APPENDIX: JOINT-CONTROLLERSHIP AGREEMENT

This Data Processing Agreement (here-after the "DPA") is part of the Terms and Conditions to reflect the agreement between Criteo and the Client (here-after the "Parties") in accordance with the requirements of Data Protection Laws.

WHEREAS

Parties are jointly determining the process and means of the Service. The Client places tags on its properties for Criteo to collect browsing information and create customized ads to serve to users. Criteo creates the ads, decides which ad to serve and where.

Parties have agreed that the DPA shall govern their mutual rights and obligations as Joint controllers.

HAVE AGREED AS FOLLOWS

ARTICLE 1: DEFINITIONS

Applicable Data Protection Laws means all present and future applicable laws and regulations relating to the Processing of Personal Data and privacy in the relevant jurisdiction, which shall include but not be limited to, for example

- in respect of the EU: the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), the E-Privacy Directive (Directive 2002/58) and all applicable national legislation implementing the Directive or supplementing the GDPR;

- in respect of the US: all federal and state legislations relating to privacy and/or information society, the rules of the Federal Trade Commission, the Children Online Privacy Protection Act ("COPPA");

- and in each case the equivalent of any of the foregoing in any relevant jurisdiction together with and any statutory modification, revision or re-enactment of the foregoing from time to time.

Data Subject means any natural person that is the subject of the Personal Data.

GDPR means 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

Joint controller means the Parties which jointly determine the purposes and means of the Processing of Personal Data.

Personal Data means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (e.g., first name, last name, phone number, IP address, ID User, Cookie ID , Hashed email address or every pseudonymous data).

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

Processor means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Joint controllers.

Pseudonymisation means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional

information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

Services means the service(s) provided by Criteo as described in the Terms and Conditions.

Third party means a natural or legal person, public authority, agency or body other than the Data Subject, controller, Processor and persons who, under the direct authority of the controller or Processor, are authorised to process Personal Data.

ARTICLE 2: PRIVACY PRINCIPLES

The Parties shall respect the following privacy principles:

Purpose limitation: Personal Data shall be collected for specified, explicit and legitimate purposes (in particular marketing purpose) and not further processed in a manner that is incompatible with those purposes.

Data minimization: Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy: Personal Data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Storage limitation: The Joint controllers shall implement mechanisms for ensuring that, by default, the only Personal Data processed is necessary for the specific purpose of the Processing and is not collected or retained beyond the minimum time limit necessary for this purpose. Personal Data that are no longer required to fulfill the legitimate purposes must be destroyed or anonymized or transferred to an archive for historical, scientific, statistical, dispute resolution, investigations or general archiving purposes to the extent that this allowed by the Data Protection Laws.

Security, integrity and confidentiality: Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The security measures should be appropriate to the level of risk of the Processing.

Transparency: Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. The Joint controllers shall take appropriate measures to provide transparency and information relating to Processing to the Data Subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. The information shall be provided at the time when Personal Data are obtained.

ARTICLE 3: ACCOUNTABILITY

The Joint controllers shall be able to demonstrate compliance with the Privacy Principles.

In particular:

- the Client undertakes to include on its properties (i) a privacy policy that includes a link to the Criteo privacy policy and when legally compulsory (ii) appropriate notice and choice mechanisms that comply with relevant laws and regulations and, where applicable, with the specific requirements of the competent local supervisory authorities.
  When applicable laws and regulations require obtaining user consent, the Client undertakes to: (i) clearly inform users that they can give or withhold consent to Criteo dropping cookies (or other tracking technologies), as well as the purposes of these cookies, in particular the purpose of serving

personalized advertising, specifying, where applicable, whether the data collected is used for Cross Device Linking purposes; (ii) allow users to express their choice by a clear positive act as well as to modify it with the same ease and; (iii) allow users to learn more and object to Criteo's Services.

The Client must also provide Criteo with proof of such consent upon request so that Criteo can rely on it at any time.

- Criteo undertakes to collect and use Personal Data in accordance with applicable laws and regulations, including but not limited to laws governing privacy and data protection. In this regard, Criteo will:[2]
  i) include a link to Criteo's Privacy Policy page (www.criteo.com/privacy) that will include information for users on how to disable Criteo Service (and insert an "opt-out" link) in all advertisements served on the Client Properties;
  ii) ensure that the Personal Data collected through its technologies for the purpose of the Service is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
  iii) provide users with an easy way to exercise their rights as a Data Subject;
  iv) respond to Data Subject requesting to exercise their rights without undue delay;
  v) implement appropriate technical and organizational measures to ensure a level of security that is appropriate to the risk presented by the data Criteo processes for the purpose of the Service;
  vi) ensure that the Personal Data processed by Criteo for the purpose of the Service will only be retained for an appropriate period of time that complies with Applicable Data Protection Laws and recommendations of the competent data protection authorities.

ARTICLE 4: RIGHTS OF DATA SUBJECTS

The Joint controllers shall facilitate the exercise of Data Subject rights set out in the GDPR, including:

Rights of rectification:
Where applicable, the Data Subject shall have the right to obtain from the Parties the rectification of inaccurate Personal Data concerning him or her.

Rights of objection:
The Data Subject shall have the right to object at any time to Processing of Personal Data concerning him or her. The Joint controller shall no longer process the Personal Data processed for marketing purpose.

Rights of access:
The Data Subject shall have the right to obtain from the Joint controller confirmation as to whether or not Personal Data concerning him or her are being processed.

The Joint controller shall provide information that they handle about the Data Subjects to them without undue delay and in any event within one month of receipt of the requests. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

ARTICLE 5: TRANSFER OF PERSONAL DATA

Personal Data may only be transferred to a third country or to an international organisation outside of the European Union in compliance with the conditions for transfer set out in Chapter V of the GDPR.

Article 6: COOPERATION BETWEEN PARTIES

The Parties and, where applicable, their representatives, shall cooperate between them and, on request, with the supervisory authority in the performance of its tasks.

The Parties and, where applicable, their representatives, shall cooperate to comply with the Applicable Data Protection Laws and to meet their obligations pursuant to this DPA.

ARTICLE 8: TERMINATION

The DPA shall terminate on the date of the termination of the Service Agreement. Expiration or termination (for any reason) of the Agreement shall not affect any accrued rights or liabilities which either Party may then have nor shall it affect any clause which is expressly or by implication intended to continue in force after expiration or termination. In particular, Article 4 shall survive during two months after the termination.