client has in place procedures in case a Data Subject wishes to exercise their rights in accordance with Data Protection Laws;

e. Client provides Client Personal Data to Provider for the Client Personal Data Purposes in accordance with the representations Client makes to individuals in Client's privacy policy and Client does not sell Client Personal Data to Provider;

f. Client shall have the sole responsibility for the accuracy, quality, and legality of Client Personal Data;

g. Client shall provide to Provider, or otherwise have Provider process, only Client Personal Data that is Permitted Client Personal Data; Client shall be solely liable for any Client Personal Data which is made available to or obtained by Provider in excess of the Permitted Client Personal Data; and

h. Client is and will remain duly and effectively authorized to give the instructions set out herein and any additional instructions as provided pursuant to the Agreement, at all relevant times and at least for as long as the Agreement is in effect and for any additional period during which Provider is lawfully processing Client Personal Data.

4.0 Sub-processing for Client Personal Data

4.1 Sub-processors. Client authorizes Provider to engage as a Sub-processor (a) any Sub-processors listed in Annex 3 (including those listed on the link to any vendor management policy page "**Vendor Management Policy Page**") and (b) any Affiliate of Provider to process Client Personal Data in accordance with the Documented Instructions. Provider shall keep a written record of all Sub-processors and shall, on request, make a copy of this record available to Client. Provider shall remain fully liable to Client for the Sub-processor's performance, as well as for any acts or omissions of the Sub-processor as regards its processing of Client Personal Data.

4.2 Contracts with Sub-processors. Provider shall ensure, before any Sub-processor processes Client Personal Data, that the Sub-processor is contractually bound to terms that are no less restrictive and at least equally protective of Client Personal Data as those imposed on Provider under this DPA (including in relation to providing such access and assistance as Client requires from time to time) and that comply with applicable Data Protection Law. Provider shall provide copies of documentation to evidence its compliance with this clause to Client promptly on request.

4.3 Changes to Sub-processors. The Sub-processors currently engaged by Provider and the link to the Vendor Management Policy Page for Provider are listed in Annex 3. The Vendor Management Policy Page includes a mechanism for Client to subscribe to notifications of any new Sub-processors or changes to the Sub-processor list and Client is responsible for ensuring that it subscribes to such notifications. Provider may add or make changes to the Sub-processors by giving no less than thirty (30) calendar days' notice in accordance with Client's subscription to notifications. Within ten (10) calendar days of such notice from Provider, Client may object to the appointment of an additional or replacement Sub-processor on reasonable grounds relating to the protection of Client Personal Data, by providing Client's notice of objection (including its reasonable grounds for objection that relate to the protection of Client Personal Data) to Provider to legal@mediaocean.com. In the event that Client provides an objection consistent with this sub-section, Provider shall have the right to cure the objection through one of the following options:

a. Provider will cancel its plans to use the Sub-processor with regard to Client Personal Data or will offer an alternative to provide the Services without such Sub-processor;

b. Provider will take corrective steps requested by Client in its objection (which remove Client's objection) and proceed to use the Sub-processor with regard to Client Personal Data; or

c. Provider may cease to provide or Client may agree not to use (temporarily or permanently) the Services which would involve the use of such Sub-processor with regard to Client Personal Data, subject to a mutual agreement of the parties to reduce the remuneration for the Services considering the reduced scope of the Services.

In the event of an objection made consistent with this sub-section, until a decision is made regarding the new Sub-processor, Provider may temporarily suspend the processing of the affected Client Personal Data and/or suspend access to the affected Services; provided that Client remains liable for all amounts due under the Agreement during this period.

If none of the above options for curing are reasonably available and the objection has not been resolved to the mutual satisfaction of the parties within thirty (30) calendar days after Provider's receipt of Client's objection, either party may terminate the Agreement and Client will be entitled to a pro-rata refund for prepaid fees for Services not performed as of the date of termination. Client will have no further claims against Provider due to the termination of the Agreement (including, without limitation, requesting refunds) and/or the DPA under the circumstances described herein.

4.4 Emergency replacement. Provider may replace a Sub-processor if the reason for the change is beyond Provider's reasonable control. In such instance, Provider will notify Client of the replacement as soon as reasonably practical, and Client shall retain the right to object to replacement Sub-processor pursuant to Section 4.3 above.

