



DATA PROCESSING AGREEMENT – CUSTOMER DATA USED IN CAMPAIGNS

This Data Processing Agreement is signed by and between:

Metadata, Inc., a company incorporated under the laws of the State of Delaware, USA, having its principal place of business at 880 Harrison St. Suite 303C, San Francisco, CA 94107 (USA) (the “**Data Processor**”);

and

The other party to the Main Agreement with Metadata, Inc., as defined below (the “**Data Controller**”).

Data Processor and Data Controller are also individually referred to herein as a “**Party**” and collectively as the “**Parties**”.

RECITALS

I. Data Processor and Data Controller agreed to an Order and the Terms of Use Agreement incorporated therein (the “**Main Agreement**”).

II. Pursuant to the Main Agreement and for the provision of, and solely for the provision of, Customer Data as defined in the Main Agreement for the purposes of Campaigns (as defined below), the Data Processor may process Personal Data contained in Customer Data on behalf of the Data Controller.

III. The Parties agree to comply with the following provisions with respect to any Personal Data transferred to the Data Processor in Customer Data in connection with the provision of Campaigns.

NOW, THEREFORE, THE PARTIES AGREE AS FOLLOWS:

1. Definitions

“**Campaigns**” means the advertising campaign activities described in the Order and the Main Agreement and provided by the Data Processor to the Data Controller under the terms agreed in the Main Agreement.

“**CCPA**” means the California Consumer Privacy Act.

“**Customer Data**” has the meaning set forth in the Main Agreement.

“**Data Controller**” means the Party that determines the purposes and means of the processing of Personal Data, namely, the entity identified above, as noted above.

“**Data Processor**” means the Party who processes Personal Data on behalf of the Data Controller, namely, Metadata, Inc., as noted above.

“**Data Protection Law(s)**” means all applicable laws relating to the processing of Personal Data and privacy that may exist in any relevant jurisdiction, including, where applicable, guidance and codes of practice issued by the supervisory authorities, and including, CCPA and, in the case of EU Personal Data, European Directives 95/46 and 2002/58 (as amended by Directive 2009/136/EC) and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them (including the General Data Protection Regulation (Regulation (EU) 2016/679), “**GDPR**”).

“**Data Subject**” means the person to whom the Personal Data relates.

“**Effective Date**” means the date of last signature by any of the Parties.

“**European Economic Area**” means a Member State of the European Union, together with Norway, Iceland, and Liechtenstein (jointly referred to as “**EEA**”).

“**EU Personal Data**” means Personal Data which is, or has been, subject to the data protection law of a Member State of the EEA, the United Kingdom, and/or Switzerland.

“**Loss**” means a loss of data that occurs during the processing of files containing Personal Data by the Data Processor.

“**Main Agreement**” means the Order, and the Terms of Use Agreement incorporated therein, between Data Controller and Data Processor, which includes but is not limited to the provision of the Campaign.

“**Main Establishment**” has the meaning set forth under the GDPR.

“**Personal Data**” means any information relating to an identified or identifiable natural person contained in the Customer Data; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person that the Data Processor has received from the Data Controller on or after the Effective Date for Processing pursuant to the Main Agreement when such data is protected as “personal data” or “personally identifiable information” or a similar term under applicable Data Protection Laws.

“**Personal Data Breach**” means any accidental, unauthorized or unlawful destruction, loss, alteration, or disclosure of, or access to Personal Data where such compromise of the Personal Data meets the definitions of both “personal data” (or like term) and “security breach” (or like term) under Applicable Law(s) governing the particular circumstances.

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

“**Sub-processor**” means any processor engaged by the Data Processor or by any other Sub-processor of the Data Processor who receives Personal Data exclusively intended for processing activities to be carried out on behalf of the Data Controller for the provision of the Campaign.



“Supervisory Authority” has the meaning set forth under the GDPR.

2. Scope of the Agreement

2.1. The Personal Data to be transferred or collected for processing pursuant to the Main Agreement shall consist of the following categories of data:

First and last name, email address, and employer’s company name

2.2. The categories of Data Subjects whose Personal Data shall be processed are:

Contact persons for Data Controller’s customers and/or prospective customers

2.3. The nature and purpose of processing activities to be undertaken by Data Processor are:

Conducting the Campaigns on behalf of Data Controller whereby Data Processor will ascertain customer audiences from the Customer Data

3. Obligations of the Data Controller

3.1. In accordance with the Data Protection Laws, the Data Controller remains responsible for ensuring the rights of the concerned Data Subjects, including but not limited to, access to their data, rectification of inaccurate or incomplete data, or erasure of their data.

