DATA PROCESSING AGREEMENT – CUSTOMER DATA

This Data Processing 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) (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 in connection with the Company Services (as defined below), Data Processor may Process Personal Data contained in Customer Data on behalf of Data Controller.

III. The Parties agree to comply with the following provisions with respect to any Personal Data transferred to Data Processor in Customer 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.
"**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 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 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 Data Controller and Data Processor, which includes but is not limited to the provision of the Customer Data.
"**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 Data Processor has received from 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 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.
"**Sub-processor**" means any processor engaged by Data Processor or by any other Sub-processor of Data Processor who receives Personal Data exclusively intended for Processing activities to be carried out on behalf of Data Controller in connection with the Company Services.
"**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, title, phone number, 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 and those of Data Controller's employees and/or contractors and/or agents involved in receiving the Company Services

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

Providing the Company Services to Data Controller

3. Obligations of Data Controller

3.1. In accordance with the applicable Data Protection Law(s), 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 as required by applicable Data Protection Law(s) and (ii) that their Personal Data will be Processed outside of the European Economic Area, the United Kingdom, Switzerland, as required by applicable Data Protection Law(s).

3.3. Data Controller shall without undue delay notify Data Processor in writing (email insufficient) at the address specified above when it discovers errors or irregularities in the Processing of Personal Data in accordance with applicable Data Protection Law(s).

3.4. Data Controller shall respond in a reasonable time to enquiries from any Supervisory Authority regarding the processing of relevant Personal Data by Data Controller. If any Party is required under applicable Data Protection Law(s) 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 Data Processor

4.1. In providing the Company Services, Data Processor shall comply with the instructions of Data Controller for the Processing of Personal Data and Process the Personal Data exclusively in connection with the provision of the Company Services. The provisions of this Data Processing Agreement are the main source of instructions issued by 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 Law(s), 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 Law(s).

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

Data Processor shall inform Data Controller without delay 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) Data Processor shall store the Personal Data as long as it is needed for the provision of the Company Services and in accordance with applicable Data Protection Law(s).
(ii) Data Processor must store the Personal Data, together with any copies or reproductions made of such Personal Data, with reasonable care and 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 Law(s).
(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 Law(s), 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 Law(s).
(iii) To the extent that Data Controller does not have the ability to correct, amend, block, or delete already transferred Personal Data, Data Processor shall comply with any reasonable request by Data Controller to facilitate such actions as required by Data Protection Law(s).
(iv) If Data Processor becomes aware of any errors or incorrectness of Personal Data, Data Processor shall notify Data Controller prior to correcting such data. Whenever a situation arises where this may be appropriate and in line with applicable Data Protection Law(s), 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 Data Processor to ensure that Data Processor is in compliance with this Data Processing Agreement. Data Processor shall provide Data Controller access to the relevant Data Processor personnel and records. Data Processor shall notify Data Controller without delay if Data Processor becomes aware that an instruction for the Processing of Personal Data given by Data Controller violates any applicable Data Protection Law(s).

4.7. To the extent that Data Controller is a "business" as defined under the CCPA, 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 Law(s), 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, 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, ("**Standard Contractual Clauses**") and acknowledges that Data Controller will be a data exporter under such clauses.

5.3. 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 EU Personal Data outside the EEA, the United Kingdom, or Switzerland, or, if Data Processor is unable to do this, to terminate the Processing of EU Personal Data.

5.4. With respect to the Processing of EU Personal Data, Data Controller grants authorization to Data Processor to appoint as Sub-processors the entities set out in Annex III attached hereto, and for the sub-processing activities described therein, as it may be updated from time to time. Data Processor shall provide Data Controller thirty (30) days' notice (email or message through Company Services sufficient) of any intended changes concerning the addition or replacement of other Sub-processors, thereby giving Data Controller the opportunity to object to such changes. Data Processor shall be fully liable for the acts and omissions of its Sub-processors' Processing of EU Personal Data to the same extent 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. 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 Law(s).

Therefore, 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 Data Processor's control and not that of 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.

At 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 Data Processor as opposed to Data Controller and it being understood and agreed by Data Controller that the scope of the Main Agreement does not require or address the Processing of any sensitive data, which Data Controller should not transmit to Data Processor without 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, 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 Data Processor is endangered by measures undertaken by third parties.

7.2. Immediately after notification, Data Processor will:

(i) investigate the Personal Data Breach and provide 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 any concerned Supervisory Authority of such Personal Data Breach.

8. Sub-processors

8.1. Data Processor may engage third-party Sub-processors, subject to this Section 8. Any such Sub-processor will Process Personal Data only in connection with Data Processor's provision of the Company Services and will be prohibited from using Personal Data for any other purpose.

8.2. Data Processor must ensure the reliability and competence of its Sub-processors and shall agree with its Sub-processors 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. 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 Company Services provided by Data Processor under the Main Agreement and that must be observed by the Parties.

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 of this Data Processing Agreement shall remain unaffected. The same shall apply in the event that this Data Processing Agreement is incomplete.

