DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is entered into by and between TypeA Holdings Ltd. and its Affiliates ("**TypeA**"), and the counterparty using TypeA ad serving technology ("**Media Company**"), both parties shall be referred to as the "**Parties**" and each, a "**Party**". This DPA forms an integral part of the agreement executed between the Parties ("**Agreement**"), capitalized terms used herein but not defined herein shall have the meanings ascribed to them in the Agreement.

This DPA sets forth the parties' responsibilities and obligations regarding the Processing of Personal Data (as such terms are defined below) during the term of the Agreement.

In the event of any conflict between certain provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement solely with respect to the Processing of Personal Data. In the event of a conflict between this DPA and the SCC (as defined below) the SCC will prevail solely with regards to international transfer of Personal Data.

1. DEFINITIONS

1.1 "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2 "**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civ. §§ 1798.100 et. seq., and its implementing regulations, as may be amended from time to time, including as emended by the California Privacy Rights Act ("**CPRA**");

1.3 "**Cross-Contextual Behavior Advertising" or "CCBA"** shall have the meaning as defined in the CCPA.

1.4 The terms, "**Controller**", "**Member State**", "**Processor**", "**Processing**" "**Supervisory Authority**", and "**Personal Data Breach**" shall have the same meaning as in the GDPR.

1.5 For the purpose of clarity, within this DPA "**Controller**" shall also mean "**Business**", and "**Processor**" shall also mean "**Service Provider**", to the extent the CCPA applies.

1.6 "**Data Protection Laws**" means all applicable and binding privacy and data protection laws and regulations, including such laws and regulations of the European Union, the European Economic Area and their Member States, Switzerland, the United Kingdom, Canada, Israel and the United States of America, as applicable to the Processing of the Personal Data under the Agreement including (without limitation) the GDPR, the UK GDPR, the CCPA, the Swiss Federal Act on Data Protection ("**Swiss FDPA**"), LGPD and the Rules and Self-Regulatory Principles of the European Interactive Digital Advertising Alliance, as applicable to the Parties in relation to the Shared Personal Data hereunder and in effect at the time of the Parties' performance hereunder.

1.7 "**Data Subject**" means the identified or identifiable person to whom the Personal Data relates.

1.8 "**End-Users**" means the individuals that interact or engage with the digital assets, websites, apps, or otherwise any digital asset in which the ads are served by TypeA.

1.9 "**EEA**" means the European Economic Area.

1.10 "**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data

and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.11 "**IAB Consent Management Framework**" means the IAB tech labs' technical specification for the GDPR transparency & consent framework.

1.12 "**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

1.13 "**Personal Data**" or "**Personal Information**" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with an identified or identifiable natural person or consumer, which is processed by a Party, under this DPA and the Agreement. For the purpose of this DPA, Personal Data shall mean and refer to "**Personal Information**".

1.14 "**Privacy Signals**" means, end users' preference regarding the processing of Personal Data, including, without limitations, "do not share or sell my personal information" under the CCPA, the Google restricted data processing "rdp", Digital Advertising Alliance (currently available at http://www.aboutads.info/principles), Network Advertising Initiative (https://thenai.org/opt-out/), and the IAB Global Privacy Platform ("GPP") or IAB Transparency & Consent Framework ("TCF") signals, Global Privacy Control ("GPC") sting, or any current, future standard signal initiated by an approved consent management platform ("CMP") which indicated the end users preference with respect to processing Personal Data and providing personalized, interest-based advertisement.

1.15 "**Shared Personal Data**" means the Personal Data shared by Media Company with TypeA as further detailed in **Annex I** attached hereto.

1.16 "**Standard Contractual Clauses**" shall mean the Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021, which may be found here: Standard Contractual Clauses, and incorporated herein by reference.

1.17 "**Swiss SCC**" shall mean the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner

1.18 "**UK Regulations**" means the Data Protection Act 2018, as well as the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419) ("**UK GDPR**"), and the UK Data Privacy and Digital Bill.

1.19 "**UK SCC**" shall mean the UK 'International data transfer addendum to the European Commission's standard contractual clauses for international data transfers', available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf as adopted, amended or updated by the UK's Information Commissioner's Office, Parliament or Secretary of State.

