Data Processing Addendum

This Data Processing Addendum ("DPA") forms part of the applicable (a) Smaato Publisher Insertion Order, (b) Mobile Advertising Service Agreement, and/or (c) other mutually executed written agreement(s) between Company (as identified in the applicable agreement(s)) and Smaato, Inc. ("Smaato") (the "Agreement"), pursuant to which Company transfers Personal Data (as defined herein) to and shares Personal Data with Smaato, as further described in the Agreement and in this DPA. The parties agree to comply with the following provisions with respect to Personal Data provided or made available by Company to Smaato.

References to the Agreement will be construed as including this DPA, and, except as modified below, the terms of the Agreement shall remain in full force and effect. Any capitalized terms not defined herein shall have the meanings given to them in the Agreement. In the event of any conflict between this DPA and the Agreement, this DPA will prevail. Reference to the Agreement includes any exhibits, work orders, SOWs, documentation, or other addenda incorporated into the Agreement.

For purposes of this DPA, and as further described below, the parties acknowledge that each party is a Data Controller of the Personal Data that it collects, Processes, or employs to deliver its services.

1.   DEFINITIONS

"Data Controller" means the entity that determines the purposes and means of the Processing of Personal Data. For purposes of this DPA, each party is a Data Controller of the Personal Data that it collects, Processes, or employs to deliver its services, absent a further amendment that sets forth circumstances in which either party is a Data Processor.

"Data Processor" means an entity that Processes Personal Data on behalf of a Data Controller.

"Data Protection Laws" means all applicable laws and regulations, including, without limitation, the laws and regulations of the EU applicable to the Processing of Personal Data, such as: (i) the EU General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"); (ii) the EU e-Privacy Directive (Directive 2002/58/EC), including subsequent variations, such as the Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (**"ePrivacy Regulation"**), if enacted; and (iii) any national data protection laws made under or pursuant to (i) or (ii).

"Data Subject" means the individual to whom Personal Data relates.

"Personal Data" means any information relating to an identified or identifiable person Processed pursuant to the Agreement and as to which a party is a Data Controller. The types of Personal Data and categories of Data Subjects Processed under this DPA are set forth in Annex I.B of the Standard Contractual Clauses, attached hereto.

"Processing" means any operation or set of operations that 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 ("Process", "Processes" and "Processed" shall have the same meaning).

"Security Incident" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

"**Transfer**" means the access by, transfer or delivery to, or disclosure of Personal Data to a person, entity, or system located in a country or jurisdiction other than the country or jurisdiction where the Personal Data originated from.

2. PURPOSE OF PROCESSING

2.1   Company and Smaato are parties to the Agreement, under which Company provides Personal Data (such as mobile advertising identifiers, IP addresses and/or precise location data) to Smaato. Company and Smaato each shall Transfer and Process such Personal Data only for the purposes described in the Agreement and this DPA, or as otherwise agreed in writing by the parties.

2.2   The parties agree that Smaato may Process the Personal Data for its own purposes, including to provide services for the benefit of other platforms and clients.

2.3   Neither party shall have responsibility for Processing special categories of Personal Data, as referenced in Article 9 of the GDPR. Neither party shall provide the other with any special categories of Personal Data.

3. CONTROLLER OBLIGATIONS

3.1   Each party shall comply with all applicable laws, including Data Protection Laws.

3.2   As further set forth herein, the parties agree that when either party acts as a Data Controller of Personal Data, it will fulfill all duties required of Data Controllers under Data Protection Laws, including, without limitation (as applicable), with regard to determining the legal basis or bases for their collection or Processing of Personal Data, providing sufficient notice to Data Subjects, appointing a data protection officer, managing and reporting Security Incidents, ensuring that rights of Data Subjects are honored, Transferring Personal Data, contracting with only those Data Processors that provide adequate protections for Personal Data, implementing required and appropriate contractual language in agreements with Data Processors and other Data Controllers, maintaining records of Processing, and conducting data protection impact assessments.

3.3   Each party shall have the sole obligation (as between the parties) to receive and manage Data Subject requests regarding its Personal Data, including without limitation any request to access, correct, amend, restrict Processing of, port, object to the Processing of, block, or delete Personal Data. If applicable, and to the extent legally permitted, the parties shall provide each other with reasonable cooperation and assistance in relation to handling of a Data Subject's request.