Annex 1
STANDARD CONTRACTUAL CLAUSES
Controller to Processor

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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

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

(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 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 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, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the 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. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 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 data, including protection against a breach of security

leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties 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 subjects. 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. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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 breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 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 and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed 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') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer 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 Regulation of (EU) 2016/679 with respect to the processing in question;

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there

are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

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) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) 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 and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) 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.

(f) The Parties agree that if one Party is held liable under paragraph (e), 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.

(g) The data importer may not invoke the conduct of a 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 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: 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 storage, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available data exporter's data as necessary to provide the Company Services in accordance with the Main Agreement, including related internal purposes (such as quality control, troubleshooting, product development, and creation of augmented customer audiences).

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

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

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Contact persons for Data Controller's customers and/or prospective customers and those of Data Controller's employees and/or contractors and/or agents involved in receiving the Company Services.

Categories of personal data transferred

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

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

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

Continuous basis, through term of Main Agreement

Nature of the processing

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

Purpose(s) of the data transfer and further processing

To provide the Company Services, as described in the Main Agreement and this Data Protection Agreement.

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 processing, as specified above, the data retention periods specified in each Party's disaster recovery plan and/or business continuity plan, the term of the Main Agreement, and data subject request.

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

See Annex III and above descriptions regarding duration of processing.

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

Security Organizational Structure
Information Security responsibility and authority is delegated by Data Processor to its Chief Security Officer (CSO). Along with the CSO, a Security Steering Committee will act as an advisory board and a channel to communicate security issues from and to the CSO.

Information Classification and Sensitivity
Data Processor categorizes all information into two main classifications: Public and Confidential.
Within the classification of Confidential information, there is a continuum, in that it is understood that some information is more sensitive than other information and should be protected in a more secure manner.

Personal Data Encryption
Confidential information will be encrypted while transmitted over external networks using TLS1.2 or above with minimum key length of 128bit. All network communication channels between Data Processor's offices and the production network Data Processor utilizes will be established through an encrypted tunnel (Site to Site VPN). Encryption algorithms and technologies in use shall be publicly validated and subject to the acceptable industry standards (e.g., AES, RSA). Confidential data stored within Data Processor's database servers will be encrypted with AES encryption as a minimum standard for customers who require encryption for data at rest. Minimum key length is 192bit; the key length requirements shall be reviewed annually and upgraded as technology improves and based on the risk analysis process and Data Processor's product and security priorities. 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 is required.

Access Control
Data Processor employs role-based access control. Access to Data Processor's information assets is restricted and will be granted to Data Processor's employees and contractors to fulfill their duties on a need-to-use basis. Data Processor employees and contractors will not be granted access to any information asset that is not directly needed in regards to their work, in line with the principles of least privilege.

Security Review and Testing
Data Processor shall review all policies and practices at least once per year. Data Processor shall have third-party vulnerability scans conducted monthly and shall commission a third-party penetration report at least once per year.

Data Storage and Deletion
Wherever possible, data is 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 must 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 must be securely destroyed when it is no longer required. Deletion should ultimately mean the complete destruction of the electronic record. This implies rendering data non-recoverable even when using forensic data recovery techniques.

Physical Security
The physical security of Data Processor's corporate offices and data centers is maintained as part of Data Processor's overall security level requirements. Data Processor's employees and subcontractors are subject to Data Processor's physical security requirements, set out in Data Processor's "Data Center Management" procedure.

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 Processor applies logging principles to Data Processor's network(s).

Disaster Recovery
Data Processor maintains a written disaster recovery plan to mitigate the effects of a disaster. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available. Data Processor's disaster recovery team tracks changes to personnel, hardware, software, vendors, or any other item documented in the plan in an effort to keep this document current and relevant.

ANNEX III

LIST OF SUB-PROCESSORS

Name	Address	Contact	Description of Processing
Amazon	https://aws.amazon.com	https://aws.amazon.com/contact-us/	Hosting
Atlassian	https://www.atlassian.com	https://support.atlassian.com	Project and Issue Tracking; Document Collaboration
Google	https://cloud.google.com	https://cloud.google.com/support/	Email and Workspace Platform
Slack	https://slack.com/	https:/slack.com/help/requests/new	Communications
DigitalOcean	https://www.digitalocean.com/	https://www.digitalocean.com/company/contact/	Hosting
Knowi	https://www.knowi.com	https://www.knowi.com	Business Intelligence
The Trade Desk	https://www.thetradedesk.com/	https://www.thetradedesk.com/company/contact-us	Advertising Channel
Databricks	https://databricks.com	https://databricks.com/company/contact	Data Warehousing and Optimization and Analytics
Xoor	https://xoor.io/us/en	https://xoor.io/us/en/contact-us	Company Services Support
Epic Software Development	https://www.epicsoftwaredev.com/	https://www.epicsoftwaredev.com/contact-us/	Company Services Support
Cloud Factory	https://www.cloudfactory.com	https://cloudfactory.com/contact	Data Enrichment
Zendesk	https://www.zendesk.com	https://www.zendesk.com/contact	Customer Support Platform