2. PROCESSING OF PERSONAL DATA

2.1 The Parties acknowledge and agree that with regard to the Shared Personal Data, TypeA and the Media Company are separate and independent Data Controllers. The Parties acknowledge and

agree that under no circumstances they will not be joint controllers (as defined in the GDPR).

2.2 When Processing the Shared Personal Data under the Agreement and this DPA, each Party shall Process the Shared Personal Data solely for the following purposes: (i) Processing in accordance with the Agreement and this DPA; and (ii) Processing as required under applicable Data Protection Laws. Notwithstanding the above, the Parties may use the Shared Personal Data for their own purpose provided that, the appropriate legal basis under applicable Data Protection Laws required for such Processing activities has been established by such Party prior to such additional Processing activities. Without derogating from the foregoing, each Party shall be responsible independently and separately for complying with the obligations that apply to it as a data Controller under Data Protection Laws and shall reasonably assist the other Party with complying to Data Protection Laws.

2.3 Each Party acknowledges and agrees that if such Party is required to share any Personal Data, including the Shared Personal Data, for the purpose of the Agreement, such Party will remain liable to ensure that such share will comply with substantially similar obligations to the terms of this DPA. TypeA will shares the Shared Personal Data, in whole or in part, with third party advertisers or service providers for the purpose of serving personalized and targeted advertisements, measuring the effectiveness of advertisements, and other purposes applicable to provide the services under the Agreement.

2.4 With respect to Processing of the Shared Personal Data, Media Company represents and warrants that, to the extent applicable: (a) it shall obtain all necessary permissions and valid consents from the End Users in accordance with Data Protection Laws and the IAB TCF Policy to lawfully permit Media Company to collect, process and share the Shared Personal Data with TypeA, for the purpose of displaying ads, including CCBA; and (b) it shall at all times maintain a mechanism for obtaining such consent from Data Subjects in accordance with the requirements of Data Protection Laws and the IAB TCF Policy, as well as a mechanism for Data Subjects to withdraw such consent (optout) in accordance with Data Protection Laws and the IAB TCF Policy. Media Company shall maintain a record of all consents obtained from data subjects, and all withdrawals of consent by data subjects, all as required by Data Protection Laws and shall provide TypeA with such records upon reasonable written request.

2.5 Media Company undertakes to implement technical tools, consent management platforms (“CMP”) that enable End Users to set their privacy preference. The CMP shall provide TypeA with any and all applicable Privacy Signals, which TypeA shall transfer “as is” and as provided by the Media Company to its advertising partners, which shall place ads based on such End Users preference.

2.6 Each Party is responsible for placing an easy-to-understand privacy policy that is in compliance with all applicable laws, rules and regulations, and industry self-regulatory guidelines and discloses the use of third-party advertising partners and tools which, directly or indirectly, process Personal Data to serve ads, including CCBA.

3. DATA SUBJECT REQUEST AND SUPERVISORY AUTHORITY REQUEST

3.1 Taking into account the nature of the Processing, the Parties each agree to provide such assistance as is reasonably required and requested by the other Party to enable it to comply, within timeframe legally required, with requests received from Data Subjects to exercise their rights under Data Protection Laws with respect to the Shared Personal Data, or any complaint, investigation, inquiry,

warrant, subpoena or proceedings from or brought by any public, governmental, or judicial agency or authority that relates to the Processing activities under the Agreement.

3.2 Each Party is responsible for maintaining records of Data Subject Requests it receives and the decisions made with respect thereto, as required under Data Protection Laws.

4. SECURITY

4.1 Each Party shall have implemented and will maintain, appropriate technical and organizational measures for the protection of the Shared Personal Data Processed hereunder as required by Data Protection Laws (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to Shared Personal Data, confidentiality and integrity of the Shared Personal Data).

4.2 Without derogating from the foregoing, each Party shall be responsible to comply with security requirements apply to it as an independent and separate Data Controller under Data Protection laws and comply at least with the requirements set forth in **Annex II**.

5. CONFIDENTIALITY

The Parties shall ensure that the Shared Personal Data is kept confidential and their personnel and advisors engaged in the Processing of Shared Personal Data have committed themselves to confidentiality.