4. PRIVACY POLICY DISCLOSURES

4.1   Each party shall designate a contact point for Data Subjects in its publicly posted privacy policy.

4.2   Each party shall post a publicly accessible privacy policy on its website and in its applications that provides such information to individuals as may be required by Data Protection Laws, such as a description of types of Personal Data and a comprehensive explanation of how, and for what purpose(s), the Personal Data will be processed. In particular, the privacy policy shall reflect the nature of the relationship and sharing of data between the parties.

5. OBLIGATIONS SPECIFIC TO OBTAINING CONSENT FROM DATA SUBJECTS

5.1   Company represents that it has implemented a consent mechanism or process (such as a consent screen or check-box) that is legally sufficient, where applicable, for purposes of compliance with Data Protection Laws, in that it permits Data Subjects to provide consent that is freely given, informed, specific, and unambiguous.

5.2   Smaato uses device identifiers and geolocation data (**"Device Data"**) to provide its services, including for the purpose of tracking Data Subject interactions for digital advertising. Company shall, and as applicable shall contractually require its data sources to, implement appropriate notice and consent mechanisms upon its digital properties so that Smaato can capture applicable Personal Data lawfully through such digital properties in order to perform its services under the Agreement. In particular, the notice and consent mechanism must contain a comprehensive description of the categories of first- and third-party cookies and other tracking technologies that may be used on Company's websites and its applications and the purposes for which they may be used, including for targeted advertising.

5.3   Each party shall use and honor any applicable signals and OpenRTB specifications that are passed to the other party, including any signal regarding (a) COPPA flagging, (b) GDPR consent, or (c) device-based opt-outs. Company shall not provide to Smaato Device Data regarding any device that has opted out through device settings unless it also provides any accompanying opt-out signal (e.g., LMT=1).

5.4   Each party shall make good faith efforts to implement, list itself in, or otherwise comply with IAB Europe's Transparency & Consent Framework and related industry-standard consent standards and mechanisms. The parties shall cooperate in good faith regarding the deployment of any such mechanism.

5.5   Upon Smaato's request, Company shall provide to Smaato any relevant information documenting its consent processes or mechanisms, and any supporting records regarding the manner in which Company obtains consent from applicable Data Subjects.

6. SECURITY

6.1   Each party will implement and maintain appropriate security measures for protection of the security, confidentiality, and integrity of Personal Data, including all measures required pursuant to Article 32 of the GDPR.

6.2   Pursuant to Article 28, Section 3(c) of the GDPR, each party will ensure (and contractually require) that any Data Processors with which it contracts take all measures required pursuant to Article 32 of the GDPR.

7. TRANSFERS OF PERSONAL DATA

7.1   To the extent the Processing of Personal Data involves a Transfer, including if Company and Smaato Transfer Personal Data through affiliates, subcontractors, or other third parties, and such Transfers of Personal Data originated from the European Economic Area ("**EEA**"), Switzerland, or other countries or jurisdictions recognizing the GDPR, each party represents and warrants that its Processing and/or Transfer of Personal Data does and will comply with all Data Protection Laws, in particular, any Transfer outside the EEA, Switzerland, or other countries or jurisdictions recognizing the GDPR is made pursuant to an appropriate transfer mechanism according to Article 44 et seq. of the GDPR.

7.2   If the Company Transfers Personal Data outside the EEA, Switzerland, or other countries or jurisdictions recognizing the GDPR to Smaato established in a country without adequacy decision of the European Commission in accordance with Article 45 of the GDPR, the Company and Smaato agree that

this transfer shall be made subject to the terms of the STANDARD CONTRACTUAL CLAUSES (MODULE 1) for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**SCC**"), (available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en (as amended, superseded or updated from time to time), and as entered into between Company and Smaato and as set forth in **Appendix B** to this DPA.

8.   SUBCONTRACTING*:* Company or Smaato may appoint third-party Data Processors to Process Personal Data for the purposes set forth herein or in the Agreement, provided that such Data Processors agree in writing to: (a) Process Personal Data in accordance with documented instructions; (b) implement appropriate technical and organizational security measures to protect the Personal Data against a Security Incident; and (c) otherwise provide sufficient guarantees that they will Process the Personal Data in a manner that will meet the requirements of applicable Data Protection Laws, including all requirements under Article 28 of the GDPR and Article 44 et seq. of the GDPR.

