[Last Updated: October 15, 2025]

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is entered by and between Perion Network Ltd., on behalf of itself and its subsidiaries and affiliated entities (collectively, "**Agency**") and the Media Company listed on the corresponding service order or agreement referencing this DPA ("**Media Company**" and "**Agreement**"), and is entered into force on the date on which the Media Company signed the corresponding Agreement ("**Effective Date**").

Capitalized terms used herein but not defined herein shall have the meanings ascribed to them in the Agreement.

WHEREAS, Agency is the developer, owner, and operator of the Agency Technology enabling publishers to use the Services

WHEREAS, during the use of the Services, the parties will process and share Personal Data (as such terms are defined below) subject to the terms and conditions of this DPA; and

WHEREAS, the parties desire to supplement this DPA to achieve compliance with the UK, EU, Swiss, United States, and other data protection laws and agree on the following:

1. DEFINITIONS

1.1 "**Adequate Country**" is a country that has an adequacy decision from the European Commission.

1.2 "**CCPA**" means the California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100 - 1798.199) of 2018, including as modified by the California Privacy Rights Act ("**CPRA**") as well as all regulations promulgated thereunder from time to time.

1.3 "**CPA**" means the Colorado Privacy Act C.R.S.A. § 6-1-1301 et seq. (SB 21-190), including any implementing regulations and amendments.

1.4 "**CTDPA**" means the Connecticut Data Privacy Act, S.B. 6 (Connecticut 2022), including any implementing regulations and amendments thereto.

1.5 "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**", "**Processing**" (and "**Process**"), "**Personal Data Breach**" and "**Special Categories of Personal Data**" shall all have the meanings given to them in EU Data Protection Law, CPA, VCDPA and CTDPA. The terms "**Business**", "**Business Purpose**", "**Consumer**", "**Cross Context Behavioral Advertising**" (also known as "**CCBA**"), "**Contractor**", **"First-Party Business",** "**Service Provider**", "**De-identified Data**" or "**Deidentified Data**", "**Share**", "**Sale**", "**Sell**" "**Third-Party Business**" and "**Targeted Advertising**", shall have the same meanings as ascribed to them in the US Data Protection Laws. "**Data Subject**" shall also mean and refer to a "**Consumer**". "**Personal Data**" shall also mean and refer to "**Personal Information"**.

1.6 "**Consent**" means an End User informed and freely given consent, that meets the requirements stipulated under Article 7 of the GDPR or the IAB Policies.

1.7 "**Data Protection Law**" means applicable privacy and data protection laws and regulations (including, where applicable, EU Data Protection Law, UK Data Protection Laws, Swiss Data

Protection Laws, Israeli Law, US Data Protection Laws, and the Brazilian General Data Protection Law ("**LGPD**") as may be amended or superseded from time to time.

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

1.9 "**End User**" means an individual visiting or browsing the Media Company Sites or any other digital property operated by the Media Company.

1.10 "**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 laws relating to data protection, the Processing of Personal Data, privacy or electronic communications in force from time to time in the United Kingdom, including the UK General Data Protection Regulation, 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 ("**UK GDPR**") and the Data Protection Act 2018, UK Data Protection and Digital Information Bill (collectively, "**UK Data Protection Laws**"), (v) the Swiss Federal Act on Data Protection ("**Swiss FDPA**"); (vi) any national data protection laws made under, pursuant to, replacing or succeeding (i) – (iii); and (vii) any legislation replacing or updating any of the foregoing.

1.11 "**IAB Framework**" means the IAB Tech Labs' technical specification for the GDPR transparency & consent framework ("**TCF**") and the Global Privacy Platform ("**GPP**").

1.12 "**IAB Policies**" means the (i) IAB Europe TCF available at: https://iabeurope.eu/wp-content/uploads/2023/05/230509-TCF-Policies-TransparencyConsentFramework_Policies_version_TCF-v2.2.pdf; (ii) IAB Global Privacy platform including the Multi State Privacy Framework ("**MSPA**") available at: https://www.iabprivacy.com/IAB%20First%20Amended%20and%20Restated%20Multi-State%20Privacy%20Agreement%20(MSPA).pdf

1.13 "**ID**" means (i) a unique identifier stored on an End-User's device; (ii) a unique identifier generated for a specific End User; (iii) an online identifier associated with a particular device; or (iii) a cookie ID, agent ID, IP address, URL or RTB tag, or any online identifier identifying an End User or a specific device.