3.2. Data Controller will inform its Data Subjects (i) about its use of Data Processor to process their Personal Data and (ii) that their Personal Data will be processed outside of the European Economic Area.

3.3. The Data Controller shall without undue delay inform the Data Processor when it discovers errors or irregularities in the processing of Personal Data in accordance with applicable Data Protection Laws.

3.4. The Data Controller shall respond in a reasonable time to enquiries from any Supervisory Authority regarding the processing of relevant Personal Data by the Data Controller. If any Party is required under applicable Data Protection Laws to issue information to any Supervisory Authority regarding the collection, processing, or use of Personal Data, the other Party may support the responding Party in its efforts to provide such information.

4. Obligations of the Data Processor

4.1. In providing the Campaigns, the Data Processor shall comply with the instructions of the Data Controller for the processing of Personal Data and process the Personal Data exclusively to ensure the provision of the Campaign. The provisions of this Data Processing Agreement are the main source of instructions issued by the Data Controller. Any amendments to the Processing requirements shall be agreed between the Parties and documented in writing.

4.2. Data Processor shall assist Data Controller:

- (i) in responding to requests by Data Subjects to exercise their rights; and
- (ii) in complying with its obligations in relation to security of Personal Data under applicable Data Protection Laws, including but not limited to, as applicable, data protection impact assessment and prior consultation, taking into account the nature of the services and the information available to Data Processor.
- (iii) carrying out a request from Data Controller to amend, transfer, or delete any of the Personal Data to the extent necessary to allow Data Controller to comply with its responsibilities as a data controller under applicable Data Protection Laws.

4.3. Notification of Non-Compliance with Data Protection Requirements:

The Data Processor shall inform the Data Controller immediately if it becomes aware:

- (i) That Data Processor’s employees, subcontractors, and/or any third party engaged in the Processing fail to comply with any requirements regarding the protection of Personal Data or any provisions of this Data Processing Agreement; and/or
- (ii) Of any other irregularity in the Processing of Personal Data.

4.4. Storage and Erasure of Data

- (i) The Data Processor shall store the Personal Data as long as it is needed for the provision of the Campaigns and in accordance with applicable Data Protection Laws.
- (ii) The Data Processor must store with reasonable care the Personal Data together with any copies or reproductions made of such Personal Data securely so that it is not accessible to third parties.
- (iii) Any Personal Data that is no longer required will be deleted in accordance with applicable Data Protection Laws.

- (iv) Upon request by Data Controller or upon termination or expiration of the Main Agreement, Data Processor shall at Data Controller's choice (a) deliver to Data Controller all Personal Data (and any copies or derivative works of same) in its possession and/or, (b), destroy all Personal Data (and any copies or derivative works of same) in its possession, and certify to Data Controller that it has done so, unless otherwise required under operation of Data Protection Laws, or as mutually agreed by the Parties, and/or (c) cease any Processing of Personal Data.

4.5. Data Access and Modification

- (i) Data Processor shall permit Data Subjects access to their respective Personal Data. In particular, Data Subjects shall be permitted to correct, amend, or delete inaccurate Personal Data at no additional cost.
- (ii) Both Parties agree that, in the event of receiving a Data Subject complaint or access request that may involve the other Party, to notify the other Party without delay and to provide such cooperation and assistance as may be reasonably required to enable that Party to deal with any Data Subject complaint or access request in accordance with the provisions of the applicable Data Protection Laws.
- (iii) To the extent that the Data Controller does not have the ability to correct, amend, block, or delete already transferred Personal Data, the Data Processor shall comply with any reasonable request by the Data Controller to facilitate such actions as required by Data Protection Laws.
- (iv) If the Data Processor becomes aware of any errors or incorrectness of Personal Data, the Data Processor shall notify the Data Controller prior to correcting such data. Whenever a situation arises where this may be appropriate and in line with statutory provisions, consideration may be given to blocking data instead of erasing it.

4.6. Upon request by Data Controller with reasonable notice, Data Controller (or a duly qualified independent auditor selected by Data Controller and not unreasonably objected to by Data Processor) may audit the Data Processor to ensure that the Data Processor is in compliance with this Data Processing Agreement. The Data Processor shall provide Data Controller access to the relevant Data Processor personnel and records. Data Processor shall notify Data Controller immediately if Data Processor becomes aware that an instruction for the Processing of Personal Data given by Data Controller infringes any applicable Data Protection Laws.