5.0 Security of Client Personal Data

5.1 Security. Provider shall implement, at its own cost and expense, appropriate technical and organizational measures designed to protect Client Personal Data from a Security Incident and in accordance with Provider's security standards as set forth in the Agreement, including Annex 2 attached. These measures shall be consistent with good industry practice for the protection of Personal Data and of at least the minimum standard required by the Data Protection Laws.

5.2 Provider Personnel. Provider shall take reasonable steps to ensure that only authorized personnel of Provider or its Sub-processors have access to Client Personal Data and to limit access to Client Personal Data to only those personnel that require access to perform their roles and responsibilities in connection with the Client Personal Data Purposes. Provider shall take reasonable steps to ensure that any persons whom it authorizes to have access to Client Personal Data including employees, agents and contractors:

a. receive appropriate training regarding their responsibilities and obligations with respect to the processing, protection and confidentiality of Client Personal Data.

b. are subject to a duty of confidentiality (whether a contractual or statutory duty) that shall survive termination of their employment and/or contractual relationship.

5.3 Deletion or Return of Client Personal Data. Upon termination or expiration of the Agreement, Provider shall, in accordance with the terms of the Agreement, delete or make available to Client for retrieval all relevant Client Personal Data in Provider's possession, save to the extent that Provider is required by any applicable law or required or permitted by the Agreement to retain some or all of Client Personal Data. In the event of such retention, Provider shall extend the protections of the Agreement and this DPA to such Client Personal Data and limit any further processing of such Client Personal Data to only those limited purposes that require or permit the retention, for so long as Provider maintains Client Personal Data. At Client's request, Provider shall provider Client with certificate of destruction and a written log evidencing any retention of Client Personal Data.

5.4 Security Incidents. Upon becoming aware of a Security Incident, Provider shall notify Client without undue delay and pursuant to the terms of the Agreement, but within no more than seventy-two (72) hours, and shall provide such timely information as Client may reasonably require to enable Client to fulfill any data breach reporting obligations under Data Protection Laws. Provider will take commercially reasonable steps to identify and remediate the cause of such Security Incident as soon as reasonably practical. If a Security Incident requires notice to any regulator, data subject or other third party, Client shall have sole control over the content, timing and method of distribution of any needed notice, unless otherwise required by applicable law. Client shall reimburse Provider all reasonable expenses incurred by Provider in connection with any notice or response with respect to any Security Incident or other breach of security or confidentiality for which Client is wholly or partially responsible. Client will not make, disclose, release or publish any finding, admission of liability, communication, notice, press release or report concerning any Security Incident which directly or indirectly identifies Provider without Provider's prior written approval, unless Client is compelled to do so pursuant to Data Protection Laws, in which case, Client shall provide Provider with reasonable prior written notice of such disclosure and will limit the disclosure to the minimum scope required.

5.5 Indemnification. Provider agrees to fully indemnify, defend and hold harmless Client, its directors, officers, employees and agents from and against any and all losses, damages, fees and expenses arising from any claims due to, arising out of, or relating in any way to a Security Incident resulting from an act or omission of Provider, except to the extent that Client is wholly or partially responsible for such Security Incident.

6.0 Controller Processing for Business Data

6.1 Controller Compliance. Each party will comply with Data Protection Law applicable to its role as a Controller for Business Data. If a party transfers or provides access to Business Data to the other party, the party initially transferring or providing such data shall be responsible for ensuring that it has, and will continue to have, the right to transfer, or provide access to, such Business Data to the other party for processing in accordance with the terms of the Agreement and this DPA.

6.2 Purposes of Business Data Processing. Provider shall only use Business Data for the Business Data Purposes. The "**Business Data Purposes**" means the Client Personal Data Purposes, plus:

a. To communicate with employees and agents of Client to market the Services and Provider's or its Affiliates' other products and services.

b. To negotiate additional agreements for products and services and facilitate the provision of products and services under such additional agreements.

