ADDENDUM TO AGREEMENT

DATA SERVICES, USE, AND PROCESSING

This Data Services, Use, and Processing Addendum (this "**Addendum**") is incorporated by reference and is made a part of the General Terms of Sale or similar agreement (the "**Agreement**") between the Parties. All terms included in this Addendum shall be in addition to, and not in replacement of, those terms set forth in the Agreement. In the event of any conflict or inconsistency between the terms of this Addendum and the terms of the Agreement, the terms of this Addendum will control. All capitalized terms not specifically defined in this Addendum shall be read to have the meaning given to those terms in the Agreement.

1. DATA DEFINITIONS

A. "**Client Data**" means any Personal Data that Quad receives in providing Work to a Client pursuant to an Order.

B. "**Controller**" means an entity that alone or jointly with others determines the purposes and means of Processing Personal Data, and includes the term "business" as defined by the CCPA.

C. "**Data Privacy Law**" means any applicable law relating to the protection of Personal Data, as the case may be, including the EU Data Protection Directive 95/46/EC (the "Directive"), the California Consumer Privacy Act ("**CCPA**") and the EU General Data Protection Regulation 2016/679 ("**GDPR**").

D. "**Data Subject**" or any similar term used in any Data Privacy Laws, such as Consumer, has the meaning set forth in the applicable Data Privacy Law.

E. "**Job Metadata**" means data that is generated by Quad and is related to the type or category of work or to facilitate production of a job, including without limitation such information as title code, job number, date produced, date mailed, brand or publication, campaign or issue, version of the pieces, business-to-business, or direct-to-consumer.

F. "**Personal Data**" or any similar term used in any Data Privacy Laws, such as "Personal Information" as that term is used in the CCPA, means any (i) information relating to an identified or identifiable natural person; an identifiable person is one who can be defined, directly or indirectly, for example by reference to a user identification such as a name, an identification number, geo-location data, an online user identification, or by reference to one or more factors specific to the Data Subject's physical, physiological, genetic, mental, economic, cultural, or social identity, and (ii) any Sensitive Data. For purposes of this Addendum, Personal Data does not include Job Metadata.

G. "**Process or Processing**" has the correlative meaning to Process as set forth in the applicable Data Privacy Law, and includes the term "service provider" as defined by the CCPA.

H. "**Quad Proprietary Dataset**" means a consumer dataset owned and controlled by Quad.

I. "**Sensitive Data**" means any data of a highly sensitive nature that is regulated under Data Privacy Laws, which may include, but is not limited to, any "Special Categories of Personal Data" as set out in Article 9 of the GDPR.

J. "**Security Incident**" means: (i) any loss or compromise of Personal Data, or (ii) any unauthorized use, disclosure and/or destruction of Personal Data, or (iii) any unauthorized modification and/or access to Personal Data.

2. MUTUAL OBLIGATIONS

A. Personal Data will be treated as Confidential Information.

B. With respect to any Personal Data received by the other Party, the Receiving Party will comply with its obligations under all applicable Data Privacy Laws.

C. Each Controller has collected all Personal Data and transferred that Personal Data to the other Party, as applicable, in accordance with its own policies, all necessary or required privacy notices, and in accordance with all applicable laws.

D. Each Party will promptly notify the other Party if it reasonably believes that an instruction issued by the other Party would violate any applicable Data Privacy Laws.

E. Each Party will provide reasonable cooperation to the other to enable it to: (i) respond to requests for exercising Data Subjects' rights under Data Privacy Laws; and (ii) comply with requests from a government or other regulatory authorities, including but not limited to in the event of an investigation. All costs of such cooperation will be borne by Controller.

F. Each Party will notify the other Party in the event it receives any request, complaint, or communication relating to either Party's obligations under Data Privacy Laws (including from a government or other regulatory authority). To the extent permitted by applicable law and as applicable, a Party acting as a processor for Controller must obtain specific written consent and instructions from the party acting as a Controller prior to responding to such request, complaint, or communication.

G. Each Party must protect Personal Data against a Security Incident in accordance with Data Privacy Law. As such, each Party will maintain Personal Data received from the other Party in a secure fashion aligned with industry standards and best practices for the management, transport, storage, and other Processing of highly valuable confidential business data, including without limitation security procedures and maintenance of physical, technical/electronic, and administrative/procedural safeguards, and commercially reasonable or better system and data security. Further, each Party must have and maintain policies and procedures reasonably designed to detect and respond to Security Incidents.

