

PREAMBLE

This Criteo Data Protection Agreement (hereafter the “**DPA**”) supplements the Criteo Umbrella Terms of Service (the “**Terms**”) and the relevant Criteo Specific Terms of Service (the “**STS**”) or any other applicable agreement with the Partner (collectively, the “**Agreement**”), and is hereby incorporated into the Agreement between Criteo and the Partner for the provision of the relevant Criteo Services.

This DPA describes the protection and security obligations of the Parties with respect to any Processing of Personal Data carried out in connection with the provision of the relevant Criteo Services, including the processing of Service Data if and then solely to the extent that such data contains Personal Data, in accordance with the requirements of Data Protection Law. This DPA is organized around the following sections:

- **Section I: Common Terms**
 - Section I applies when Partner has ordered Services from Criteo, regardless of the type of Services ordered.
- **Section II: Joint Controller Terms**
 - Section II applies when Partner has ordered Services in which Criteo and Partner act as Joint Controllers as set out in the relevant STS (the “**Joint Controller Services**”).

Section I of this DPA always applies to the Parties. Application of Section II will depend on the status under which Criteo operates and that is specified in the STS or in any other applicable arrangement applying to the Service ordered by the Partner.

Section I: Common Terms**1 Definitions**

Unless otherwise stated herein, definitions set out in the Agreement apply to this DPA. The additional definitions set out below shall apply to this DPA.

“Consent”	means any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.
“Controller”	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. Under Section II of this DPA, Criteo S.A., as the parent company for Criteo Group, and the Partner act as Joint Controllers. The term “Controller” includes “Business”, as defined under the CCPA.
“Data Protection Law”	means any and all applicable international, national, federal and state laws and regulations relating to data protection and privacy, including but not limited to: (a) the General Data Protection Regulation (“EU GDPR”), (b) the UK Data Protection Act (“UK GDPR”), (c) the California Consumer Privacy Act (“CCPA”) as amended by the California Privacy Rights Act of 2020, (d) the Virginia Consumer Data Protection Act (“VCDPA”), (e) the Colorado Privacy Act (“CPA”), (f) the Connecticut Data Privacy Act (“CTDPA”), (g) the Utah Consumer Privacy Act (“UCPA”), (h) the Oregon Consumer Privacy Act (“OCPA”), (i) the Texas Data Privacy and Security Act (“TDPSA”), (j) the Montana Consumer Data Privacy Act (“MTCDPA”), (k) Delaware Personal Data Privacy Act, (l) Iowa Consumer Data Protection Act, (m) Nebraska Data Privacy Act, (n) New Hampshire Data Privacy Act, (o) New Jersey Data Privacy Law, (p) the Korean Personal Information Protection Act (“PIPA”); each as implemented in each jurisdiction, and any amending or replacement legislation (or similar) from time to time. For the sake of clarity, Data Protection Law also includes all legally binding requirements issued by the competent data protection authorities i) governing the processing and security of information relating to individuals and providing rules for the protection of such individuals’ rights and freedoms with regard to the processing of data relating to them, ii) specifying rules for the protection of privacy in relation to data processing and electronic communications, or iii) enacting rights for individuals which are enforceable towards organizations with respect to the processing



of their personal data, including rights of access, rectification and erasure. Any Data Protection Law listed herein only apply to the Partner to the extent this is provided for under the criteria set by law.

- “Data Subject”** means an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier (e.g., a name, an identification number, location data, an online identifier) or to one or more factors specific to that natural person. For the purpose of this DPA, “Data Subject” refers to the natural persons whose Personal Data is processed as part of the provision of the relevant Criteo Services.
- “Joint Controller”** means a Controller acting jointly with one or several others. Under Section II of this DPA, Criteo and the Partner act as joint controllers.
- “Personal Data”** means any information identifying, relating to, describing, or is capable of being associated with, or can reasonably be linked with, an identified or identifiable natural person or household Processed in connection with the provision of the relevant Criteo Services.
- “Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
- “Processor”** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller. Processor includes “Service Provider”, as defined under the CCPA.
- “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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- “Regulatory Authority”** means the applicable public authority or government agency responsible for supervising compliance with Data Protection Law, including but not limited to: the French CNIL (Criteo’s supervisory authority), UK Information Commissioner’s Office, California Privacy Protection Agency or yet U.S. state attorneys general.

The terms “Business,” “Business Purpose,” “Sale,” and “Share” shall have the same meaning as in the applicable Data Protection Law, and their cognate terms shall be construed accordingly.

2 Compliance with Law

- 2.1** Each Party shall comply and shall be able to demonstrate its compliance with its respective obligations under Data Protection Law and in accordance with this DPA.
- 2.2** The Partner specifically acknowledges and agrees that its use of the Joint Controller Services is compliant with Data Protection Law.

3 Authorizations

- 3.1** A Party shall not disclose Personal Data to the other Party, except where the disclosing Party warrants to the other Party that this disclosure is compliant with Data Protection Law and that it has complied with any applicable requirement(s) of information, notification to, or of authorization or consent from the relevant public authority(ies) or the relevant Data Subjects, with respect to any Personal Data provided by the disclosing Party to the other Party. Each disclosing Party must retain evidence of compliance with any such requirements for the duration of the Agreement and provide it promptly to the other Party upon request.
- 3.2** Nothing in this DPA shall prohibit or limit Criteo’s rights to implement anonymization or de-identification of Personal Data processed in connection with the Agreement, and to the extent required under Data Protection Law, Partner hereby authorizes Criteo to implement anonymization techniques in compliance with Data Protection Law. For the sake of clarity, data resulting from effective and compliant anonymization or de-identification is not subject to this DPA and more generally to Data Protection Law.