1.14 "**Israeli Law**" means Israeli Privacy Protection Law, 5741-1981, the regulations promulgated pursuant thereto, including the Israeli Privacy Protection Regulations (Data Security), 5777-2017, and other related privacy regulations.

1.15 "**Privacy Signals**" means the End Users' preference signals, indicating the End Users' preference for Processing Personal Data, such as: requesting to opt-out from selling or sharing Personal Data, opt-out from Processing Personal Data for Targeted Advertising, including without limitations flags or signals sent through a cookie banner, cookie manager, consent management platform or other technology ("**CMP**") such as IAB Global Privacy Platform ("**GPP**") or otherwise the CCPA "Do Not Sell Or Share My Personal Information" signals, Google restricted data Processing ("**RDP**") signals, Global Consent Platform ("**GCP**") signals, and any other opt-out from interest-based advertising signals such as the Digital Advertising Alliance (**DAA**) and the Network Advertising Initiative (**NAI**), as applicable.

1.16 "**Security Incident**" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data of the other party. For the avoidance of doubt, any Personal Data Breach of the other party's Personal Data will comprise a Security Incident.

1.17 "**Standard Contractual Clauses**" or "**SSC**" mean the standard contractual clauses for the transfer of Personal Data to third countries pursuant to the GDPR and adopted by the European Commission **Decision 2021/914** of 4 June 2021 which is attached herein by linked reference: https://eur-ex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN.

1.18 "**Swiss Data Protection Laws**" or **"FADP"** shall mean the Swiss Federal Act on Data Protection of June 19, 1992, SR 235.1, and any other applicable data protection or privacy laws of the Swiss Confederation as amended, revised, consolidated, re-enacted or replaced from time to time, and to the extent applicable to the Processing of Personal Data under the Agreement.

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

1.20 "**UK SCC**" means the UK's 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.

1.1 "**UCPA**" means the Utah Consumer Privacy Act, Utah Code Ann. § 13-61-101 et seq.

1.2 "**US Data Protection Laws**" means any U.S. federal and state privacy laws effective and apply to the Processing of Personal Data, and any implementing regulations and amendment thereto, including without limitation, the CCPA, the CPA, the CTDPA, the VCDPA, and the UCPA.

1.3 "**VCDPA**" means the Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-575 et seq. (SB 1392), including any implementing regulations and amendments thereto.

Any other terms that are not defined herein shall have the meaning provided under the Agreement or applicable Law. A reference to any term or section of US Data Protection Laws, UK Data Protection Laws, or GDPR means the version as amended. Any references to the GDPR in this DPA shall mean the GDPR and/or UK GDPR depending on the applicable Law.

2. RELATIONSHIP OF THE PARTIES

2.1 Pursuant to this DPA and in the course of the engagement set for the therein, Agency and Media Partner will Process the Personal Data described in **Annex I**.

2.2 The parties acknowledge that: (where applicable) **(a)** the parties shall be joint Controllers of the Joint Processed Data as detailed and defined under **Annex I** and each party will process the Joint Processed Data solely for the limited and specified purposes set forth in **Annex I**; **(b)** under the US Privacy Law Addendum (detailed in **Annex VIII**) and solely for the Processing the Personal Data by the Agency for the Restricted Purpose, the Agency shall be considered as a Service Provider or Processor, as applicable and a Service Provider/ Processor when providing the Analytics and Throttling Service; and **(c)** except for sub-section a and b herein, the parties shall be independent Controllers or otherwise Under the CCPA the Agency shall be a Third Party business and each party shall be liable for processing any Personal Data under its control in compliance with applicable Data Protection Laws.

2.3 Except as otherwise agreed in by the parties under Section 2.2 above, each party shall be individually and separately responsible for complying, and shall be able to demonstrate compliance, with applicable Data Protection Laws. The purpose, subject matter, and duration

of the Processing, the type of Personal Data, and categories of Data Subjects are described in **Annex I** attached hereto.

3. REPRESENTATIONS AND WARRANTIES

3.1 Each Party shall comply with its obligation to report a Personal Data Breach to the appropriate Supervisory Authority and (where applicable) data subjects under applicable Data Protection Law and to respond to a data subject request under applicable Data Protection Law.