4.7. It is the understanding of the Parties that Processor is a "service provider" as defined under CCPA with respect to the Customer Data. Except for usage of Personal Data as necessary to bring and defend claims, to comply with requirements of the legal process, to cooperate with regulatory authorities, and to exercise other similar permissible uses as expressly provided under applicable Data Protection Laws, Data Processor shall not retain, use, sell or disclose the Personal Data (that is not de-identified) for any purpose, including other commercial purposes, outside of the direct business relationship with Data Controller.

5. International Data Transfers

5.1. By the Effective Date of this Data Processing Agreement, the Data Controller acknowledges that it will carry out EU Personal Data transfers to the following country/ies: United States of America.

5.2. Data Processor hereby agrees to comply with the obligations of a data importer as set out in the EU Commission's "Controller-to-Processor Standard Contractual Clauses" for the transfer of EU Personal Data to processors established in third countries, attached in Annex 1 hereto, and acknowledges that Data Controller will be a data exporter under such clauses.

5.3. Data Processor agrees that its obligations under the Standard Contractual Clauses shall be governed by the law of the Main Establishment of the Data Controller.

5.4. The Parties agree that they will provide additional information about the transfer and will co-operate, without delay, where this is required by a Supervisory Authority in any EEA Member State, the United Kingdom, and/or Switzerland. In the event that a Supervisory Authority revokes or adapts the decision that it made approving the Standard Contractual Clauses, then Data Controller shall have the right forthwith to require Data Processor to cease to process Personal Data outside the EEA, the United Kingdom, or Switzerland, or, if Data Processor is unable to do this, to terminate the Campaign(s).

5.5. With respect to the Processing of EU Person Data, Data Controller grants a general authorization to Data Processor to appoint its affiliates as Sub-processors, and a specific authorization to Data Processor and its affiliates to appoint as Sub-processors the entities set out in Annex 2 attached hereto, and for the sub-processing activities described thereon, as it may be updated from time to time. In the case of general written authorization, Data Processor shall inform Data Controller of any intended changes concerning the addition or replacement of other Sub-processors, thereby giving Data Controller the opportunity to object to such changes. The Data Processor shall be fully liable for the acts and omissions of its Sub-processors' Processing of EU Personal Data to the same extent the Data Processor would be liable if performing the services of each Sub-processor directly under the terms of this Data Processing Agreement.

6. Security Measures

6.1. The Data Processor shall implement and adhere to appropriate technical and organizational measures in order to protect Personal Data, in particular where the processing involves the transmission of data over a network. These measures shall include the requirements established under applicable Data Protection Laws.

Therefore, the Data Processor agrees to undertake appropriate technical and organizational measures with the following purposes:

- (i) protect the Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, alteration, or disclosure;
- (ii) ensure, to the extent within the Data Processor's control and not that of the Data Controller, that Personal Data cannot be read, copied, modified, or removed without authorization during electronic transmission, transport, or storage and that it is possible to examine, control, and establish to which parties the transfer of Personal Data by means of data transmission facilities is envisaged (transmission control); and
- (iii) ensure that it is possible to retrospectively examine, control, and establish whether and by whom Personal Data has been introduced into data processing systems, including any modifications or removal (input control).

6.2. These measures shall be appropriate to the harm which might result from any unauthorized or unlawful processing, accidental loss, destruction, damage, or theft of the Personal Data and having regard to the nature of the Personal Data which is to be protected.

As a minimum, these measures should include, but not be limited to:

- (i) encrypting sensitive and other Personal Data in transit (but solely to the extent such transit is initiated by the Data Processor as opposed to the Data Controller and it being understood and agreed by the Data Controller that the scope of the Main Agreement does not require or address the processing of any sensitive data, which the Data Controller should not transmit to the Data Processor without the Data Processor's express written consent);
- (ii) ensuring least privileged access rights on systems containing Data Controller sensitive and other Personal Data;
- (iii) regularly reviewing access permissions to Data Controller's Personal Data;
- (iv) ensuring the use of complex passwords or two-factor authentication when used;
- (v) ensuring proper physical access controls to all systems containing Data Controller Personal Data; and
- (vi) ensuring proper disposal of any sensitive and other Personal Data, in print or electronic media, properly patching systems containing Data Controller's Personal Data, and ensuring an up-to-date antivirus application is installed on all systems processing and/or containing Data Controller's Personal Data.

7. Data Breaches

7.1. Data Processor shall notify Data Controller promptly and in writing if it becomes aware of any actual or potential Personal Data Breach on Data Processor's equipment or in Data Processor's facilities, or sub-processors' if any.

In particular, the Data Processor must notify Data Controller immediately in writing in the event that the property of Data Controller or its Personal Data in the possession or control of the Data Processor is endangered by measures undertaken by third parties.