6. DATA INCIDENT MANAGEMENT AND NOTIFICATION

Each Party shall: **(i)** without undue delay, and within 48 hours, notify the other party of the existence, nature and scope of any Personal Data Breach affecting Shared Personal Data; **(ii)** take actions required by Data Protection Laws and industry standards to prevent further security incidents, including Personal Data Breach; and **(iii)** cooperate in good faith to agree and take applicable actions as may be necessary to mitigate or remedy the effects of the Personal Data Breach and minimize any effects of and investigate any security incident and to identify its cause.

7. CROSS BORDER TRANSFERS

7.1 **Transfers from the EEA, Switzerland and the United Kingdom to countries that offer adequate level of data protection**. Personal Data may be transferred from the EEA, Switzerland and the United Kingdom ("**UK**") to an Adequate Country.

7.2 **Transfers from the EEA, Switzerland and the United Kingdom to other countries**. If the Parties' sharing of the Shared Personal Data under this DPA includes a transfer (either directly or via an onward transfer):

7.2.1. transfer of Shared Personal Data from the EEA the terms set forth in Annex IV shall apply transfer of Shared Personal Data from the UK, the terms set forth in Annex V shall apply transfer of Shared Personal Data from Switzerland, the terms set forth in Annex VI shall apply

8. GOVERNING LAW

To the maximum extent permitted by law, this DPA shall be governed by the laws governing the Agreement, except for those provisions of clauses which dictate the application of another law for particular purposes.

ANNEX I- DETAILS OF THE SHARED PERSONAL DATA

This Annex I include certain details of the Processing of the Personal Data as required by Article 28(3) GDPR.

Categories of Data Subjects

EEA, UK and Swiss End-Users (as defined under Section 1.8 above).

Categories of Personal Data

IP addresses, IFV and IFA (e.g., IDFA/ AAID or any IDs), Privacy String, cookies data or unique identifiers, information about End-Users' device and End-User's browsing behavior.

Special Categories of Personal Data:

Not Applicable

Nature of the processing:

Collection, storage, organization, analysis, modification, retrieval, disclosure, communication and other uses in performance of the services as set out in the Agreement.

Purpose of Data Sharing

1. Sharing the Personal Data by Media Company in accordance with the purposes stipulated in the Agreement and this DPA, among others for placing ads, including CCBA on or within Media Company's assets;
2. Complying with applicable laws and regulations;

Process Frequency:

The Personal Data is transferred on a continuous basis.

Duration of the Processing

Between 7 to 30 days for fraud prevention purposes.

ANNEX II- SECURITY REQUIREMENTS

Each Party shall implement and maintain current and appropriate technical and organizational measures to protect Personal Data against accidental, unauthorized or unlawful Processing and against accidental loss, destruction, damage, alteration, disclosure or access, as set forth below:

1. Provide third-party attestation of static or dynamic application security testing or penetration testing on all software or systems Processing Personal Data, remediate any identified high vulnerabilities, provide written remediation plans for medium and low vulnerabilities.

2. Maintain a level of security appropriate to the harm that may result from any unauthorized or unlawful Processing or accidental loss, destruction, damage, denial of service, alteration or disclosure, and appropriate to the nature of Personal Data;

3. Oblige its employees, agents or other persons to whom it provides access to Personal Data to keep it confidential; take reasonable steps to ensure the integrity of any employees who have access to Personal Data; provide annual training to staff and subcontractors on the security requirements contained herein;

4. Maintain measures designed to ensure the ongoing confidentiality, integrity, availability and resilience of Advertiser's systems and services;

5. Adhere password policies for standard and privileged accounts consistent with industry best practices;

6. Ensure that only those personnel who need to have access to Personal Data are granted access, such access is limited to the least amount required, and only granted for the purposes of performing the services and the obligations under this DPA;

7. Maintain a physical security program that is consistent with industry best practices;

8. Ensure that any storage media (whether magnetic, optical, non-volatile solid state, paper, or otherwise capable of retaining information) that captures Personal Data, if applicable, is securely erased or destroyed before repurposing or disposal;

ANNEX III – EEA Transfers

1. The Parties agree that the terms of the EU Standard Contractual Clauses are hereby incorporated by reference and shall apply to an EEA Transfer.

2. Module One (Controller to Controller) of the Standard Contractual Clauses shall apply where the EEA Transfer is effectuated by Media Company as the data controller of the Shared Personal Data and TypeA is an independent and separate data Controller of the Shared Personal Data.

