CRITEO DATA PROTECTION AGREEMENT

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 III: Controller-to-Processor Terms (only applicable to Mabaya)**
  - Section III applies when Partner has ordered Services in which Partner acts as Controller and Criteo acts as a Processor, processing Personal Data on behalf of Partner as set out in the relevant STS (the "**Controller-to-Processor Services**").

Section I of this DPA always applies to the Parties. Application of Section II and/or III 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

The provisions of this Section I "Common Terms" always apply when Partner has ordered Services from Criteo, regardless of the type of Services ordered.

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 and under Section III of this DPA, the Partner acts as Controller. The term "Controller" is considered as "Business "under the CPRA.
"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") and the California Privacy Rights Act ("CPRA"), (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) 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. Under Section II of this DPA, the processors that can be engaged either by Criteo or the Partner are Processors and under Section III of this DPA, Criteo S.A., as the parent company for Criteo Group, acts as Processor.
"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**," "**Service Provider**," 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 and Controller-to-Processor 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 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 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 with respect to the Joint Controller and Controller-to-Processor Services.

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 or Controller-to-Processor 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 CPRA, 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 CPRA: (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 CPRA 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.

Section III - Controller-to-Processor Terms (only applicable to Mabaya)

10 Scope of this Section III

10.1 This Section III shall apply only with respect to Processing of Personal Data carried out in the context of Controller-to-Processor Services ordered by the Partner, acting as a Controller or Business (as applicable), for which Criteo is acting as a Processor or Service Provider (as applicable), and for which the subject-matter, the nature and purpose, the type of Personal Data, categories of Data Subjects and duration of Processing are set out in Appendix 1 "Controller-to-Processor Services - Details of Processing of Personal Data".

11 Obligations of Partner

11.1 The Partner shall not provide Personal Data to Criteo except as is necessary for performance of the Criteo Services and unless Partner shall have given the necessary notices and obtained the necessary consents, in each case, from the applicable Data Subjects whose Personal Data is Processed by Criteo pursuant to the Agreement. Partner shall, in its use of the Criteo Services, Process Personal Data in accordance with the requirements of Data Protection Law and shall immediately notify Criteo if Partner is in violation of any Data Protection Law. The Partner's instructions to Criteo related to the Processing of Personal Data shall comply with Data Protection Law. The Partner shall be solely responsible to ensure the accuracy, lawfulness, and quality of the Personal Data and to ensure that the Processing entrusted to Criteo has an adequate legal basis pursuant to Data Protection Law.

12 Obligations of Criteo

12.1 **Partner Instructions.** Criteo shall process Personal Data for the relevant Controller-to-Processor Services only on the documented instructions from Partner. Partner may not instruct Criteo to process Personal Data in a manner not compatible with the Agreement and more particularly this DPA. Criteo shall immediately inform Partner if Criteo reasonably believes it is unable to follow Partner's instructions, or if such instructions are not compatible with the STS or more generally with the Agreement.

12.2 **Inaccurate or Outdated Data.** Criteo shall inform Partner if Criteo becomes aware that the Personal Data is inaccurate or has become outdated, and Criteo shall cooperate on request with Partner to erase or rectify such data.

12.3 **Personal Data Processing.** To the extent required by applicable Data Protection Law, Partner shall only instruct Criteo to Process Personal Data for those Business Purposes permitted under applicable Data Protection Law and shall disclose Personal Data to Criteo only for the limited and specified purposes specified in the Agreement. Partner reserves the right, upon reasonable notice, to take reasonable and appropriate steps to help ensure that Criteo uses Personal Data transferred in a manner consistent with Partner's obligations under applicable Data Protection Law, including reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

Criteo shall not: (a) Sell or Share Personal Data; (b) retain, use, or disclose Personal Data for any purpose other than for the Business Purposes specified in the Agreement; (c) retain, use, or disclose Personal Data outside of the direct business relationship between Partner and Criteo; or (d) combine Personal Data it receives from Partner with Personal Data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with data subjects, provided that Criteo may combine Personal Data to perform a Business Purpose (with the exception of "advertising and marketing services," as defined under applicable Data Protection Law). Criteo shall comply with applicable obligations and provide the same level of privacy protection as required by the applicable Data Protection Law and shall assist Partner through appropriate technical and organizational measures to comply with Data Protection Law requirements, taking into account the nature of the processing. Criteo shall notify Partner if it makes a determination that it can no longer meet its obligations under the applicable Data Protection Law.

