DATA TRANSFER AGREEMENT – SUPPLEMENTARY DATA

This Data Transfer Agreement is effective by and between:

Metadata, Inc., a company incorporated under the laws of the State of Delaware, USA, having its principal place of business at 11001 W. 120th Avenue, Suite 440, Broomfield, CO 80021 (USA) ("**Metadata**");

and

The other party to the Main Agreement, as defined below, with Metadata (the "**Customer**").

Metadata and Customer are also individually referred to herein as a "**Party**" and collectively as the "**Parties**".

RECITALS

I. Metadata and Customer agreed to an Order and the Terms of Use Agreement incorporated therein (the "**Main Agreement**");

II. This Data Transfer Agreement supplements the Main Agreement solely with respect to the provision of Supplementary Data, as defined below, by Metadata to Customer under the Main Agreement.

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

NOW, THEREFORE, THE PARTIES AGREE AS FOLLOWS:

1. Definitions

"**CCPA**" means the California Consumer Privacy Act.
"**Company Services**" has the meaning ascribed to it in the Main Agreement.
"**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 on which the Main Agreement between the Parties became effective.
"**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.
"**Main Agreement**'' means the Order, and the Terms of Use Agreement incorporated therein, as well as any amendments or add-on Orders, between Metadata and Customer, which includes but is not limited to the provision of the Supplementary Data.
"**Personal Data**" means any information relating to an identified or identifiable natural person contained in the Supplementary 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 Customer has received from Metadata on or after the Effective Date 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 Data Protection Law(s) governing the particular circumstances.
"**Process**" or "**Processing**" or "**Processed**" 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, blocking, erasure or destruction.
"**Supervisory Authority**" has the meaning set forth under the GDPR.

"**Supplementary Data**" means data points that augment Customer Data (as defined in the Main Agreement), or other data points for prospects that are similar to the customers contained in the Customer Data, but, for the avoidance of doubt, excluding Customer Data.

2. **Processing Personal Data**. The Parties acknowledge that in connection with the Main Agreement, Metadata may provide or make available to Customer Supplementary Data that may contain Personal Data. Customer shall Process such data: (i) for the purposes described in the Main Agreement; and/or (ii) as may otherwise be permitted under applicable Data Protection Law(s). Each Party will Process the copy of the Personal Data in its possession or control as an independent controller (not as a joint controller with the other Party).

3. **International Transfers**. Where the Data Protection Law(s) of the EU, United Kingdom, and/or Switzerland apply to the EU Personal Data, neither Party shall Process any EU Personal Data (nor permit any EU Personal Data to be Processed) in a territory outside of the EU, United Kingdom, and/or Switzerland (as applicable) unless it has taken such measures as are necessary to ensure the transfer complies with applicable Data Protection Laws in the EU, United Kingdom, and/or Switzerland (as applicable). To the extent Metadata transfers EU Personal Data to Customer, Customer agrees to comply with the obligations of data importer as set out in the EU Commission's "Controller-to-Controller Standard Contractual Clauses" for the transfer of EU Personal Data to controllers established in third countries, attached in Annex 1 hereto, ("**Standard Contractual Clauses**") and acknowledges that Metadata will be a data exporter under such clauses. 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 Metadata shall have the right forthwith to require Customer to cease to Process EU Personal Data outside the EEA, the United Kingdom, or Switzerland (as applicable), or, if Customer is unable to do this, to terminate provision of the applicable EU Personal Data.

4. **Compliance with Data Protection Law(s).**

4.1. Each Party shall separately comply with its obligations under applicable Data Protection Law(s) and this Data Transfer Agreement when Processing Personal Data. Neither Party shall be responsible for the other Party's compliance with applicable Data Protection Law(s). In particular, each Party shall be individually responsible for ensuring that its Processing of the Personal Data is lawful, fair, and transparent, and shall make available to Data Subjects a privacy statement that fulfils the requirements of applicable Data Protection Law(s).

4.2. Customer shall implement and maintain all appropriate technical and organizational measures to protect any copies of the Supplementary Data in its possession or control from (i) accidental or unlawful destruction, and (ii) loss, alteration, or unauthorized disclosure or access and to preserve the security and confidentiality of such Supplementary Data. Notwithstanding the generality of the foregoing, Customer shall: (a) employ reasonable administrative, physical, and technical safeguards (including commercially reasonable safeguards against worms, Trojan horses, and other disabling or damaging codes) to afford protection of the Supplementary Data in accordance with applicable Data Protection Law(s) as would be appropriate based on the nature of the Supplementary Data; and (b) utilize its best efforts to keep the Supplementary Data reasonably secure and in an encrypted form, and use industry standard security practices and systems applicable to the use of Personal Data to prevent, and take prompt and proper remedial action against, unauthorized access, copying, modification, storage, reproduction, display, or distribution of Personal Data.

4.3. Each Party will promptly, without undue delay, after becoming aware of a Personal Data Breach (a) notify the other Party of the Personal Data Breach; (b) investigate the Personal Data Breach; (c) provide the other Party with details about the Personal Data Breach; and (d) take reasonable actions to prevent a recurrence of the Personal Data Breach. The Parties agree to cooperate together in the handling of the matter by: (i) providing reasonable assistance in the investigation of the Personal Data Breach; and (ii) making available relevant records, logs, files, data reporting, and other materials related to the Personal Data Breach's effects, as may be required to comply with applicable Data Protection Law(s).

5. **Term and Termination**

5.1. This Data Transfer 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 4.2 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.

5.2. Metadata shall deem any breach of this Data Transfer Agreement as a breach of the Main Agreement and thus the same provisions for the termination of this Data Transfer Agreement shall be applicable.