4 Cooperation

- 4.1** The Parties shall cooperate to comply with Data Protection Law and to meet their obligations pursuant to this DPA.
- 4.2** The Parties shall keep appropriate documentation on the Processing activities carried out by each of them and on their compliance with Data Protection Law and with this DPA.
- 4.3** In the event of an investigation, proceeding, formal request for information or documentation, or any similar event in connection with a data protection authority and in relation to the Joint Controller Services or to Personal Data, the Parties shall promptly and adequately deal with enquiries from the other Party that relate to the Processing of Personal Data under the Agreement.
- 4.4** In the event of any change to or new Data Protection Law(s), the Parties shall mutually agree upon any reasonably necessary amendments or revisions to this DPA.

5 Data Protection Officers

- 5.1** Criteo and the Partner appointed a data protection officer. Criteo's data protection officer may be reached at: dpo@criteo.com. The contact details of the Partner's data protection officer must be communicated to Criteo.

Section II – Joint Controller Terms

6 Scope of this Section II

- 6.1** This Section II shall apply only with respect to Processing of Personal Data carried out in the context of the provision by Criteo of the Joint Controller Services ordered by the Partner.
- 6.2** In accordance with article 26 of the GDPR, the Parties hereby determine their respective responsibilities for compliance with their obligations under GDPR.
- 6.3** For purposes of the CCPA, Partner shall be a "Business" and Criteo shall be a "Third Party."

7 Obligations of the Parties when acting as Joint Controllers

- 7.1** When Processing Personal Data as Joint Controllers under Section II of this DPA, each Party agree that it shall:
- (a) Comply with any requirements arising under Data Protection Law and not perform its obligations under this DPA and/or ask the other Joint Controller to perform its obligations in such a way as to cause the other Joint Controller to breach any of its obligations under Data Protection Law.
 - (b) Take into account all the data protection principles provided for in the Data Protection Law, including but not limited to the principles of purpose limitation, data minimization, accuracy, storage limitation, security, integrity and confidentiality, transparency and protection of Personal Data by design and by default.
 - (c) Maintain a record of the Processing of the Personal Data under its responsibility.
 - (d) Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the Processing of the Personal Data that it carries out (including, for the Partner, in relation to the Partner Digital Properties), in particular to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.
 - (e) Take all the measures necessary to address any Personal Data Breach relating to the Personal Data it processes, mitigate its effects, prevent further Personal Data Breach and, when required, notify the competent data protection authority(ies) and the Data Subjects.
 - (f) Cooperate to the preparation of the required data protection impact assessments.
 - (g) Carry out any assessment, consultation and/or notification to competent data protection authorities or Data Subjects, in relation to the Processing it carries out; and



- (h) Handle any Data Subject's requests and/or complaints it receives, in particular the requests relating to the exercise of their rights under Data Protection Law, including the rights of access, rectification, erasure and objection and the right to withdraw Consent. Where a Party receives a Data Subject's right request in respect of Personal Data processed by the other Party, such receiving Party will direct the Data Subject to the other Party's privacy policy explaining how to exercise his or her right request with such other Party, in order to enable such other Party to reply directly to the Data Subject's request.

8 Criteo's Obligations

8.1 Criteo shall be solely responsible, in accordance with and to the extent required by Data Protection Law, for including a link to Criteo's Privacy Policy page (www.criteo.com/privacy) that will include information for Data Subjects on how to disable Criteo Service (and insert an "opt-out" link) in all advertisements served on the Partner Digital Properties.

8.2 To the extent that Criteo is a Third Party under the CCPA: (a) Criteo's use of Personal Data is limited to the specific purposes identified in the Agreement and Criteo shall not exceed such specific purposes; (b) Criteo shall comply with applicable obligations and provide the same level of privacy protection as required of a Business pursuant to the CCPA with respect to Personal Data; (c) Criteo grants the Partner the right, upon reasonable notice, to take reasonable and appropriate steps to ensure that Criteo uses Personal Data in a manner consistent with this Agreement and applicable Data Protection Laws, including reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data; and (d) Criteo shall notify the Partner if it determines that it can no longer meet its obligations under applicable Data Protection Laws.

9 Obligations of the Partner

9.1 Partner shall be solely responsible, in accordance with and to the extent required by Data Protection Law for:

- (a) providing the Data Subjects with all necessary information pursuant to Data Protection Law, including in accordance with Articles 13 and 14 of the GDPR, in respect of the Processing of the Personal Data in relation to the Joint Controller Services;
- (b) providing appropriate notice on Partner's Digital Properties for any relevant Processing of Personal Data by Criteo for the Joint Controller Services, including by providing a link to Criteo's privacy policy (www.criteo.com/privacy);
- (c) collecting and documenting Consent or opt-out provisions, as applicable, obtained from Data Subjects;
- (d) implementing choice mechanisms to request valid Consent from Data Subjects or opt-out provisions, as applicable, in compliance with Data Protection Law and, where applicable, with the specific requirements of the competent local supervisory authorities;
- (e) where opt-out provisions are applicable, offering Data Subjects the right to opt-out of the sale and share of their Personal Data or use of the Personal Data for purposes of targeted advertising;
- (f) complying with the requirements applicable to the validity period of the Consent collected and request Consent from the Data Subjects once this validity period has expired;
- (g) where applicable, Partner represents and warrants that each third-party advertising technology partner that Partner works with in relation to the advertising space on Digital Properties that is made available for sale through Criteo Platform (each a "Consented Third-party Vendor") fully complies with the provision of this DPA;
- (h) providing promptly to Criteo, upon request and at any time, proof that a Data Subject's Consent has been obtained by the Partner.

Last updated: May 2025