3.2 Each party shall implement and maintain an information security program with appropriate technical and organizational measures. This program is to ensure a level of security that will be appropriate to the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the Processing, which includes at a minimum (i) the security measures set forth in **Annex II**; and (ii) where required by Data Protection Laws, the appointment of a Data Protection Officer to oversee the privacy program.

3.3 Each party shall provide reasonable cooperation and assistance to the other party in ensuring compliance with its obligation to carry out data protection impact assessments.

3.4 Each party shall 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 Personal Data; (ii) that persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.5 In addition, and if applicable based on the applicable jurisdiction, each party shall Process the Personal Data solely as provided through the Privacy Signals, including the IAB Policies and the IAB Framework, and similar industry frameworks or guidelines applicable to the Agreement.

3.6 IAB Specifications where applicable: Media Company acknowledges and agrees that the End User does not have a direct relationship with Agency, however, certain features of the Agency Services are dependent and based upon End User's consent or any other demonstrated lawful bases, that shall be obtained by Media Company and which Agency

relies on, amongst others, in its capacity as an Agency under the IAB Framework. The Media Company also acknowledges that it shall be able to demonstrate such consent at any time and represents that such consent exists. Agency shall transfer the Privacy Signal "as is" to the applicable demand partner, as it was provided by the Media Company. The Media Company acknowledges and agrees that such Privacy Signal is directly transmitted to the demand partner "as is", and such demand partner will respond following the Privacy Signal instructions. Agency, as the technical provider, has no actual control over such demand partner and shall not be responsible or liable for the demand partner's actions based on the Privacy Signal or any misuse by the applicable demand partner. Agency is not and will not be liable for any act or omission, misuse or damages, caused by the demand partner, however will contractually require the demand partner to comply with terms similar to the terms of this DPA and the Privacy Signals.

3.7 Notwithstanding the above, it is hereby clarified that: (i) in the EEA, UK and under the TCF, Agency requires Consent for Purpose 1 of the IAB Policy (storage access), and the Media Company shall ensure to call Agency solely upon receiving consent for Purpose 1; (ii) in the EEA, UK or other applicable jurisdiction which requires consent for cookie access or storage (such as ePrivacy Section 5(3)), in case that the Media Company does not have a TCF CMP, the Media Company shall solely call or load Agency's applicable Services upon receiving End User Consent for placing or accessing cookies.

3.8 The Media Company shall (i) provide End Users with applicable privacy documentations and disclosures, including without limitation, a compliant privacy policy that is compliant with applicable Data Protection Laws; (ii) use a CMP approved by the IAB; (iii) document any needed consents and opt-outs, as required under applicable Data Protection Laws and the TCF; and (iv) ensure that End Users can re-access the CMP and easily to manage their privacy choices and preferences.

4. DATA TRANSFER

4.1 Any transfer of Personal Data Processed in connection with the Agreement outside of the jurisdiction from which it was collected shall be transferred subject to and in compliance with an approved transfer mechanism.

4.2 Personal Data may be transferred from the EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland), and the United Kingdom (collectively, "**EEA**") to Adequate Country, without any further safeguard being necessary.

4.3 If the transfers of Personal Data include transfers from the EEA to countries that are not Adequate Country, then parties agree to rely on the Standard Contractual Clauses to facilitate such transfer:

4.3.1 Transfer of Personal Data from the EEA The terms set forth in **Annex III** shall apply.

4.3.2 Transfer of Personal Data from the UK, the terms set forth in **Annex IV** shall apply; and

4.3.3 Transfer of Personal Data from Switzerland, the terms set forth in **Annex NEX V** shall apply.

5. CONFLICT

5.1 In the event of a conflict between the terms and conditions of this DPA and the Agreement, this DPA shall prevail. For the avoidance of doubt, in the event that the Standard Contractual Clauses have been executed between the parties, the terms of the Standard Contractual Clauses shall prevail over those of this DPA solely with regards to international transfer of Personal Data. Except as set forth herein, all of the terms and conditions of the Agreement shall remain in full force and effect.

