

DATA TRANSFER AGREEMENT – SUPPLEMENTARY DATA

This Data Transfer Agreement is signed by and between:

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

and

the other party to the Main Agreement with Metadata, as defined below (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 Campaigns (as defined below).

NOW, THEREFORE, THE PARTIES AGREE AS FOLLOWS:

1. Definitions. For the purpose of this Data Transfer Agreement, these terms shall mean the following:

“**Applicable Laws**” shall mean all applicable federal, state and foreign data protection, privacy and data security laws, as well as applicable regulations and formal directives intended by their nature to have the force of law, including, without limitation, the EU Data Protection Laws and the California Consumer Privacy Act (“**CCPA**”) but excluding, without limitation, consent decrees.

“**Authorized Personnel**” means (a) Customer’s employees who have a need to know or otherwise access Personal Data for the purposes of implementing advertising campaigns on behalf of Customer; and (b) Customer’s contractors, agents, and auditors who have a need to know or otherwise access Personal Data under this Data Transfer Agreement, and who are bound in writing by confidentiality and other obligations sufficient to protect Personal Data in accordance with the terms and conditions of this Data Transfer Agreement.

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

“**EU Data Protection Laws**” means all applicable laws relating to the Processing of EU Personal Data, including, where applicable, guidance and codes of practice issued by the applicable supervisory authorities, and including, 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 GDPR).

“**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.

“**GDPR**” means the General Data Protection Regulation (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).

“**Personal Data**” means any data relating to an identified or identifiable person that is contained in the Supplementary Data, when such data is protected as “personal data” or “personally identifiable information” or a similar term under Applicable Laws.

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

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

“**Standard Contractual Clauses (Controller-Controller)**” means the model clauses for the transfer of personal data from the European Union to third countries (controller to controller transfers) as approved by the European

Commission and available at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0915> (as amended, superseded or updated from time to time) and as set forth on Schedule 1 attached hereto.

“**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 Laws. 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 in Compliance with EU Data Protection Laws. Where EU Data Protection Laws 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 unless it has taken such measures as are necessary to ensure the transfer is in compliance with applicable EU Data Protection Laws. To the extent Metadata transfers EU Personal Data to Customer, Customer agrees to abide by and process such EU Personal Data as the “data importer” in accordance with the Standard Contractual Clauses (Controller-Controller). Metadata agrees to abide by and process such EU Personal Data as the “data exporter” in accordance with the Standard Contractual Clauses (Controller-Controller). The terms of the Standard Contractual Clauses (Controller-Controller), together with Annex B set out in Schedule 1 to this Data Transfer Agreement, are incorporated in this Data Transfer Agreement by this reference solely as required with respect to EU Personal Data transferred as part of the Supplementary Data. In the event any defined term in the Standard Contractual Clauses (Controller-Controller) is in conflict with a definition in Section 1 of this Data Transfer Agreement, the definitions in the Standard Contractual Clauses (Controller-Controller) shall control solely with respect to (i) the provisions in such Clauses and (ii) EU Personal Data.

4. Compliance with Data Protection Laws.

4.1. Each Party shall separately comply with its obligations under Applicable Laws and this Data Transfer Agreement when processing Personal Data. Neither Party shall be responsible for the other Party's compliance with Applicable Laws. 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 Laws.

4.2. Customer shall implement and maintain all appropriate technical and organizational measures to protect any copies of the Personal 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 Personal 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 Personal Data in accordance with Applicable Laws as would be appropriate based on the nature of the Personal Data; and (b) utilize its best efforts to keep the Personal Data reasonably secure and in an encrypted form, and use industry standard security practices and systems applicable to the use of Personal Data (such as ISO 27001) to prevent, and take prompt and proper remedial action against unauthorized access, copying, modification, storage, reproduction, display or distribution of Personal Data.

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

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 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.

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 advertising campaigns provided by Metadata under the Main Agreement and that must be observed by Customer.

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 Law, Applicable Law shall prevail. In the event of any conflict or inconsistency between the terms of this Data Transfer Agreement Data Transfer Agreement and the terms of the 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 data protection authority that the Agreement or this Data Transfer Agreement is insufficient to comply with the applicable Data Protection Laws, or to the extent required otherwise by any changes in the applicable data protection laws, Metadata and Customer agree to cooperate in good faith to amend the Agreement or this Data Transfer Agreement or enter into further mutually agreeable data processing agreements in an effort to comply with Applicable Laws.

SCHEDULE 1

STANDARD CONTRACTUAL CLAUSES – DATA CONTROLLER TO DATA CONTROLLER

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

and

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

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

RECITALS

I. Pursuant to the Main Agreement and for the provision of, and solely for the provision of, Supplementary Data, the Data Exporter may transfer Personal Data to the Data Importer.

II. Data Exporter and Data Importer agree to comply with the following Clauses with respect to any Personal Data transferred by the Data Exporter to the Data Importer in Supplementary Data.

III. The details of the transfer (as well as the Personal Data covered) are specified in *Annex B*, which forms an integral part of the Clauses.

NOW, THEREFORE, THE PARTIES AGREE AS FOLLOWS:

1. DEFINITIONS

For the purposes of the Clauses:

- (a) “**Personal Data**”, “**Special Categories of Data**”/“**Sensitive Data**”, “**Process**”/“**Processing**”, “**Controller**”, “**Processor**”, “**Data Subject**” and “**Supervisory Authority**”/“**Authority**” (whereby the **Authority** shall mean the competent data protection Authority in the territory in which the Data Exporter is established) shall have the same meaning as defined in the Data Protection Law(s).
- (b) “**Data Exporter**” means the Controller who transfers Personal Data.
- (c) “**Data Importer**” means the Controller who agrees to receive Personal Data from the Data Exporter for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection.
- (d) “**Clauses**” means these contractual Clauses, which are a free-standing document that does not incorporate commercial business terms established by the Parties under the Main Agreement or any other separate commercial arrangements.
- (e) “**Data Protection Law(s)**” means all applicable laws relating to the Processing of Personal Data, including, where applicable, guidance and codes of practice issued by the Supervisory Authorities, and including, 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**”).

2. OBLIGATIONS OF THE DATA EXPORTER

The Data Exporter warrants and undertakes that:

- (a) The Personal Data have been collected, Processed and transferred in accordance with the laws applicable to the Data Exporter.

(b) It has used reasonable efforts to determine that the Data Importer is able to satisfy its legal obligations under these Clauses.

(c) It will provide the Data Importer, when so requested, with copies of relevant Data Protection Laws or references to them (where relevant, and not including legal advice) of the country in which the Data Exporter is established.

(d) It will respond to enquiries from Data Subjects and the Authority concerning Processing of the Personal Data by the Data Importer, unless the Parties have agreed that the Data Importer will so respond, in which case the Data Exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the Data Importer is unwilling or unable to respond. Responses will be made within a reasonable time.

(e) It will make available, upon request, a copy of the Clauses to Data Subjects who are third party beneficiaries under *Clause 4*, unless the Clauses contain confidential information, in which case it may remove such information. Where information is removed, the Data Exporter shall inform Data Subjects in writing of the reason for removal and of their right to draw the removal to the attention of the Authority. However, the Data Exporter shall abide by a decision of the Authority regarding access to the full text of the Clauses by Data Subjects, as long as Data Subjects have agreed to respect the confidentiality of the confidential information removed. The Data Exporter shall also provide a copy of the Clauses to the Authority where required.

3. OBLIGATIONS OF THE DATA IMPORTER

The Data Importer warrants and undertakes that:

(a) It will have in place appropriate technical and organisational measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the Processing and the nature of the data to be protected.

(b) It will have in place procedures so that any third party it authorises to have access to the Personal Data, including Processors, will respect and maintain the confidentiality and security of the Personal Data. Any person acting under the Authority of the Data Importer, including a data Processor, shall be obligated to Process the Personal Data only on instructions from the Data Importer. This provision does not apply to persons authorised or required by law or regulation to have access to the Personal Data.

(c) It has no reason to believe, at the time of entering into these Clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these Clauses, and it will inform the Data Exporter (which will pass such notification on to the Authority where required) if it becomes aware of any such laws.

(d) It will Process the Personal Data for purposes described in *Annex B* and has the legal authority to give the warranties and fulfil the undertakings set out in these Clauses.