7.0 Transfers of Personal Data (Applicable to Client Personal Data and Business Data)

7.1 Transfers of Personal Data outside the EU/EEA. To the extent that Personal Data is transferred from the EEA, directly or via onward transfer, to any Third Country, Provider and Client agree to comply with the EU SCCs and hereby incorporate the following EU SCC modules by reference: (i) with respect to Business Data, Module 1 (controller to controller); (ii) with respect to Client Personal Data where Client is the Controller, Module 2 (controller to processor); and (iii) with respect to Client Personal Data where Client is the Processor, Module 3 (processor to processor), which EU SCCs shall be deemed completed as follows:

a. Optional Clause 7 (docking clause) shall be deemed incorporated.

b. Client may exercise its right of audit under Clause 8.9 as set out in, and subject to the requirements of, Section 9.2 of this DPA.

c. In Clause 9, Option 2 (General Written Authorization) shall apply, subject to the requirements of Sections 4.3 and 4.4 of this DPA, and the time period for prior notice of Sub-processor changes shall be thirty (30) days.

d. In Clause 11, the optional language shall not apply.

e. In Clause 17, Option 1 shall apply, and the EU SCCs will be governed by the law of [Ireland].

f. In Clause 18(b), disputes shall be resolved before the courts of [Ireland].

g. Annex I of the EU SCCs shall be deemed completed with the information set out in Annex 1A, Annex 1B and Annex 1C attached hereto.

h. Annex II of the EU SCCs shall be deemed completed with the information set out in Annex 2 attached hereto. and

i. Annex III of the EU SCCs shall be deemed completed with the information set out in Annex 3 attached hereto.

In the event that any provision of this DPA contradicts, directly or indirectly, the EU SCCs, the EU SCCs shall prevail. Alternatively, Provider may ensure that other appropriate safeguards are in place, for example binding corporate rules in accordance with Article 47 of the GDPR. For the avoidance of doubt, this Section 7.1 and the EU SCCs shall not apply to Personal Data that is not transferred, either directly or via onward transfer, outside the EEA to a Third Country.

7.2 Transfers of Personal Data outside the UK. To the extent that Personal Data is transferred from the UK directly or via onward transfer, to any Third Country, Provider and Client agree to comply with the UK Addendum and hereby incorporate the UK Addendum by reference, which shall be deemed completed as outlined below:

a. Table 1 shall be deemed completed with the information set out in Annex 1 attached hereto, as appropriate, the contents of which are hereby agreed by the parties.

b. In Table 2, the parties select the checkbox that reads: "*Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum*", and the table shall be deemed to be completed according to the parties preferences outlined in Section 7.1 of the DPA above.

c. Table 3 shall be deemed completed with the information set out in Annex 1 and Annex 2 attached hereto, the contents of which are hereby agreed by the parties.

d. In Table 4, the parties agree that neither party may end the UK Addendum as set out in Section 19 of the UK Addendum.

In the event that any provision of this DPA contradicts, directly or indirectly, the UK Addendum, the UK Addendum shall prevail. For the avoidance of doubt, this Section 7.2 and the UK Addendum shall not apply to Personal Data that is not transferred, either directly or via onward transfer, outside the UK to a Third Country.

7.3 Transfers of Personal Data outside Switzerland. To the extent that Personal Data is transferred from Switzerland, directly or via onward transfer, to any Third Country, Provider and Client agree that such transfers from Switzerland are made pursuant to the EU SCCs with the following modifications:

a. The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the EU SCCs shall be interpreted to include the FADP and the Revised FADP with respect to data transfers subject to the FADP and Revised FADP.

b. The terms of the EU SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.

c. Clause 13 of the EU SCCs is modified to provide that the FDPIC shall have authority over data transfers governed by the FADP and the appropriate EU Supervisory Authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Clause 13 shall be observed.

d. The term "EU Member State" as utilised in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

8.0 Cooperation

8.1 Data Subjects' Rights. With respect to Client Personal Data, Client is responsible for responding to Data Subject Requests and any inquiry or communication from a Data Subject, except to the extent that Client and Provider have agreed that Provider shall respond to certain Data Subject Requests in the Agreement and/or this DPA. Provider shall provide commercially reasonable assistance, including by appropriate technical and organizational measures as reasonably practical, to enable Client to respond to any inquiry or communication from a Data Subject or any Data Subject Request related to Client Personal Data, at Client's sole expense. In the event such inquiry, communication or Data Subject Request is made directly to Provider, Provider shall promptly inform Client by providing the full details of the inquiry, communication or request. With respect to Business Data, the party that receives an inquiry or communication from a Data Subject or a Data Subject Request shall be responsible for responding it and shall have no obligation to notify the other party; provided however, a party receiving a complaint from a Data Subject relating to the other party (or any act or omission of the other party), shall promptly notify the other party by providing the full details of the complaint.