9.   MISCELLANEOUS PROVISIONS

9.1   Nothing in this DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA.

9.2   This DPA takes effect as of the date of last signature below ("**Effective Date**") and shall remain in effect during the existence of the Agreement. Without prejudice to the remedies as set forth elsewhere herein or in the Agreement, if either party violates this DPA, the other party is entitled to terminate the Agreement in its sole discretion and without any extra costs or expenses (provided any payments due and owing shall remain so).

9.3   Each party represents and warrants that (a) the person executing this DPA on its respective behalf has the legal authority to bind such party, and (b) it has right, power, and authority to (i) enter into this DPA, (ii) make the representations and warranties contained herein, and (iii) commit to and perform the respective duties, obligations, and covenants set forth hereunder.

Signed and Agreed between the parties on the Effective Date by:

By: By:

_____   _____

Company: **Smaato, Inc.**

Name: Name:

Title: Title:

Date: Date:

Appendix B

**STANDARD CONTRACTUAL CLAUSES –
MODULE ONE: Transfer Controller to Controller (C2C)**

<u>SECTION I</u>

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)[1] 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.

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

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

        (iii)   Clause 9 – [*not used in Module One (C2C) Standard Contractual Clauses*];

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

        (v)   Clause 13;

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

        (vii)   Clause 16(e);

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

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

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

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

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

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1   Purpose limitation

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

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

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

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

8.2   Transparency

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

       (i)   of its identity and contact details;

       (ii)   of the categories of personal data processed;

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

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

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

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

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

8.3 Accuracy and data minimisation

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

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

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

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymization[2] of the data and all back-ups at the end of the retention period.

8.5 Security of processing

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

---

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible

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

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

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

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

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

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

8.6   Sensitive data

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

8.7   Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union[3] (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

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

---

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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

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

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

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

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

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

8.8   Processing under the authority of the data importer

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

8.9   Documentation and compliance

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

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

Clause 9

Use of sub-processors

[*Not used in Module One (C2C) Standard Contractual Clauses*]

Clause 10

Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request[4]. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any

---

[4] [Footnote 10 in original doc.] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

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

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

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

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

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

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

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

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

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

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

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

<div align="center">

Clause 11
Redress

</div>

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

Clause 13

Supervision

(a) 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.

(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[5];

   (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.

---

[5] [Footnote 12 in original doc.] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(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 authorities, 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 suspensory 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 Federal Republic of Germany.

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 Hamburg, Federal Republic of Germany.

(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

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

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*]

1.	Name:	
	Address:	
	Contact person's name, position and contact details:	
	Activities relevant to the data transferred under these Clauses:	
	Signature and date:	
	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*]

1.	Name:	Smaato, Inc.
	Address:	350 Fifth Ave. Ste. 7700, New York, NY USA
	Contact person's name, position and contact details:	Data Protection Officer privacy@smaato.com
	Activities relevant to the data transferred under these Clauses:	Performance of services pursuant to the Agreement executed between Company and Smaato.
	Signature and date:	

Role (controller/processor):	Controller	

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred	Data subjects accessing or using data exporter's, applications and/or sites under the Agreement;
Categories of personal data transferred	- Advertising identifiers (e.g., IDFA, Google Advertising IDs); - IP addresses; - Demographic information (e.g., age, gender) (if provided by data exporter); - Precise geolocation information (if provided by data exporter); - Other unique identifiers.
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 to the extent that data exporter transfers data to data importer under the Agreement.
Nature of the processing	Adserving, bidding and/or reporting that will transfer data for advertising and reporting services provided by business units in the US or outside the EEA.
Purpose(s) of the data transfer and further processing	- Provision of the data importer services under the Agreement; - Address fraud, security, and technical issues; - Compliance with legal and regulatory requirements; - Exercise or defense of legal claims; - Financial and accounting record-keeping;

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	Personal data will be retained by the data exporter and data importer for the period necessary for the purposes for which such personal data collected. Criteria used to determine the applicable retention period include: • the sensitivity of the personal data; • technical and organisational measures implemented; • additional legal obligations (e.g, for financial and tax reporting); •
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	N/A

C.   COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Ludwig-Erhard-Str. 22 7.OG 20459 Hamburg E-Mail: mailbox@datenschutz.hamburg.de