12.4 **Technical and Organizational Measures.** Criteo shall implement appropriate technical and organizational measures to ensure the security of the Personal Data, including protection against a Personal Data Breach. In complying with its obligations under this paragraph, Criteo shall at least implement the technical and organizational measures specified

in Appendix 2 "Security Schedule". Partner hereby confirms to Criteo that it considers that Criteo's technical and organizational measures as specified in Appendix 2 "Security Schedule" provide an appropriate level of security. Criteo shall also assist Partner in complying with its obligations in relation to the security of Processing Personal Data, including under article 32 of the GDPR.

12.5 **Personal Data Breaches.** In the event of a Personal Data Breach relating to Personal Data processed by Criteo, Criteo shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. Criteo shall also notify Partner without undue delay after having become aware of the breach and providing for the time necessary to provide relevant information, including e.g. a description of the nature of the breach (including, where possible, categories and approximate number of Data Subjects and Personal Data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. In the event of a Personal Data Breach relating to Personal Data processed by Criteo, Partner shall be solely responsible for notifying Data Subjects and/or Regulatory Authorities as required by Data Protection Law, and Criteo shall cooperate with and assist Partner to enable compliance with any request from a competent authority and/or affected Data Subjects, taking into account the nature of Processing and the information available to Criteo. Before any such notification is made, Partner shall consult with and provide Criteo an opportunity to comment on any notification made in connection with a Personal Data Breach. Nothing in this DPA shall be construed to require Criteo to violate, or delay compliance with, any legal obligation it may have with respect to a Personal Data Breach. Criteo shall have no liability for the Personal Data Breach management and notification obligations described in this Section unless the Personal Data Breach is caused by Criteo's breach of the security obligations under Section 12.4 of this DPA or other violation of Data Protection Law by Criteo.

12.6 **Access to Personal Data.** Criteo shall grant access to the Personal Data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the Agreement and in accordance with this DPA. It shall ensure that persons authorized to process the Personal Data have committed themselves to one or several confidentiality agreements or are under an appropriate statutory obligation of confidentiality.

13 **Data Subjects' Rights.** To the extent legally permitted, Criteo shall promptly notify the Partner of any request it has received from a Data Subject to exercise the Data Subject's rights, including the rights to: knowledge/access; correction; deletion; restriction; objection; data portability; opt out of the Processing of and/or the Sale or Sharing of Personal Data; limit the use or disclosure of sensitive Personal Data; or any other request with respect to Personal Data of the applicable Data Subject, as set forth under applicable Data Protection Law. Criteo shall not respond to the request itself. Criteo shall reasonably assist the Partner by implementing appropriate technical and organizational measures, insofar as this is possible, in fulfilling its obligations to respond to Data Subjects' requests to exercise their rights under Data Protection Law, taking into account the nature of the Processing. To the extent legally permitted, Partner shall be responsible for any costs arising from Criteo's provision of such assistance. Nothing in this Section 13 shall require Criteo to disclose or reveal any trade secrets.

13.1 **Data Protection Impact Assessment.** Upon Partner's request, at Partner's cost, and to the extent required under Data Protection Law, Criteo shall assist Partner in complying with any required data protection impact assessment on Partner's request, taking into account the information available to Criteo. To the extent required under the GDPR or UK GDPR, Criteo shall provide reasonable assistance to Partner in its cooperation or prior consultation with a Regulatory Authority in the performance of its tasks relating to this Section 13.1.

13.2 **Sub-Processors.** Criteo may engage sub-Processors as set out in Appendix 1 "Controller-to-Processor Services - Details of Processing of Personal Data**"**. Partner provides Criteo with general authorization to engage other sub-Processors to carry out Processing for the relevant Controller-to-Processor Services. Upon written request from Partner, Criteo shall inform Partner of any changes concerning the addition or replacement of sub-Processors. If Partner objects to such changes on reasonable grounds [concerning data protection] within thirty (30) days from the notification by Criteo to Partner, the Parties will discuss in good faith with a view to find a mutually acceptable solution. If the Parties fail to agree, Criteo may terminate the Agreement in whole, or in part with respect only to the affected Controller-to-Processor Services. When engaging another Processor, Criteo shall enter into an agreement binding on such Processor and setting out the same or more stringent data protection obligations as set out in this DPA, in particular, providing sufficient guarantees to implement similar technical and organizational measures.

13.3 **Processing Personal Data outside of the Partner's Instructions.** Notwithstanding the above, if applicable law or a binding decision from a competent authority requires Criteo to process Personal Data outside of Partner's instructions

for the purposes of providing the Controller-to-Processor Services, Criteo shall inform Partner unless otherwise prohibited under applicable law.

13.4 **Audit.** Partner may request in writing, at reasonable intervals, that Criteo makes available to Partner information regarding Criteo's compliance its obligations pursuant to Section III of this DPA in the form of a copy of Criteo's then most recent third-party audits or certifications.

Partner can request an on-site audit of Criteo's Processing activities described in Section III of this DPA by providing Criteo with reasonable notice. Such on-side audit may only be conducted where (i) the information made available by Criteo as set out above is insufficient, (ii) a Personal Data Breach has occurred or (iii) such audit is required by Data Protection Law or a Regulatory Authority.

The Parties shall agree on the scope, timing and duration of the audit. The audit may not unreasonably interfere with Criteo's activities.

The Partner may only appoint a third-party auditor which is not a competitor of Criteo. Such third-party auditor shall enter into a non-disclosure agreement with Criteo and the Partner before carrying out the audit.

After the on-site audit, the Partner shall promptly share the results of such audit with Criteo.

The Parties shall make available, upon request, to a Regulatory Authority, the information referred to in this clause, including the results of any audits.

Partner shall bear all costs related to audits.

13.5 **Transfers of Personal Data.** Any transfer of data to a third country or an international organization by Criteo shall be done only on the basis of documented instructions from the Partner in compliance with Chapter V of GDPR. The Partner agrees that where the Criteo engages a sub-Processor in accordance with Clause 13.2 for carrying out specific Processing activities (on behalf of the Partner) and those Processing activities involve a transfer of Personal Data within the meaning of Chapter V of GDPR, Criteo and the sub-Processor can ensure compliance with Chapter V of GDPR by using standard contractual clauses adopted by the European Commission in accordance with of Article 46(2) of GDPR, provided the conditions for the use of those standard contractual clauses are met.

13.6 **Consequences of Termination.** If Partner terminates a Controller-to-Processor Service, or if the Agreement expires or terminates for any reason whatsoever, Criteo shall, at the choice of the Partner, delete all Personal Data processed only for that Controller-to-Processor Service, or return all such Personal Data to Partner. Criteo shall provide certification as applicable that copies of such Personal Data have been deleted, on request in writing from the Partner, without prejudice to any operational backups maintained by Criteo for a reasonable period in accordance with industry standards. If applicable law prohibits Criteo from deleting the Personal Data, Criteo warrants that it will continue to ensure compliance with this DPA and will only process such Personal Data to the extent and for as long as required by applicable law.

The Parties' authorized signatories have duly executed this DPA:

PARTNER	**CRITEO**
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

APPENDIX 1: Controller-to-Processor Services- Details of Processing of Personal Data

(only applicable to Mabaya)

Category of Data Subjects			
Categories of Data Subjects whose Personal Data is Processed	Partner Digital Properties users (shoppers)	Controller's employees	Sellers (employees/representatives)
Categories of Personal Data Processed	Identifiers consisting of a series of characters (identifier contained in a cookie or other) provided by Controller (when these data are qualified as Personal Data under Data Protection Law)	Name and email addresses of authorized Controller employees/representatives	Email addresses of Sellers (to send them reports and notifications)
Sensitive data	N/A		
Nature of the Processing	Collecting, hosting, processing to provide the Service, deleting		
Purpose(s) for which the Personal Data is Processed on behalf of the Controller	Matching conversions to clicks (in the context of the Ads)	Identity checks (login page) Account administration	Emails notification to Sellers
Duration of the Processing	Term of the Agreement		

Partner acknowledges and authorizes Criteo's use of the following entities as sub-Processors, as applicable, with respect to the relevant Controller-to-Processor Services:

Sub-Processor	**Subject matter of the Processing**	**Nature of the Processing**	**Categories of Data Subjects**	**Categories of Personal Data Processed**	**Duration of the Processing**
Amazon Web Services (AWS)	Hosting (data center in Ireland)	Hosting	See above	See above	Term of the Agreement
Sendgrid	Sending emails to clients (US)	Use contact data to send emails	Partner's employees	Email addresses	Term of the contract

Appendix 2 - Criteo Security Schedule

This security schedule (the "**Schedule**") represents security controls relative to the Criteo Service(s) and overall security governance.

This Schedule is supplemental to the terms between Criteo and the Partner and forms part of the Agreement. In case of contradiction between the Agreement and this Schedule, this Schedule shall supersede.

1. **Definitions**

The following definitions support the provisions specified within this Schedule:

Confidential Information: means, specifically in the context of this Schedule, Partner and Criteo information process, stored and transmitted by Criteo service platforms and related data assets and supporting security controls applied to protect data security.

Data Assets: means any technology platforms, components, data or information processed through Criteo service product platforms processing, transmitting or storing Confidential Information.