8.2 Data Protection Impact Assessments and Prior Consultation. With respect to Client Personal Data, Provider shall, to the extent required by Data Protection Laws, provide Client with reasonable assistance with data protection impact assessments or prior consultations with data protection authorities that Client is required to carry out. With respect to Business Data, each party shall, to the extent required by Data Protection Laws, provide the other party with reasonable assistance with data protection impact assessments or prior consultations with data protection authorities that the other party is required to carry out.

9.0 Security Reports and Audits

9.1 Security Reports. With respect to Client Personal Data, Provider will make available to Client all information reasonably requested to demonstrate compliance with requirements of the Data Protection Laws and allow for and contribute to audits, including inspections, conducted by Client or Client's designated representative. With respect to Business Data, each party will make available to the other party all information reasonably requested demonstrate compliance with requirements of the Data Protection Laws and allow for and contribute to audits, including inspections, conducted by the other party or the other party's designated representative.

9.2 Audits. With respect to Client Personal Data, no more than once per year, Client shall have the right to audit Provider's data privacy compliance upon written request. With respect to Business Data, no more than once per year, each party shall have the right to audit the other party's data privacy compliance upon written request. The parties shall bear their own costs in connection with activities under this paragraph, except that, in the event that a Client requests onsite validation, Provider has not disclosed a Security Incident and Client does not have a reasonable suspicion that Provider has had a Security Incident, Provider may charge a reasonable fee for assistance provided to allow for such onsite validation. If such onsite validation reveals material non-compliance with Provider's obligations under this clause, however, then Client shall not be responsible to Provider for any such fees. Client shall use (and ensure that each of its auditors use) its best efforts to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to Provider's premises, equipment, personnel and business while Client's personnel are on Provider's premises in the course of such an audit or inspection. In connection with an audit under this Section 9.2 and upon request, Provider will provide Client with annual SOC2 Type II report as evidence of its compliance with the Data Protection Laws and this DPA. Any provision of security attestation reports (such as SOC2, Type II or equivalent report) or audits shall take place in accordance with Client's rights under the Agreement.

9.3 Confidentiality. All information provided to or obtained by Client in the course of an audit or otherwise under this Section 9 is Provider's Confidential Information under the Agreement. Provider may require Client's employees, agents or auditors to sign a confidentiality agreement before providing them with information in connection with Provider's obligations under this Section 9.

10.0 Miscellaneous

10.1 This DPA supplements and amends and forms part of the Agreement. Except as amended by this DPA, the Agreement will remain in full force and effect.

10.2 If there is a conflict between the Agreement and this DPA, the terms of this DPA will take precedence.

10.3 Any claims brought under this DPA shall be subject to the terms and conditions, including the exclusions and limitations set forth in the Agreement.

10.4 The applicable law and jurisdiction as set forth in the Agreement apply to this DPA.

10.5 Client and Provider agree to cooperate in good faith to amend this DPA as necessary to: (i) comply with changes to Data Protection Laws; and (ii) comply with the instructions of the Controller in the event that Client is a Processor or joint Controller with respect to any Client Personal Data.

10.6 Client and Provider, along with the data exporter(s) and data importer(s) (if different from Client and Provider), have entered into this DPA, including the EU SCCs, UK Addendum and all Annexes, by their signature on the Agreement incorporating this DPA by reference. This DPA, including the EU SCCs, UK Addendum and all, are legally binding on the parties and allows Data Subjects to enforce their rights as set forth in this DPA.

ANNEX 1A: LIST OF PARTIES

Data exporter(s)

[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name: The Client entity named in the Agreement incorporating this DPA by reference.

Address: as provided in the Agreement incorporating this DPA by reference.

Contact person's name, position and contact details: as provided in the Agreement incorporating this DPA by reference.

Activities relevant to the data transferred under these Clauses: As described in Annex 1B.

Signature and Date: on the Agreement incorporating this DPA by reference.

Role (controller/processor): Controller and Processor.

Data importer(s)

Name: The Provider entity named in the Agreement incorporating this DPA by reference.

Address: as provided in the Agreement incorporating this DPA by reference.

Contact person's name, position and contact details: as provided in the Agreement incorporating this DPA by reference.

Activities relevant to the data transferred under these Clauses: As described in Annex 1B.
Signature and Date: on the Agreement incorporating this DPA by reference.

Role (controller/processor): Processor (Client Personal Data) and Controller (Business Data).

ANNEX 1B: DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred	**Client Personal Data:** Visitors to websites on which Client's ads or Provider's tags on behalf of Client are placed. **Business Data:** Client's or its Affiliates' employees, contractors and other personnel using the Services or acting as administrative or business representatives with respect to the Services. **Service-Specific Categories (applicable to identified Services Only):** **Flashtalking FTrack:** Visitors to websites on which Client's ads or Provider's tags on behalf of Client are placed. **Protected Media:** Employees, contractors, suppliers, job applicants, visitors, prospects, trainees, next of kin.
Categories of personal data transferred	**Client Personal Data:** IP addresses, pseudonymous online identifiers including cookie ids and device ids, and online behavioral activity. **Business Data:** business contact information (name, work email address, work phone number, job title and employer), user authentication details, logs of actions taken by users within the system and transaction data, including financial account data. **Service-Specific Categories (applicable to identified Services Only):** **Flashtalking Audience Marketplace**: email, Mobile ad ID, and PELs. **Flashtalking Social Ads Manager Audience Hub Services and/or Audience HQ Services:** name, address, email, city, state, zip, birthdate, phone number, IP address, Adobe Audience Manager ID, Neustar ID, Horizon BluID, Mobile ad ID. **Flashtalking FTrack:** IP addresses, pseudonymous online identifiers including cookie ids and device ids, and online behavioral activity. **Protected Media**: Name, individual identifier, location and free form text limited to (a) naming conventions on shared or group channels and folder or file names, and (b) email subject lines. **Third-Party Data:** as described in Section 3.3 with respect to the Services covered by Section 3.3.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as 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 measures.	Not applicable.

ANNEX 1B: DESCRIPTION OF TRANSFER	
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	Continuous.
Nature of the processing	Provider processes Personal Data, including recording, organizing, storing, retrieving and disclosing Personal Data, as necessary: (a) to fulfill the Client Personal Data Purposes and the Business Data Purposes, as applicable; and (b) to fulfill the Documented Instructions and as otherwise instructed by Client with respect to Client Personal Data.
Purpose(s) of Processing and Purpose(s) of the data transfer and further processing	To fulfill the Client Personal Data Purposes and the Business Data Purposes, as applicable.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	**Client Personal Data:** Provider will retain Client Personal Data for the duration of the Agreement except to the extent that Client determines a shorter retention period for the Client Personal Data within production systems. Provider will further retain back-ups in line with Provider's data retention policies, for only as long as is required to meet Provider's legal, regulatory and operational requirements or as necessary for the Client Personal Data Purposes. **Business Data:** For the duration of the business relationship between Provider and its Affiliates and Client and its Affiliates (including business relationship with respect to Provider and its Affiliates marketing other products and services to Client and its Affiliates), as long as is required to meet Provider's legal, regulatory and operational requirements or as necessary for the Business Data Purposes.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	**Client Personal Data:** The subject matter and duration of the processing are set forth in the Agreement. The nature of the processing is to process Client Personal Data, including recording, organizing, storing, retrieving and disclosing Client Personal Data, as necessary: (a) to fulfill the Client Personal Data Purposes; and (b) to fulfill the Documented Instructions and as otherwise instructed by Client with respect to Client Personal Data. **Business Data:** Not applicable.

ANNEX 1C: COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

CNIL

Commission Nationale de l'Informatique et des Libertés

3 Place de Fontenoy

TSA 80715

75334 PARIS CEDEX 07

France

ANNEX 2: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational 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.