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measures of pseudonymisation and encryption of personal data	Data is pseudonymised 7 days after receipt. In the period before pseudonymisation, it is stored (encrypted). Encryption at rest is always enabled.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Confidentiality: Only a specific set of people and processes that need to access the data can read or write to the storage location. Access is protected by physical, system (logical), and data access controls. Integrity: Storage systems have built-in redundancy, hardware fault detection and automatic error correction, across multiple availability zones (different data centers in the same region). Databases are also backed by EBS volume, and production databases have at least two replicas hosted in separate data centers in the same region. If an EBS device fails, the error would be detected and a new replica created from the same copy. Availability/Resiliency: GCP has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	For business critical services processing personal data the teams are using several monitoring and notification services. Third party services are sending status updates to responsible admins by mail and provide a status pages. Incident escalation is documented in our

	Incident Response Plan and will be reported the Incident Response Coordinator.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	There is a data protection and security concept in place, which is checked periodically and adapted to changing conditions, if necessary. This includes the Information Security Incident Response Plan, which provides a well-defined and organized approach for handling actual or potential threats to Smaato's business or user information maintained electronically (on computers and/or networks), or maintained physically in any other format. The plan also identifies and describes the roles and responsibilities of the Security Incident Response Team who will put the plan into action.
Measures for user identification and authorisation	Only employees and verified contractors can access systems and data and have to be logged in via Smaato's identity provider with strong, double-factor authentication. Smaato then has RBAC (Role-Based Access Control) to ensure as-needed access.
Measures for the protection of data during transmission	Data in transit between our systems is Encrypted with TLSv1.2 or later using private endpoints within our network.
Measures for the protection of data during storage	Personal Data is kept for only as long as necessary for incident response and forensic analysis. After 10 days, for long term storage, Personal data is removed from the data.
Measures for ensuring physical security of locations at which personal data are processed	See https://cloud.google.com/docs/security/overview/whitepaper Data is encrypted: should there be a physical security breach in a data centre, it would be impossible to read, or even identify, the data.

Measures for ensuring events logging	We utilize GCP Audit logs for infrastructure and Data access, as well as application-specific Audit logs to track data access. SPX and SDX have a change history that log all changes done to the system.
Measures for ensuring system configuration, including default configuration	Use of infrastructure as code and cryptographically secure version control systems, which are able to redeploy platform infrastructure when needed.
Measures for internal IT and IT security governance and management	There is a data protection and security concept in place, which is checked periodically and adapted to changing conditions, if necessary. This includes the Information Security Incident Response Plan, which identifies and describes the roles and responsibilities of the Security Incident Response Team who will put the plan into action.
Measures for certification/assurance of processes and products	Smaato is engaging a service provider only if either the security of the data processing is guaranteed by suitable and up-to-date documented evidence or Smaato has verified the security of the data processing after conducting an independent audit of the service provider.
Measures for ensuring data minimisation	Data exporter and data importer implement the industry-standard OpenRTB technical specifications related to the data made available to Pursuant to the agreement between data exporter and data importer, the parties agree not to share any special category personal data under Art. 9 of the GDPR or Personal Data such as names, email addresses and government identifiers.
Measures for ensuring data quality	- Accuracy: from our application servers to our storage, we use streaming solutions that have "at least once semantics" and unique IDs for deduplication. Every record that fails to be sent to the stream is reported as a metric on a separate platform for monitoring. - Relevancy: as we do not know how our demand partners make their bidding decision, it is important for us to store the whole data

	pertaining to each interaction to be used as evidence for disputed transactions
	• Completeness: "at least once semantics" and unique IDs for deduplication ensure that the data is complete. In case of data stream downtime, we have a backup solution that stores the data on GCS.
	• Timeliness: We have monitoring in place and receive alerts if data processing takes longer than expected.
	• Consistency: we use a structured, self-describing data format (Apache Parquet) so that we have guarantees against deviations and can use tools with clear, unambiguous semantics, like spark SQL for querying.
Measures for ensuring limited data retention	Main logs of the operational system handling AdRequests have stored Personal Dataremoved after 10 days.
Measures for ensuring accountability	There is an unalterable audit trail when accessing Smaato systems and data at rest. It serves as a deterrent as well as a tool for incident response.
Measures for allowing data portability and ensuring erasure	Media storage devices used to store customer data are classified by GCP as Critical and treated accordingly, as high impact, throughout their life-cycles. GCP has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, GCP decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from GCP control until it has been securely decommissioned.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter