Data Protection Addendum

This Data Protection Addendum ("**Addendum**") forms part of the Master Services Agreement by and between Anteriad, LLC ("**Anteriad**") and the customer named in the Agreement ("**Customer**"), each a "**Party**" and collectively the "**Parties.**" This Addendum applies to and takes precedence over that document and any associated contractual document between the Parties, such as an order form, statement of work or data protection addendum thereunder (collectively, together with the Master Services Agreement, the "**Agreement**"), to the extent of any conflict.

Customer and Anteriad agree as follows:

1. **Definitions**. For purposes of this Addendum:

   a. "**Data Privacy Law(s)**" means all applicable laws, regulations, and other legal or self-regulatory requirements in any jurisdiction relating to privacy, data protection, data security, breach notification, or the Processing of Personal Data, including without limitation, to the extent applicable, the General Data Protection Regulation, Regulation (EU) 2016/679 ("**GDPR**"), the United Kingdom Data Protection Act of 2018 ("**UK Privacy Act**"), the Swiss Federal Act on Data Protection ("**FADP**"), the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* and associated regulations ("**CCPA**"), and the following, when effective and together with any associated regulations: the California Privacy Rights Act ("**CPRA**"), the Colorado Privacy Act ("**CPA**"), Connecticut's Act Concerning Personal Data Privacy and Online Monitoring ("**Connecticut Data Privacy Act**" or "**CDPA**"), the Utah Consumer Privacy Act ("**UCPA**"), and the Virginia Consumer Data Protection Act ("**VCDPA**"). For the avoidance of doubt, if Anteriad's Processing activities involving Personal Data are not within the scope of a given Data Privacy Law, such law is not applicable for purposes of this Addendum.

   b. "**Data Subject**" means an identified or identifiable natural person about whom Personal Data relates.

   c. "**EU SCCs**" means the Standard Contractual Clauses issued pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 *on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, located http://data.europa.eu/eli/dec_impl/2021/914/oj and completed as set forth in Section 7 below.

   d. "**Personal Data**" includes "personal data," "personal information," "personally identifiable information," and similar terms, and such terms shall have the same meaning as defined by applicable Data Privacy Laws, that is Processed in relation to the Agreement.

   e. "**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

f. "**Security Breach**" means any accidental or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

2. **Scope and Purposes of Processing**.

a. The scope, nature, purposes, and duration of the processing, the types of Personal Data Processed, and the Data Subjects concerned are set forth in this Addendum, including its Exhibits. The details provided in Exhibit A are deemed to satisfy any requirement to provide some or all of such details under any Data Privacy Law.

b. Anteriad will Process Personal Data solely: (1) to fulfill its obligations to Customer under the Agreement, including this Addendum; (2) on Customer's behalf; and (3) in compliance with Data Privacy Laws. Anteriad will not "sell" Personal Data (as such term is defined in applicable Data Privacy Laws), "share" Personal Data for purposes of "cross-context behavioral advertising" (as such terms are defined in applicable Data Privacy Laws), or otherwise Process Personal Data for any purpose other than for the specific purposes set forth herein or outside of the direct business relationship with Customer.

3. **Personal Data Processing Requirements**. Anteriad will comply with any applicable restrictions under Data Privacy Laws on combining Personal Data with personal data that Anteriad receives from, or on behalf of, another person or persons, or that Anteriad collects from any interaction between it and a Data Subject. Anteriad will:

a. Provide the same level of protection for Personal Data as is required under the Data Privacy Laws applicable to Customer.

b. Ensure that the persons it authorizes to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c. Assist Customer in the fulfilment of Customer's obligations to respond to verifiable requests by Data Subjects (or their lawful representatives) for exercising their rights under Data Privacy Laws (such as rights to access or delete Personal Data).

d. Promptly, and in any event within fifteen (15) days, notify Customer of (i) any third-party or Data Subject complaints regarding the Processing of Personal Data; or (ii) any government or Data Subject requests for access to or information about Anteriad's Processing of Personal Data on Customer's behalf, unless prohibited by Data Privacy Laws. If Anteriad receives a third-party, Data Subject, or governmental request, Anteriad will await written instructions from Customer on how, if at all, to assist in responding to the request. Anteriad will provide Customer with reasonable cooperation and assistance in relation to any such request. If Anteriad is prohibited from providing notice regarding a government request and determines that the request would interfere with Anteriad's ability to meet its obligations under this Addendum, Anteriad will notify Customer that Anteriad can no longer comply with this Addendum, without being required to identify the specific provision with which it can no longer comply.

e. Provide reasonable assistance to and cooperation with Customer for Customer's performance of a data protection impact assessment of Processing or proposed Processing of Personal

Data, when required by applicable Data Privacy Laws.

f. Provide reasonable assistance to and cooperation with Customer for Customer's consultation with regulatory authorities in relation to the Processing or proposed Processing of Personal Data, including complying with any obligation applicable to Anteriad under Data Privacy Laws to consult with a regulatory authority in relation to Anteriad's Processing or proposed Processing of Personal Data.

4. **Data Security**. Anteriad will implement appropriate administrative, technical, physical, and organizational measures to protect Personal Data, as set forth in Exhibit B.

5. **Security Breach**. Anteriad will notify Customer promptly, and in any event within seventy-two hours, of any Security Breach. Anteriad will comply with the Security Breach-related obligations directly applicable to it under Data Privacy Laws and will assist Customer in Customer's compliance with its Security Breach-related obligations, including without limitation by:

a. At Anteriad's own expense, taking steps to mitigate the effects of the Security Breach and reduce the risk to Data Subjects whose Personal Data was involved; and

b. Providing Customer with the following information, to the extent known:

i. The nature of the Security Breach, including, where possible, how the Security Breach occurred, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;

ii. The likely consequences of the Security Breach; and

iii. Measures taken or proposed to be taken by Anteriad to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects.

6. **Subcontractors**.

a. Customer acknowledges and agrees that Anteriad may use Anteriad affiliates and other subcontractors to Process Personal Data in accordance with the provisions within this Addendum and Data Privacy Laws. Where Anteriad sub-contracts any of its rights or obligations concerning Personal Data, including to any affiliate, Anteriad will: (1) take steps to select and retain subcontractors that are capable of maintaining appropriate privacy and security measures to protect Personal Data consistent with applicable Data Privacy Laws; and (ii) require that each subcontractor complies with obligations that are no less restrictive than those imposed on Anteriad under this Addendum.

b. To the extent required by applicable Data Privacy Laws where applicable, Anteriad has provided a current list of Anteriad's subprocessors listed herein as Exhibit C, and Customer hereby consents to Anteriad's use of such subprocessors. Anteriad will maintain an up-to-date list of its subprocessors, and it will provide Customer with reasonable notice of any new subprocessor added to the list. In the event Customer objects to a new subprocessor, Anteriad will not transfer Personal Data to the new subprocessor and will use reasonable efforts to make available to Customer a change in the services or recommend a commercially reasonable change to Customer's use of the services to avoid Processing of Personal Data by

the objected-to subprocessor without unreasonably burdening the Customer. Where such accommodation cannot be made to the satisfaction of both parties, either party may terminate the Agreement on ten (10) days' written notice to the other.

7. **Data Transfers.**

a. Anteriad will not engage in any cross-border Processing of Personal Data, or transmit, directly or indirectly, any Personal Data to any country outside of the country from which such Personal Data was collected, without complying with applicable Data Privacy Laws. Where Anteriad engages in an onward transfer of Personal Data, Anteriad shall ensure that a lawful data transfer mechanism is in place prior to transferring Personal Data from one country to another.

b. To the extent legally required, by signing this Addendum, Customer and Anteriad are deemed to have signed the EU SCCs, which form part of this Addendum and (except as described in Section 7(c) and (d) below) will be deemed completed as follows:

i. Module 2 of the EU SCCs applies to transfers of Personal Data from Customer (as a controller) to Anteriad (as a processor);

ii. Clause 7 (the optional docking clause) is not included;

iii. Under Clause 9 (Use of sub-processors), the Parties select Option 2 (General written authorization). The initial list of sub-processors is set forth in Exhibit C of this Addendum and Anteriad shall propose an update to that list at least 10 business days in advance of any intended additions or replacements of sub-processors in accordance with Section 6(b) of this Addendum;

iv. Under Clause 11 (Redress), the optional language requiring that data subjects be permitted to lodge a complaint with an independent dispute resolution body shall not be deemed to be included;

v. Under Clause 17 (Governing law), the Parties choose Option 1 (the law of an EU Member State that allows for third-Party beneficiary rights). The Parties select the law of Ireland;

vi. Under Clause 18 (Choice of forum and jurisdiction), the Parties select the courts of Ireland;

vii. Annex I(A) and I(B) (List of Parties) is completed as set forth in Exhibit A of this Addendum;

viii. Under Annex I(C) (Competent supervisory authority), the Parties shall follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the Irish Data Protection Commission.

ix. Annex II (Technical and organizational measures) is completed with Exhibit B of this Addendum; and

x. Annex III (List of subprocessors) is not applicable as the Parties have chosen General Authorization under Clause 9.

c. With respect to Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available as of the Effective Date at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) ("UK SCCs") forms part of this Addendum and takes precedence over the rest of this Addendum as set forth in the UK SCCs. Undefined capitalized terms used in this provision shall mean the definitions in the UK SCCs. For purposes of the UK SCCs, they shall be deemed completed as follows:

i. Table 1 of the UK SCCs:

1. The Parties' details shall be the Parties and their affiliates to the extent any of them is involved in such transfer.

2. The Key Contact shall be the contacts set forth in the Agreement.

ii. Table 2 of the UK SCCs: The Approved EU SCCs referenced in Table 2 shall be the EU SCCs as executed by the Parties.

iii. Table 3 of the UK SCCs: Annex 1A, 1B, II, and III shall be set forth in Exhibits A, B, and C below.

iv. Table 4 of the UK SCCs: Either Party may end this Addendum as set out in Section 19 of the UK SCCs.

v. By entering into this Addendum, the Parties are deemed to be signing the UK SCCs.

d. For transfers of Personal Data that are subject to the FADP, the EU SCCs form part of this Addendum as set forth in Section 7(b) of this Addendum, but with the following differences to the extent required by the FADP: (1) references to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR; (2) references to personal data in the EU SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope; (3) term "member state" in EU SCCs shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs; and (4) the relevant supervisory authority is the Swiss Federal Data Protection and Information Commissioner (for transfers subject to the FADP and not the GDPR), or both such Commissioner and the supervisory authority identified in the EU SCCs (where the FADP and GDPR apply, respectively).

8. **Audits**. Anteriad will make available to Customer information sufficient to demonstrate compliance with this Addendum, including with respect to information security protocols (such as, for instance, providing copies of most recent information security audits, redacted as necessary to preserve sensitive or proprietary information).

9. **Return or Destruction of Personal Data**. Except to the extent required otherwise by Data Privacy Laws, Anteriad will, at the choice of Customer, return to Customer and/or securely destroy all Personal Data upon (a) written request of Customer or (b) termination of the Agreement. Except to the extent prohibited by Data Privacy Laws, Anteriad will inform Customer if it is not able to return or delete the Personal Data.

10. **Survival**. The provisions of this Addendum survive the termination or expiration of the Agreement for so long as Anteriad or its subcontractors Process the Personal Data.

Exhibit A

A. LIST OF PARTIES

Data exporter(s):
Name: The data exporter is Customer.

Activities relevant to the data transferred under these SCCs: The data exporter is a user of the data importer's Services pursuant to their underlying Agreement. The data exporter acts as a controller with respect to its own personal data. To the extent permitted by the Agreement, the exporter also is permitted to use the contracted Services as a processor on behalf of third parties.

Signature and date: The Parties agree that execution of the Agreement shall constitute execution of these SCCs by both Parties.

Data importer(s):
Name: The data importer is Anteriad.

Activities relevant to the data transferred under these SCCs: The data importer is the provider of Services to the data exporter and its customers pursuant to their underlying Agreement. The data importer acts as the data exporter's processor.

Signature and date: The Parties agree that execution of the Agreement shall constitute execution of these SCCs by both Parties.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: The personal data transferred concerns data regarding potential leads for marketing and advertising.

Categories of personal data transferred: The personal data transferred concern the names and email addresses of potential leads (related business information).

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: N/A

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

Nature of the processing: Data importer's Processing activities shall be limited to those discussed in the Agreement and the Addendum.

Purpose(s) of the data transfer and further processing: The objective of the transfer and further processing of personal data by Anteriad is to provide services to the Customer.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Personal data will be retained for the period of time necessary to provide the Services to Customer under the Agreement, the Addendum, and/or in accordance with applicable legal requirements.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: Same as above to the extent such information is provided to subprocessors for purposes of providing the Services.

C. COMPETENT SUPERVISORY AUTHORITY

See Section 7(b)(viii) of the Addendum.

Exhibit B

ANTERIAD DATA SECURITY MEASURES

Anteriad will implement and maintain the following administrative, technical, physical, and organizational security measures for the Processing of Personal Data:

Anteriad's Information Security Program includes specific security requirements for its personnel and all subcontractors or agents who have access to Personal Data ("**Data Personnel**"). Anteriad's security requirements covers the following areas:

1. Information Security Policies and Standards. Anteriad will maintain written information security policies, standards and procedures. These policies, standards, and procedures shall be kept up to date, and revised whenever relevant changes are made to the information systems that use or store Personal Data. These policies, standards, and procedures shall be designed and implemented to:

    a. Prevent unauthorized persons from gaining physical access to Personal Data Processing systems (e.g. physical access controls);

    b. Designate one or more employees, or competent subcontractors, to coordinate the Information Security Program;

    c. Prevent Personal Data Processing systems from being used without authorization (e.g. logical access control); and

    d. Ensure that all systems that Process Personal Data are subject to regular vulnerability scanning.

2. Physical Security. Anteriad will maintain commercially reasonable security systems at all Anteriad sites at which an information system that uses or stores Personal Data is located ("**Processing Locations**") that include reasonably restricting access to such Processing Locations, and implementing measures to detect, prevent, and respond to intrusions.

3. Organizational Security. Anteriad will maintain information security policies and procedures addressing:

    a. Data Disposal. Procedures for when media are to be disposed or reused have been implemented to prevent any subsequent retrieval of any Personal Data stored on media before they are withdrawn from the Anteriad's inventory or control.

    b. Data Minimization. Procedures for when media are to leave the premises at which the files are located as a result of maintenance operations have been implemented to prevent undue retrieval of Personal Data stored on media.

    c. Incident Response. All Security Breaches are managed in accordance with appropriate incident response and remediation procedures.

4. Network Security. Anteriad maintains commercially reasonable information security policies and procedures addressing network security.

5. Access Control (Governance).

    a. Anteriad governs access to information systems that Process Personal Data.

    b. Only authorized Anteriad staff can grant, modify or revoke access to an information system that Processes Personal Data.

    c. Anteriad implements commercially reasonable physical and technical safeguards to create and protect passwords.

6. Virus and Malware Controls. Anteriad protects Personal Data from malicious code and will install and maintain anti-virus and malware protection software on any system that handles Personal Data.

7. Personnel.

    a. Anteriad has implemented and maintains a security awareness program to train employees about their security obligations.

    b. Anteriad shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may Process Personal Data.

Exhibit C

ANTERIAD SUBPROCESSORS

Entity Name	**Subprocessing Activities**	**Location(s) of Processing**