(e) It will identify to the Data Exporter a contact point within its organization authorized to respond to enquiries concerning Processing of the Personal Data and will cooperate in good faith with the Data Exporter, the Data Subject and the Authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the Data Exporter, or if the Parties have so agreed, the Data Importer will assume responsibility for compliance with the provisions of *Clause 2(e)*.

(f) At the request of the Data Exporter, it will provide the Data Exporter with evidence of financial resources sufficient to fulfil its responsibilities under *Clause 4* (which may include insurance coverage).

(g) Upon reasonable request of the Data Exporter, it will submit its data Processing facilities, data files and documentation needed for Processing to reviewing, auditing and/or certifying by the Data Exporter (or any independent or impartial inspection agents or auditors, selected by the Data Exporter and not reasonably objected to by the Data Importer) to ascertain compliance with the warranties and undertakings in these Clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or Supervisory Authority within the country of the Data Importer, which consent or approval the Data Importer will attempt to obtain in a timely fashion.

- (h) It will Process the Personal Data in accordance with the data Processing principles set forth in *Annex A*.
- (i) It will not disclose or transfer the Personal Data to a third party data Controller located outside the European Economic Area (EEA) unless it notifies the Data Exporter about the transfer and
 - (i) the third party data Controller Processes the Personal Data in accordance with a Commission decision finding that a third country provides adequate protection, or
 - (ii) the third party data Controller becomes a signatory to these Clauses or another data transfer agreement approved by a competent Authority in the EU, or
 - (iii) Data Subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or
 - (iv) with regard to onward transfers of Sensitive Data, Data Subjects have given their unambiguous consent to the onward transfer.

4. LIABILITY AND THIRD-PARTY RIGHTS

(a) Each Party shall be liable to the other Parties for damages it causes by any breach of these Clauses. Liability as between the Parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a Party for its outrageous conduct) are specifically excluded. Each Party shall be liable to Data Subjects for damages it causes by any breach of third party rights under these Clauses. This does not affect the liability of the Data Exporter under its Data Protection Law.

(b) The Parties agree that a Data Subject shall have the right to enforce as a third party beneficiary this Clause and *Clause 2(b)*, *Clause 2(d)*, *Clause 2(e)*, *Clause 3(a)*, *Clause 3(c)*, *Clause 3(d)*, *Clause 3(e)*, *Clause 3(h)*, *Clause 3(j)*, *Clause 4(a)*, *Clause 6*, *Clause 7(d)* and *Clause 8* against the Data Importer or the Data Exporter, for their respective breach of their contractual obligations, with regard to his Personal Data, and accept jurisdiction for this purpose in the Data Exporter's country of establishment. In cases involving allegations of breach by the Data Importer, the Data Subject must first request the Data Exporter to take appropriate action to enforce his rights against the Data Importer; if the Data Exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the Data Subject may then enforce his rights against the Data Importer directly. A Data Subject is entitled to proceed directly against a Data Exporter that has failed to use reasonable efforts to determine that the Data Importer is able to satisfy its legal obligations under these Clauses (the Data Exporter shall have the burden to prove that it took reasonable efforts).

5. LAW APPLICABLE TO THE CLAUSES

These Clauses shall be governed by the law of the country in which the Data Exporter is established, with the exception of the laws and regulations relating to Processing of the Personal Data by the Data Importer under *Clause 3(h)*, which shall apply only if so selected by the Data Importer under that clause.

6. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR THE AUTHORITY

(a) In the event of a dispute or claim brought by a Data Subject or the Authority concerning the Processing of the Personal Data against either or both of the Parties, the Parties will inform each other about any such disputes or claims and will cooperate with a view to settling them amicably in a timely fashion.

(b) The Parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the Authority. If they do participate in the proceedings, the Parties may elect to do so remotely (such as by telephone or other electronic means). The Parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each Party shall abide by a decision of a competent court of the Data Exporter's country of establishment or of the Authority which is final and against which no further appeal is possible.

7. TERMINATION

(a) In the event that the Data Importer is in breach of its obligations under these Clauses, then the Data Exporter may temporarily suspend the transfer of Personal Data to the Data Importer until the breach is repaired or the contract is terminated.