Testing and Evaluation

- Mediaocean’s Ad Infrastructure division achieved SOC 1 and SOC 2 compliance in 2012. Mediaocean has maintained SOC 1 type II and SOC 2 type II compliance for the associated Services and is currently SOC 2 type II compliant.
- Mediaocean's Ad Tech division, achieved SOC 2 compliance in 2018. Flashtalking has maintained SOC 2 type II compliance for all primary products since the Audit period of 2019, and is currently SOC 2 type II compliant.
- External Penetration testing for web-based applications is performed no less than annually to identify security weaknesses and vulnerabilities. Any identified vulnerabilities are risk assessed and remediation plans are implemented appropriately.
- Internal audits are conducted as feasible.

Access and Security

- IT systems security for staff access is managed and administered by authorized security administrators, and access to modify security configurations is restricted to appropriate personnel.
- Access is restricted through the use of identification and authentication mechanisms, including the use of user IDs assigned to users.
- Access is granted based on the principle of least privileged, ensuring that users receive only the minimum permissions necessary.
- Access privileges for employees are reviewed at least annually by the respective data owners for completeness and accuracy. Inappropriate access is identified by the data owners and is removed by appropriate security administrators.
- System access and activities are logged and monitored. Logs are reviewed as needed.
- Mediaocean requires the use of two-factor authentication for employees connecting remotely to the Mediaocean corporate network.

- Industry-standard encryption is used for data at rest and in transit
- Production systems are protected by dedicated network infrastructure including firewalls. Mediaocean maintains a segmented network with separate vlans for dedicated purposes.
- Firewall tools are configured to send alerts to designated personnel summarizing activity, including potential security breaches and other security incidents.
- Internal vulnerability scans are conducted on regular basis. Results are reviewed and any issues identified are researched and resolved as part of the patching and/or incident change management process.

Confidentiality, Integrity, Availability, and Resilience

- The necessary controls pertaining to Confidentiality, Integrity, Availability, and Resilience are comprehensively covered and thoroughly examined in the aforementioned SOC audits. Audits provide assurance that as an organization Mediaocean maintains robust safeguards and practices to protect information assets and ensure system reliability.
- SLAs are documented and tailored appropriately to their associated services, ensuring clear performance metrics, responsibilities, and expectations for each service offering.

Risk Assessments

- Mediaocean has put in place a vendor management policy which defines security, confidentiality, and privacy requirements by vendor class.
- Mediaocean performs security reviews in line with the requirements of the vendor management policy when onboarding a new vendor, critical system or sub-processor.
- Mediaocean performs vendor security assessments periodically in line with the requirements of the vendor management policy to ensure adherence to stipulated requirements.
- Information Security team works with process owners to identify treatments to identified risks. Risk treatments are evaluated on at least annual basis, and are formally assessed and documented on the Risk Register.
- Mediaocean maintains registers of personal data processing, which outlines the Company's legal basis for processing data and for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information. The register is reviewed on at least annual basis.

Business Continuity and Disaster Recovery

- Business Continuity and Disaster Recovery policies and plans are in place and regularly tested.
- Backups are retained encrypted in cloud storage.
- Backups are managed using automated scheduling tools configured by appropriate personnel. A recovery test is performed at least annually to ensure that a full system recovery can be performed completely and accurately.
- RPO & RTO are documented within the appropriate internal documentation and plans.

ANNEX 2A: Protected Media

For Services provided by Protected Media, this Annex 2A shall apply instead of Annex 2 above.

Provider shall implement and maintain industry-standard technical and organizational measures to protect the Client Personal Data processed hereunder, against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, as set forth in the security documentation applicable to the Services purchased by Client under the Agreement, as updated from time to time and as made reasonably available by Provider, including, as appropriate, the measures required pursuant to Article 32 of the GDPR. Such security measures include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of Provider's systems and services; to help restore timely access to Client Personal Data following an incident; and for regular testing of effectiveness.

ANNEX 3: LIST OF SUB-PROCESSORS

Client has authorized the use of the following Sub-processors for the following Providers:

1. **Any Sub-Processor for Provider identified on the Vendor Management Policy Page**
   https://support-na.mediaocean.com/hc/en-us/sections/27908523524759-Mediaocean-and-sub-processors