3. Clause 7 of the Standard Contractual Clauses (Docking Clause) shall not apply.

4. In Clause 11 of the Standard Contractual Clauses, the optional language will not apply.

5. With respect to Clause 17 of the Standard Contractual Clauses the Parties agree that the Standard Contractual Clauses shall be governed by the laws of the Republic of Ireland.

6. In Clause 18(b) of the Standard Contractual Clauses, disputes will be resolved before the courts of the Republic of Ireland.

7. Annex I.A of the Standard Contractual Clauses shall be completed as follows:

   Data Exporter: Media Company

   Contact details: As detailed in the Agreement.

   Data Exporter Role: Module One: The Data Exporter is an independent and separate data Controller.

   Signature and Date: By entering into the Agreement and DPA, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

   Data Importer: TypeA

   Contact details: As detailed in the Agreement.

   Data Importer Role: Module One: The Data Importer is an independent and separate data controller.

   Signature and Date: By entering into the Agreement and DPA, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

8. Annex I.B of the Standard Contractual Clauses shall be completed as follows:

   The categories of data subjects, categories of personal data, frequency of the transfer, nature of the processing, purpose of the processing and the duration are all detailed in **Annex I** (Details of Processing) of this DPA.

   The technical security measures are detailed in Annex II of the DPA.

9. Annex I.C of the Standard Contractual Clauses shall be completed as follows:

   The competent supervisory authority in accordance with Clause 13 is the supervisory authority in the Member State stipulated in Section 5 above.

ANNEX IV – UK TRANSFERS

1. The Parties agree that the terms of the Standard Contractual Clauses as amended by the UK Standard Contractual Clauses, and as amended in this **Annex IV**, are hereby incorporated by reference and shall apply to transfer of Personal Data from the UK to other countries that are not deemed as Adequate Countries.
2. This Annex IV is intended to provide appropriate safeguards for the purposes of transfers of Personal Data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and with respect to data transfers from controllers to controllers.

   Where this Annex IV uses terms that are defined in the Standard Contractual Clauses, those terms shall have the same meaning as in the Standard Contractual Clauses.
3. This **Annex IV** shall (i) be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 of the UK GDPR, and (ii) not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.
4. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, reenacted and/or replaced after this DPA has been entered into.
5. Amendments to the UK Standard Contractual Clauses:
   a. Part 1: Tables
      i. Table 1 Parties: shall be completed as set forth in **Annex III** above.
      ii. Table 2 Selected SCCs, Modules and Selected Clauses: the EU SCC as as set forth in Section **Annex III** above.
      iii. Table 3 Appendix Information:

   Annex 1A: List of Parties: shall be completed as set forth in **Annex III** above.

   Annex 1B: Description of Transfer: shall be completed as set forth in **Annex I** above.

   Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: shall be completed as set forth in **Annex II** above.

      iv. Table 4 Ending this Addendum when the Approved Addendum Changes: shall be completed as "neither party".

Additional Safeguards:

1. In the event of an EEA Transfer or a UK Transfer, the Parties agree to supplement these with the following safeguards and representations, where appropriate:
   a. The Data Importer shall have in place and maintain in accordance with good industry practice measures to protect the Personal Data from interception (including in transit from the Data Exporter to the Data Importer and between different systems and services). This includes having in place and maintaining network protection intended to deny attackers the ability to intercept data and encryption of Personal Data whilst in transit and at rest intended to deny attackers the ability to read data.
   b. The Data Importer will make commercially reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the Personal Data protected under GDPR or the UK GDPR, including under section 702 of the United States Foreign Intelligence Surveillance Act ("**FISA**");

c. If the Data Importer becomes aware that any government authority (including law enforcement) wishes to obtain access to or a copy of some or all of the Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited or under a mandatory legal compulsion that requires otherwise:

   I. The Data Importer shall inform Data Exporter in writing;

   II. The Data Importer will use commercially reasonable legal mechanisms to challenge any such demand for access to Personal Data which is under the Data Importer's control and notify the Data Exporter, immediately after first becoming aware of such demand for access and provide the Data Exporter with all relevant details of the same, unless and to the extent legally prohibited to do so.

2. Once in every 12-month period, the Data Importer will inform the Data Exporter, at the Data Exporter's written request, of the types of binding legal demands for Personal Data it has received and solely to the extent such demands have been received, including national security orders and directives, which shall encompass any process issued under section 702 of FISA. In the event of an EEA Transfer or a UK Transfer, the Parties agree to have in place and maintain in accordance with good industry practice measures to protect the Shared Personal Data from interception (including in transit from Data Exporter to Data Importer and between different systems and services).