6. TERM AND TERMINATION

6.1 This DPA shall be effective as of the Effective Date and shall remain in force until the Agreement terminates.

ANNEX I.A

DETAILS OF PROCESSING- Web & App Services, CTV Services, Media Services

This Annex I include certain details of the Processing as required by the SCC where the Agency is Vidazoo Ltd or Intercept Interactive, INC. .

Categories of Data Subjects:

Media Company's End Users / Data Subjects that viewed ads or content which are placed on the Media Company Sites and the ads displayed through the Agency Services.

Categories of Personal Data:

Joint Processed Data: IDs, Privacy String**.**

Agency *Independent Controller Data:*** any Personal Data processed excluding the ID and the Privacy String: tracking data, usage data, approximate location data, referred URL, aggregated insights such as ads viewed, impression data, optimization data, ad delivery data, ad effectiveness data, ad viewability data**.**

Purpose of processing and Joint Controllers:

Agency processes the Agency Independent Controller data to display ad campaigns within the Media Company's assets and properties; analytics and attribution of such advertising campaigns; Frequency capping, audience verification, system maintenance, fraud detection, tracking and measurement of such advertising campaigns.

The Joint Processing Data shall be processed by both Agency and Media Company solely for the purpose of obtaining End Users' preference and choices ("**Permitted Purpose**"). Except for this Permitted Purpose, the parties shall not process the Joint Processed Data for any other purpose or means.

Special Categories of Personal Data:

Not Applicable

Process Frequency:

The Personal Data is transferred on a continuous basis.

Nature of the processing:

Collection, storage, organization, analysis, modification, retrieval, disclosure, communication, and other uses in the performance of the Services as set out in the Agreement. The Joint Processed Data shall be solely collected, stored and transferred.

Retention Period:

For as long as needed to provide the Services and/or comply with applicable laws.

ANNEX I.B

DETAILS OF PROCESSING- Analytics and Throttling Service

This Annex I include certain details of the Processing as required by Article 28(3) GDPR where the Agency is Greenbids SAS ("**GreenBids**").

Categories of Data Subjects:

Media Company's End Users / Data Subjects website users/visitors.

Categories of Personal Data:

IP address (country level)/user agent

Purpose of processing:

Provision of the Services.

Special Categories of Personal Data:

Not Applicable

Process Frequency:

The Personal Data is transferred on a continuous basis.

Nature of the processing:

Temporary collection & real time analysis.

ANNEX II
TECHNICAL AND ORGANISATIONSL MEASURES

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. Conduct security testing or penetration testing, remediate any identified high vulnerabilities, provide written remediation plans for medium and low vulnerabilities;
2. Maintain a level of security appropriate to protect against 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. Adhere password policies for standard and privileged accounts consistent with industry best practices;
5. 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;
6. Maintain a physical security program that is consistent with the corresponding industry practices;
7. 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;
8. Measures and assurances regarding US government surveillance ("**Additional Safeguards**") see **Annex III.**

ANNEX III

EU INTERNATIONAL TRANSFERS AND SCC

1. The parties agree that the terms of the Standard Contractual Clauses are hereby incorporated by reference and shall apply to transfer of Personal Data from the EEA to other countries that are not deemed as Adequate Countries.
2. Module One (Controller to Controller) of the Standard Contractual Clauses shall apply where the transfer is effectuated by the Media Company as the Data Controller of the Personal Data and Agency as the Data Controller of the Personal Data.
3. The parties agree that for the purpose of transfer of Personal Data between the Media Company (as Data Exporter) and the Agency (as Data Importer), the following shall apply:
   a) Clause 7 of the Standard Contractual Clauses shall not be applicable.
   b) In Clause 9, shall not be applicable.
   c) In Clause 11, the optional language will not apply, and data subjects shall not be able to lodge a complaint with an independent dispute resolution body.
   d) In Clause 17, option 1 shall apply. The parties agree that the Standard Contractual Clauses shall be governed by the laws of the EU Member State in which the Media Company is established (where applicable).
   e) In Clause 18(b) the parties choose the courts of the Republic of Ireland, as their choice of forum and jurisdiction.
4. **Annex I.A** of the Standard Contractual Clauses shall be completed as follows:
   1.a.1. "**Data Exporter**": Media Company
   1.a.2. "**Data Importer**": Agency
   1.a.3. Roles: (A) With respect to Module One: (i) Data Exporter is a Data Controller and (ii) the Data Importer is a Data Controller.
   1.a.4. Data Importer Contact Details: As detailed in the Agreement; with copy to privacy@perion.com.
   1.a.5. Signature and Date: By entering into the Agreement and DPA, Data Exporter and Data Importer are deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.
5. **Annex I.B** of the Standard Contractual Clauses shall be completed as follows:
   a) The purpose of the processing, nature of the processing, categories of data subjects, categories of personal data and the parties' intention with respect to the transfer of special categories are as described in **Annex I** (Details of Processing) of this DPA.
   b) The frequency of the transfer and the retention period of the personal data is as described in **Annex I** (Details of Processing) of this DPA.
6. **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 3 above.
7. **Annex II** of this DPA (Technical and Organizational Measures) serves as **Annex II** of the