7.2. Immediately after notification, the Data Processor will:

- (i) investigate the Personal Data Breach and provide the Data Controller with a detailed description of the Personal Data Breach, the type of data and other Personal Data that was the subject of the Personal Data Breach and the identity of each affected person, as soon as such information can be collected or otherwise becomes available (as well as periodic updates to this information and any other information Data Controller may reasonably request relating to the Personal Data Breach);
- (ii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Personal Data Breach; and
- (iii) provide its full assistance and support to Data Controller in the event that Data Controller determines that it is necessary to notify Data Subjects or concerned Supervisory Authority of such Personal Data Breach.

8. Sub-processors

8.1. The Data Processor may engage third-party Sub-processors, subject to this Section 8. Any such Sub-processor will process Personal Data only to deliver the Campaign and will be prohibited from using Personal Data for any other purpose.

8.2. The Data Processor must ensure the reliability and competence of its subcontractors and shall agree with its subcontractors to protect and process the Personal Data under terms and conditions no less restrictive than those contained in this Data Processing Agreement.

9. Term and Termination

9.1. This Data Processing Agreement shall enter into effect on the Effective Date and its term shall be coextensive with the term of the Main Agreement. The obligations under Section 4.4 shall survive any termination or expiration of the Main Agreement. Any other obligation, excepting those that reasonably or under any applicable laws have to survive a termination or expiration of the Main Agreement, shall terminate upon termination or expiration of the Main Agreement.

9.2. The Data Controller shall deem any breach of this Data Processing Agreement as a breach of the Main Agreement and thus the same provisions for the termination of this Data Processing Agreement shall be applicable.

10. Miscellaneous

10.1 This Data Processing Agreement is intended to ensure the adequate level of protection of Personal Data and does not otherwise affect the rights and obligations under any other agreements between the Parties.

10.2. Nothing in this Data Processing Agreement shall be construed as an exclusion of any laws, regulations, or rules pertaining to protection of Personal Data or export regulations that may be applicable to the Campaigns provided by the Data Processor under the Main Agreement and that must be observed by Data Processor.

10.3. If any term or provision of this Data Processing Agreement shall be held to be illegal or unenforceable in whole or in part, the validity of the remaining provisions and of this Data Processing Agreement itself shall remain unaffected. The same shall apply in the event that this Data Processing Agreement is incomplete.

11. Applicable Law

This Data Processing Agreement and any contractual obligations arising out of or in relation to it shall be governed by the national law of the Main Establishment of the Data Controller.

**Annex 1
Model Clauses**

**Commission Decision C(2010)593
Standard Contractual Clauses (processors)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: The other party to the Main Agreement with Metadata, Inc.

Address: As specified in the Main Agreement

Tel.: As specified in the Main Agreement; e-mail: As specified in the Main Agreement

.....
(the data **exporter**)

and

Name of the data importing organisation: Metadata, Inc.

Address: 880 Harrison St. Suite 303C, San Francisco, CA 94107 (USA)

Other information needed to identify the organisation:

.....
(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) *'the data exporter'* means the controller who transfers the personal data;
- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the

data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

An entity that has licensed from data importer, subject to the Main Agreement (defined above) certain offerings, a portion of which includes the Campaigns (defined above).

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

An owner and operator of a platform that provides Campaigns on behalf of its customers.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Contact persons for Data Controller's customers and/or prospective customers.

Categories of data

The personal data transferred concern the following categories of data (please specify):

Contact details, including first and last name, email address, and employer's company name.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

N/A

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The processes may include storage, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available data exporter's data as necessary to provide the Campaigns in accordance with the Main Agreement, including related internal purposes (such as quality control, troubleshooting, product development, and creation of augmented customer audiences).



APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer will maintain reasonable administrative, physical, and technical safeguards for the protection of the security, confidentiality, and integrity of personal data transferred to data importer, including, without limitation those specified in Section 6 of the Data Processing Agreement to which this Appendix 2 to the Standard Contractual Clauses is affixed.

Annex 2
Data Processors' Sub-Processors

Sub-processor name	Permitted sub-processing activities
Zoom Information Inc.	Data Enrichment
InsideView Technologies, Inc.	Data Enrichment
LiveRamp Holdings, Inc.	Data Enrichment
Throttle, Inc.	Data Enrichment
CloudFactory Limited	Data Enrichment
People Data Labs, Inc.	Data Enrichment
Google Display Network	Advertising Channel
The Trade Desk, Inc.	Advertising Channel
LinkedIn Corporation	Advertising Channel
Facebook, Inc.	Advertising Channel
Amazon Web Services, Inc.	Web and Database Hosting
DigitalOcean, Inc.	Web and Database Hosting