(b) In the event that:

(i) the transfer of Personal Data to the Data Importer has been temporarily suspended by the Data Exporter for longer than one month pursuant to *Clause 7(a)*;

(ii) compliance by the Data Importer with these Clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the Data Importer is in substantial or persistent breach of any warranties or undertakings given by it under these Clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the Data Exporter's country of establishment or of the Authority rules that there has been a breach of the Clauses by the Data Importer or the Data Exporter; or

(v) a petition is presented for the administration or winding up of the Data Importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the Data Importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the Data Exporter, without prejudice to any other rights which it may have against the Data Importer, shall be entitled to terminate these Clauses, in which case the Authority shall be informed where required. In cases covered by *Clause 7(b)(i)*, *Clause 7(b)(ii)*, or *Clause 7(b)(iv)* above, the Data Importer may also terminate these Clauses.

(c) Either Party may terminate these Clauses if

(i) any positive adequacy decision under the applicable Data Protection Law(s) (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and Processed by the Data Importer, or

(ii) the applicable Data Protection Law(s) (or any superseding text) becomes directly applicable in such country.

(d) The Parties agree that the termination of these Clauses at any time, in any circumstances and for whatever reason (except for termination under *Clause 7(c)*) does not exempt them from the obligations and/or conditions under the Clauses as regards the Processing of the Personal Data transferred.

8. VARIATION OF THESE CLAUSES

The Parties may not modify these Clauses except to update any information in *Annex B*, in which case they will inform the Authority where required. This does not preclude the Parties from adding additional commercial Clauses where required.

9. DESCRIPTION OF THE TRANSFER

The details of the transfer and of the Personal Data are specified in *Annex B*. The Parties agree that *Annex B* may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under *Clause 2(e)*. The Parties may execute additional annexes to cover additional transfers, which will be submitted to the Authority where required. *Annex B* may, in the alternative, be drafted to cover multiple transfers.

ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be Processed and subsequently used or further communicated only for purposes described in *Annex B* or subsequently authorised by the Data Subject.
2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The Personal Data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further Processed.
3. Transparency: Data Subjects must be provided with information necessary to ensure fair Processing (such as information about the purposes of Processing and about the transfer), unless such information has already been given by the Data Exporter.
4. Security and confidentiality: Technical and organisational security measures must be taken by the data Controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the Processing. Any person acting under the authority of the data Controller, including a Processor, must not Process the data except on instructions from the data Controller.
5. Rights of access, rectification, deletion and objection: As provided in the Data Protection Law(s), Data Subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the Data Exporter. Provided that the Authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the Data Importer or other organisations dealing with the Data Importer and such interests are not overridden by the interests for fundamental rights and freedoms of the Data Subject. The sources of the Personal Data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data Subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or Processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A Data Subject must also be able to object to the Processing of the Personal Data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the Data Importer, and the Data Subject may always challenge a refusal before the Authority.
6. Sensitive data: The Data Importer shall take such additional measures (e.g. relating to security) as are necessary to protect such Sensitive Data in accordance with its obligations under *Clause 3*.
7. Data used for marketing purposes: Where data are Processed for the purposes of direct marketing, effective procedures should exist allowing the Data Subject at any time to “opt-out” from having his data used for such purposes.
8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the Data Exporter or the Data Importer which produces legal effects concerning a Data Subject or significantly affects a Data Subject and which is based solely on automated Processing of Personal Data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The Data Importer shall not make any automated decisions concerning Data Subjects, except when:
 - (a) (i) such decisions are made by the Data Importer in entering into or performing a contract with the Data Subject, and
 - (ii) the Data Subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to those parties.or
 - (b) where otherwise provided by the law of the Data Exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

Data Subjects

The Personal Data transferred concern the following categories of Data Subjects:

Prospective customers and current or former customers of products and services provided by Data Importer.

Purpose of the Transfer(s)

The transfer is made for the following purposes:

So that Data Importer may direct online advertising to prospective customers and current or former customers, for the purposes of learning more about Data Importer's products and/or services

Categories of Data

The Personal Data transferred concern the following categories of data:

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
- Employer
- Title
- Telephone Number
- 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

Recipients

The Personal Data transferred may be disclosed only to the following recipients or categories of recipients:

Only those employees or contractors of Data Importer whom Data Importer assigns the task of directing or implementing targeted advertising campaigns and/or contacting prospective, current, and/or former customers or licensees on Data Importer's behalf.