Standard Contractual Clauses.

8. Each party agrees and hereby represents it maintains, and will continue to maintain, the following additional safeguards in connection with any Personal Data transferred under this **Annex III**:

   a. Maintain industry standard measures to protect the Personal Data from interception (including in transit from Media Company to Agency and between different systems and services). This includes maintaining encryption of Personal Data in transit and at rest.

   b. Make reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the Personal Data protected under the GDPR or the UK GDPR, including (if applicable) under section 702 of the United States Foreign Intelligence Surveillance Court ("**FISA**").

   c. If either party becomes aware of any law enforcement agency or other governmental authority ("**Authority**") attempt or demand to gain access to or a copy of the Personal Data (or part thereof), whether on a voluntary or a mandatory basis, then, unless legally prohibited or under a mandatory legal compulsion that requires otherwise, each party shall: inform the other party, in writing without undue delay, of such Authority demand for access to the Personal Data; and provide reasonable cooperation and assistance to the other party by using reasonable legal mechanisms to challenge any such demand for access to Personal Data which is under the it's control.

   d. Each party shall inform the other party, upon written request (and not more than once a year), of the types of binding legal demands for Personal Data each party has received and complied with, including demands under national security orders and directives, specifically including any process under Section 702 of FISA.

ANNEX IV

UK INTERNATIONAL TRANSFERS AND SCC

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 V** is intended to provide appropriate safeguards for the purposes of transfers of Personal Data to a third country in reliance on Article 46 of the UK GDPR and with respect to data transfers from Controllers to Controllers.

3. Terms used in this **Annex V** that are defined in the Standard Contractual Clauses, shall have the same meaning as in the Standard Contractual Clauses.

4. This **Annex V** shall (i) be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that if fulfills 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.

5. Amendments to the UK Standard Contractual Clauses:

   5.1. Part 1: Tables

      5.1.1. Table 1 Parties: shall be completed as set forth **Annex III** above.

      5.1.2. Table 2 Selected SCCs, Modules and Selected Clauses: shall be completed as set forth in **Annex III** above.

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

      5.1.4. Table 4 Ending this Addendum when the Approved Addendum Changes: shall be completed as “neither party”.

ANNEX V

SUPPLEMENTARY TERMS FOR SWISS DATA PROTECTION LAW TRANSFERS ONLY

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 to 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

US PRIVACY LAWS ADDENDUM

1. This US Privacy Law Addendum ("**US Addendum**") adds specifications applicable to US Data Protection Laws and is in addition to the obligations set forth in the DPA. All terms used but not defined in this US Addendum shall have the meaning set forth in the DPA.

2. Notwithstanding the above, in the event the parties are members of the MSPA, the MSPA shall prevail.

3. ROLES:

3.1. Parties shall act as a separate independent Controllers, except when the Processing is for a Restricted Purpose, in which Agency may be deemed a Processor. Specifically, under the CCPA, the Agency shall be a Third Party except when processing Personal Information for a Restricted Purpose, in which it shall be defined as a Service Provider.

3.2. For the purpose of this US Addendum the "**Restricted Purposes**" means advertising-related processing that qualifies as a Business Purpose, including (i) auditing, security and integrity purposes, debugging, short term, transient uses, and internal research or improvement of the Services; (ii) technical advertising services that are not targeted, cross-contextual or profiling and include frequency capping, measurement, fraud detection and prevention, and ensuring and measuring viewability; and (iii) contextual advertising which includes first-party advertising to the extent such activity does not result in a Sale or Share of Personal Data or constitute processing of Personal Data for Targeted Advertising purposes.