H. To the extent either Party receives a request from a third party public authority including a law enforcement agency or government agency for disclosure of the Personal Data, the Receiving Party must, without undue delay, notify the Disclosing Party in writing of such request unless otherwise legally prohibited (such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). Such notification will set out: (i) the scope of the request; (ii) the reason for the request; and (iii) the form of the disclosure requested, in so far as the Party is able to describe such aspects. Where a Party is legally prohibited from notifying the other, the Receiving Party must use reasonable efforts to request the third party public authority to direct the request directly to Disclosing Party.

3. ADDITIONAL QUAD OBLIGATIONS

A. Quad will Process Client Data in accordance with the documented instructions received from the Client as Controller. Quad shall not: (i) sell (as defined by the CCPA) the Client Data; (ii) retain, use, or disclose the Client Data other than in connection with its obligations under the Agreement, including for a commercial purpose, except to the extent permitted by applicable law and as specified in Section 5 of this Addendum; or (iii) retain, use, or disclose any Client Data outside of the direct business relationship between Client and Quad except as specified in Section 5 of this Addendum. Client, acting as Controller, may provide Quad with general or specific instructions regarding the data Processing provided as part of the Work. Instructions must be issued in writing or via e-mail. For the avoidance of doubt, this paragraph does not apply to Job Metadata.

B. Quad will delete and destroy all Client Data (including copies thereof) within a reasonable time after providing the Work.

C. In the event Quad engages a subprocessor to Process Client Data, Quad will require such subprocessor to comply with the same obligations applicable to Quad under this Addendum.

4. ADDITIONAL CLIENT OBLIGATIONS

A. Client will only provide Quad with the minimum necessary Personal Data that is required for Quad to perform the Work.

B. Client will specifically identify any Sensitive Data in writing prior to transferring that Sensitive Data to Quad so that Quad may use the appropriate operational platforms and protocols structured to comply with applicable Data Privacy Laws.

C. Client must only provide instructions to Quad that comply with applicable law, and Client represents and warrants that the Processing of Personal Data in accordance with Client's instructions must not cause Quad to be in breach of any applicable laws.

5. Quad Use of Job Metadata

A. The Parties acknowledge and agree that Quad:

i. is authorized to use Client Data for the limited purpose of matching individuals associated with a job (e.g., individuals that are included in mailing lists) with existing information about those individuals that have been separately obtained in the Quad Proprietary Dataset and to append the associated Job Metadata to the existing information about those individuals in the Quad Proprietary Dataset;

ii. shall not otherwise collect, use, retain or further disclose Client Data other than in connection with its obligations under the Agreement; and

iii. is not providing Client with any monetary or other valuable consideration in connection with its use of Client Data as contemplated under this Section.

B. For the avoidance of doubt, Quad is authorized to retain, use and further disclose Job Metadata for the purpose of analytics, to test, develop, and create new product and service offerings, or for other business or commercial purposes.

6. SECURITY INCIDENTS

A. In the event of a Security Incident affecting one or both of the Parties' Personal Data, the Party responsible for the Security Incident must, at its own cost: (i) notify the Disclosing Party about the Security Incident without undue delay after becoming aware of the Security Incident, and as part of the notification provide a description of the Security Incident including to the extent possible the nature of the Security Incident, the categories and approximate number of Data Subjects affected, and the categories and approximate number of data records affected; (ii) promptly begin a full investigation into the circumstances surrounding the Security Incident; and (iii) take such actions as may be necessary or reasonably expected to minimize the effects of the Security Incident and to prevent a reoccurrence of the Security Incident.

B. The Parties will cooperate with each other with respect to the investigation of, response to, and remediation of, any such Security Incident, and will share all applicable information (except to the extent prohibited by applicable law) to the other with respect to the Security Incident. Each Party will use all reasonable efforts in good faith to mitigate any reputational and brand damage to the other affected Party and any loss or damage that may arise from the Security Incident.

C. Any Security Incident and all information, analyses, and conclusions resulting from the investigation into the Security Incident will be considered Confidential Information of the Receiving Party.

D. Except to the extent that the Security Incident is caused by the Disclosing Party, the Receiving Party is responsible for all documented out-of-pocket costs for the following resulting from its failure to comply with its obligations under this Addendum:

iv. preparing and providing notice of any Security Incident to government bodies, data protection authorities, or supervisory authorities required to be notified under Data Privacy Laws;

v. preparing and providing notices to Data Subjects affected by the Security Incident that are legally required by Data Privacy Laws; and

vi. any remediation, or correction activities that are required by Data Privacy Laws to be provided to the affected Data Subjects in connection with the Security Incident, provided, however, that unless otherwise required by law, no such disclosures or notifications will be made by a Party without first cooperating with the affected Party.