Data Breach: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Security Breach: means any actual or potential unauthorized access to or use, disclosure, alteration, or destruction of Confidential Information, or any act or omission that compromises data relevant to the contract services that relate to the protection of the security, confidentiality or integrity of Confidential Information.

2. **Security controls**

The following security and privacy controls are maintained and supported by Criteo related to the Criteo services:

Security Governance and Management: Criteo will maintain a Security Management System similar to ISO 27002, inclusive of other industry known privacy and security best practices and supporting security controls. This will include appropriate documentation (security policies, processes, guidelines, standards, configuration standards and associated security controls to assure adequate protection to Criteo and Partner data assets throughout the Service lifecycle.

Security Assessments: No more than once per calendar year and only upon receipt of a written request with no less than thirty (45) business days' notice, Partner shall be permitted perform security assessments on Criteo's Security Management System and associated security controls directly associated with the services provided as Processor. Security Assessments will be limited to general detail security questionnaires, queries or specific questions related to the contracted services and exclude physical audits, penetration tests, scans or other intrusive activities. The Security Assessments should be preferably done by a third party auditor, which will be subject to confidentiality and shall subject its report for validation to Criteo before final results are provided to the Partner. Such requests will be promptly supported providing access to Criteo security controls applied to protect Criteo and Partner data assets against security threats, risks and vulnerabilities, with responses provided within reasonable timeframes, and accurately represented.

3rd Party Security Assurance: Criteo will maintain appropriate security assurance controls to appropriate manage data security risks for 3rd party services to ensure the protection of Criteo and Partner data assets.

Security Training: Criteo will maintain appropriate security and privacy security awareness programs to proactively protect Criteo and Partner data assets with content aligned to industry best practices to mitigate risks to data security.

Physical and Environmental Security Controls: Criteo will maintain appropriate physical and environmental security controls to protect against data security risks, protect against risks to confidentiality, integrity and availability. All such controls will be aligned to applicable industry, operational and security best practices protecting against physical and environmental security risk, including physical access controls, physical security monitoring and environmental protections against power disruptions, fire hazards, and related operational risks.

Access Control: Criteo will maintain a comprehensive access control management system aligned industry best practices to protect Criteo and client data assets with appropriate governance for the access, ensuring appropriate controls for authorization and authentication, based on the principle of least privileged. These controls shall include identification of privilege accounts with appropriate multifactor authentication (MFA) applied to permissions with access to Confidential Security Information. All authorized accounts, general or administrative, will have access logs collected, monitored, with permissions reviewed on a regular basis.

Business Continuity Management (BCM) System: Criteo will maintain a Business Continuity Management ("BCM") System that will detail continuity controls, roles, responsibilities and recovery measures to maintain contracted Service availability requirements in response to a broad spectrum of potential disasters and operations risks that could disrupt operations and timely delivery of materials and services. Criteo will maintain a BCM System that includes regular testing intervals to ensure effectiveness of controls. Upon specific written request of the Partner, Criteo will support reasonable assessments and questions relating to the effectiveness of its BCM System controls.

Application and Software Security: Criteo will maintain appropriate Secure Software Development ("SDL") processes that ensure effective release, change and configuration controls are operated and appropriate application security controls are maintained to protect company and client data assets. This shall include maintaining software versions and components at appropriate levels to ensure adequate protection.

Device Security: Criteo will maintain appropriate device security for its employees that includes 24x7x365 security monitoring, detection and response through EDR endpoint protection and configuration baselines applied.

Network Security: Criteo will maintain appropriate network security controls to protect against disruption of Service availability or a Security Breach. This will include 24x7x365 security incident monitoring and detection response, and application of security best practices, including segmentation and vulnerability scanning.

Encryption: Criteo will maintain appropriate encryption ciphers and protocols to protect data in transit, with appropriate encryption or equivalent controls applied if data assets are required to transferred through external media if requested.

Security Breach Reporting: Criteo will notify the Partner of any Security Breach of Confidential Security Information (including Personal Information), within 72 hours. Criteo at its own expense will mitigate, investigate and provide an appropriate relevant data and information in a security incident report, detailing the impacted data and necessary related information, if a security breach is detected impacts Confidential Information.

Security Incident Management: Criteo will maintain 24x7x365 security detection and response capabilities to assure appropriate detection and response to actual and potential data security risks to Criteo data assets. These security incident management controls will be operated and maintain by a dedicated Security Team.

Vulnerability Management: Criteo will maintain and operate a comprehensive vulnerability management system, with appropriate controls aligned to industry best practices and standards. These controls include vulnerability scans across production environment platforms, with reporting, analysis and mitigation of detected vulnerabilities appropriately managed, such scans will be applied internally and externally.