6. Miscellaneous

6.1. This Data Transfer 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.

6.2. Nothing in this Data Transfer 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 Company Services provided by Metadata under the Main Agreement and that must be observed by the Parties.

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

6.4. This Data Transfer Agreement and any contractual obligations arising out of or in relation to it shall be governed by the law set forth in the Main Agreement.

6.5. In the event of any conflict or inconsistency between this Data Transfer Agreement and applicable Data Protection Law(s), the applicable Data Protection Law(s) shall prevail. In the event of any conflict or inconsistency between the terms of this Data Transfer Agreement and the terms of the Main Agreement, the terms of this Data Transfer Agreement shall prevail solely to the extent that the subject matter concerns the Processing of Personal Data contained in Supplementary Data.

6.6. To the extent that it is determined by any Supervisory Authority that the Main Agreement or this Data Transfer Agreement is insufficient to comply with the applicable Data Protection Law(s), or to the extent required otherwise by any changes in the applicable Data Protection Law(s), Metadata and Customer agree to cooperate in good faith to amend the Main Agreement or this Data Transfer Agreement or enter into further mutually agreeable data processing agreements in an effort to comply with applicable Data Protection Law(s).

Annex 1
STANDARD CONTRACTUAL CLAUSES
Controller to Controller

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.5 (e) and Clause 8.9(b);

(iii) N/A

(iv) Clause 12(a) and (d);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

N/A

Clause 10

Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory

authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

  (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

  (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

  (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

  (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

  (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal

data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland (*specify Member State*).

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Republic of Ireland (*specify Member State*).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: Metadata, Inc.
Address: 11001 W. 120th Avenue, Suite 440, Broomfield, CO 80021 (USA)
Contact person's name, position and contact details: privacy@metadata.io

Activities relevant to the data transferred under these Clauses:

Activities relevant to the data transferred under these clauses may include data importer's direct online adverstising to prospective customers and current or former customers, for the purposes of learning more about data importer's products and/or services.

Signature and date: See Main Agreement
Role (controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: See Main Agreement ("Customer")
Address: See Main Agreement
Contact person's name, position and contact details: See Main Agreement

Activities relevant to the data transferred under these Clauses:

Activities relevant to the data transferred under these clauses may include data importer's direct online adverstising to prospective customers and current or former customers, for the purposes of learning more about data importer's products and/or services.

Signature and date: See Main Agreement
Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Prospective customers and current or former customers of products and services provided by data importer.

Categories of personal data transferred

Contact Information for prospective customers and current or former customers, which may include:

- First and Last Name (or first initial of one or both)
- Email Address(es)
- Employer
- Title
- Telephone Number(s)
- Employer Address
- LinkedIn Profile URL
- Professional life data
- Personal Data transferred may also include information about the computer or other electronic device through which an individual may access websites, advertisements or other user interface including: usage information and statistics, IP address, personal device type and model, browser type, personal device ID, domain names, access times, referring website addresses, personal device settings and history and geolocation 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).

One-off basis, but potentially refreshed on command

Nature of the processing

Processing may include data importer's direct online adverstising to prospective customers and current or former customers, for the purposes of learning more about data importer's products and/or services.

Purpose(s) of the data transfer and further processing

So that data importer may internally analyze the effectiveness of data importer's online advertising, such as lead scoring, lead-to-account matching, and lead routing.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Criteria used to determine retention periods include the status of fulfillment of the purpose of the data transfer and further processing, as specified above, the data retention periods specified in each Party's disaster recovery plan and/or business continuity plan, and data subject request.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

N/A

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The Republic of Ireland

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Security Measures
Data Importer shall implement and maintain appropriate technical and organizational security measures that are designed to protect Supplementary Data from Security Incidents and designed to preserve the security and confidentiality of Supplementary Data.

Security Organizational Structure
Information Security responsibility and authority shall be delegated by Data Importer to an appropriate senior-level officer or employee.

Information Classification and Sensitivity
Data Importer will properly classify all information, based on whether it is public or confidential, and, within confidential information, will further classify such information on a continuum that reflects the sensitivity of such information. All information should be protected in a manner reflective of its classification.

Personal Data Encryption
Confidential information will be encrypted while transmitted over external networks using TLS1.2 or above with minimum key length of 128bit. Encryption algorithms and technologies in use shall be publicly validated and subject to the acceptable industry standards (e.g., AES, RSA). The key length requirements shall be reviewed regularly and upgraded as technology improves and based on a risk analysis process. Authentication related information (e.g., passwords) must not be stored in clear text. The use of a one-way hash (minimum standard is SHA2) + salt function to irreversibly encrypt such data will be used.

Access Control
Data Importer will employ role-based access control.

Security Review and Testing
Data Importer will review all policies and practices at least once per year and conducted appropriate testing at regular intervals.

Data Storage and Deletion
Wherever possible, data will be stored electronically, restricted to authorized users only, and as secure as practically possible to protect from misuse or loss. The data will be stored while taking into consideration the period of retention required and the frequency with which access will be made to the record. The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded, and due regard to security will also be given to archived filing. Data and records should not be kept for longer than is necessary. All information of a confidential or sensitive nature on paper or electronic media will be securely destroyed when it is no longer required.

Physical Security
The physical security of Data Importer’s offices and data centers will be maintained as part of Data Importer’s overall security level requirements. Data Importer's employees, contractors, and subcontractors will be subject to Data Importer’s physical security requirements.

Information Logging
Logging from critical systems, applications, and services can provide key information and potential indicators of compromise. Although logging information may not be viewed on a daily basis, it is critical to have from a forensics standpoint. Accordingly, Data Importer will apply logging principles to Data Importer’s network(s).

Disaster Recovery
Data Importer will maintain a written disaster recovery plan to mitigate the effects of a disaster.