3.3. The subject matter, duration, nature, and purpose of the Processing, types of Personal Information Processed, and categories of Data Subjects are as described in **Annex I**.

4. CONTROLLER TO CONTROLLER:

In their roles as Controllers, Business or Third Party, each party shall, when Processing End User Personal Data:

4.1. Be individually and separately responsible for complying with applicable US Data Protection Laws, and to the extent applicable to the IAB Policies.

4.2. Provide End Users with clear and conspicuous disclosures and notices on how the Personal Information is Processed, the purpose of Processing, the categories of Personal Information shared and the categories of the recipients, as well as the End Users' rights, including the right to appeal and the ability to opt out of the Sale, Share of Personal Information or from Targeted Advertising, all in compliance with and as required by the US Data Protection Laws.

4.3. Ensure that it provides an opt-out mechanism and it enables the End User to send a Privacy Signal and transfer the Privacy Signal down the advertising chain. When a Privacy Signal is received, neither party will process such End Users' Personal Information for Targeted Advertising, or Cross Contextual Advertising purposes.

4.4. Comply with requirements for processing Deidentified Information, including by not attempting to re-identify it, using reasonable, technical, and organizational measures to prevent re-identifying it, and publicly committing to such actions.

5. CONTROLLER TO PROCESSOR

Where **(i)** Agency licenses the Agency Technology to the Media Company as a white label, or otherwise; **(ii)** processing Personal Information for the Restricted Purpose processing, in its role as a Processor or Service Provider, as applicable the Agency shall be deemed a Processor or Service Provider as applicable and shall comply with the DPA and the additional requirements and obligations set forth below:

5.1. **Representation and Undertaking**: a party shall process the End User Personal Information only on behalf of and under the instructions of the other party and in accordance with US Data Protection Laws and shall not: (**i**) Sell or Share the Personal Information; (**ii**) retain, use or disclose the Personal Information for any purpose other than for a Business Purpose or Restricted Purpose as specified in the Agreement; (**iii**) combine the End User Personal Information with other Personal Information that it receives from, or on behalf of, another partner, or collects from its own; or (**iv**) if and to the extent applicable limit the use of its Sensitive Personal Information ("**SPI**").

5.2. **Sub-processors or Sub-contractors**: The Controller party provides a general authorization to engage sub-processors to the extent the Processor party undertakes it will restrict the onward sub-processor's access only to what is strictly necessary, and will prohibit the sub-processor from Processing the Personal Information for any other purpose other than for a Business Purpose or Restricted Purpose as specified in the Agreement. The Processor party shall impose contractual obligations as required by US Data Protection Laws on such sub-processors.

5.3. **Audit**: A Controller party has the right to ensure the Processor party is in compliance with US Data Protection Laws. For this purpose, the Processor party, upon receiving a reasonable written request from the Controller party, will make available to the Controller party information necessary to demonstrate compliance with this DPA and US Data Protection Laws. To the extent required by applicable US Data Protection Laws, and upon receiving prior written notice, the Processor party will allow audits, including inspections, by the Controller party (or an auditor on its behalf). Any such audit must be tailored to what is reasonably necessary to verify compliance with this DPA, and must occur during normal business hours, and not more than once per calendar year. The results of the audit will be the confidential information of the Processor party. Notwithstanding the above, under US Data Protection Laws and subject to the Media Company's consent, the Processor party may alternately, in response to the Controller party's on-premise audit request to initiate an independent auditing on its own, to verify its compliance with its obligations under US Data Protection Laws and provide the Media Company with the results. In any case, the expenses of the audit shall be paid by the Controller party. The Processor party may refuse

audit or access to certain information if it determines it may harm other partners or customers, or it may cause a security breach, or it is not related or necessary for the purpose of demonstrating compliance with US Data Protection Laws.

5.4. **Certification**: The Processor party certifies that it understands the rules, requirements, and definitions of the CCPA and agrees to refrain from Selling or Sharing Personal Information. The Processor party acknowledges and confirms that it does not receive any monetary goods, payments, or discounts in exchange for processing the Personal Information for a Business Purpose or Restricted Purpose as specified in the Agreement.