ANNEX V – SWISS SCC

The following terms supplement the Clauses only if and to the extent the Clauses apply with respect to data transfers subject to Swiss Data Protection Law, and specifically the FDPA:

- The term 'Member State' will be interpreted in such a way as to allow data subjects in Switzerland to exercise their rights under the Clauses in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Clauses.
- The clauses in the DPA protect the Personal Data of legal entities until the entry into force of the Revised Swiss FDPA.
- All references in this DPA to the GDPR should be understood as references to the FDPA insofar as the data transfers are subject to the FDPA.
- References to the "competent supervisory authority", "competent courts" and "governing law" shall be interpreted as Swiss Data Protection Laws and Swiss Information Commissioner, the competent courts in Switzerland, and the laws of Switzerland (for Restricted Transfers from Switzerland).
- In respect of data transfers governed by Swiss Data Protection Laws and Regulations, the EU SCCs will also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws and Regulations until such laws are amended to no longer apply to a legal entity.
- The competent supervisory authority is the Swiss Federal Data Protection Information Commissioner

ANNEX VI – CCPA TERMS

This **Annex VI** shall apply and bind the Parties if and to the extent that the Shared Personal Information includes Personal Information of California residents.

Capitalized terms not specifically defined herein shall have the meanings ascribed to them in the DPA, or CCPA, as applicable.

In relation to the Processing of the Shared Personal Information under the Agreement and solely for the purposes of the CCPA TypeA is a Third-Party Business and the Media Company is a first party Business. Solely to the extent the purpose of processing of Personal Information is for a Business Purpose (as defined under the CCPA), TypeA shall be deemed a Service Provider.

1. CCBA

When placing CCBA on Media Company's assets, the following shall apply:

1.1. TypeA shall be the Third Party Business and the Media Company is the First Party Business. The processing of the Personal Information is for profiling, personalization, and targeting advertisement.

1.2. Each party shall independently responsible for complying with the CCPA obligations as a "Business".

1.3. TypeA requires and relies on the Media Company to provide the Consumers the Notice at Collection ("**N@C**") as required by the CCPA, and include in such notice the processing of Personal Information by third party advertising partners for the purpose of CCPA. The N@C shall include an opt out from "Sharing and Selling Personal Information".

1.4. The Media Company shall include a CCPA Notice which complies with the CCPA and enabled the Consumers to understand their Personal Information is Shared and Sold for CCBA.

1.5. The Media Company undertakes and warrant to comply with the CCPA and to technically enable and transfer the Privacy Signals applicable to the CCPA, including without limitations the IAB GPP, the IAB "us_privacy", GPC, and Google restricted data processing. In the event a Consumer exercised the right to opt out from "Sharing and Selling Personal Information" through a Privacy Signal, the Media Company undertakes to pass such signal to TypeA.

2. BUSINESS PURPOSE

When processing Personal Information for a Business Purpose (as defined under the CCPA) the following shall apply:

2.1. TypeA shall be the Service Provider and the Media Company shall be the Business. The processing of Personal Information shall be **solely** for the purpose of debugging, fraud, contextual advertisement, optimization, and technically placing the ads or selecting basic ads.

2.2. TypeA in its role as a Service Provider shall process Personal Information on behalf of the Media Company as a and shall not: (1) sell or share the Personal Information; (2) retain, use or disclose the Personal Information for any purpose other than as specified in section 2.1 above; or (3) combine the Personal Information that TypeA receives from, or on behalf of, Media Company with other Personal Information that it receives from, or on behalf of, another customer, or collects from its own interaction with California residents, expect as otherwise permitted by the CCPA.

2.3. Solely in the position of a Service Provider, and to the extent applicable TypeA shall immediately notify Media Company in the event TypeA makes a determination that it can no longer meet its obligations under the CCPA.

2.4. Solely in the position of a Service Provider, and to the extent applicable TypeA acknowledges and confirms that it does not receive or process the Personal Information as consideration for any Services.

2.5. Solely in the position of a Service Provider, and to the extent applicable TypeA certifies that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from selling (as such term is defined in the CCPA) the Personal Information.