Quantcast Choice Terms of Service

Last Updated: May 7, 2020

Once you have agreed to these **Terms and Conditions** you will be able to download and install the Quantcast Choice CMP Agreement to these Terms and Conditions does not require you to become a Quantcast Choice customer. These terms will apply only after such download and installation of the Quantcast Choice CMP on your site.

These Quantcast Choice Terms of Service, including the attached Quantcast Choice Processing Terms (collectively, this "**Agreement**"), describe the terms and conditions on which Quantcast makes Quantcast Choice (the "**Solution**") available to Customer.

BY USING THE SOLUTION, CUSTOMER IS AGREEING TO BE BOUND BY THIS AGREEMENT. IF CUSTOMER IS ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, CUSTOMER REPRESENTS THAT CUSTOMER HAS THE AUTHORITY TO BIND SUCH ENTITY, IN WHICH CASE THE TERM "**CUSTOMER**" WILL REFER TO SUCH ENTITY (OR, IF SUCH ENTITY IS ACTING AS AN AUTHORIZED THIRD PARTY, THEN THE TERM "**CUSTOMER**" WILL REFER TO SUCH ENTITY, THE AUTHORIZING PARTY(IES), OR BOTH, AS APPLICABLE). QUANTCAST MAY MODIFY THIS AGREEMENT FROM TIME TO TIME; CONTINUED USE 30 DAYS AFTER NOTIFICATION WILL CONSTITUTE ACCEPTANCE (SEE SECTION 6). PLEASE READ THIS AGREEMENT CAREFULLY.

1. Certain Definitions.

"**Applicable Privacy Laws**" means the GDPR and the CCPA.

"**IAB Privacy Frameworks**" means the IAB Europe Transparency and Consent Framework and the IAB CCPA Compliance Framework.

"**CCPA**" means Title 1.81.5 of the California Civil Code.

"**EU 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.

"**UK GDPR**" means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, if in force.

"**GDPR**" means, as applicable: (a) the EU GDPR; and/or (b) the UK GDPR.

"**Choice Tag**" means the particular JavaScript code or SDK provided to Customer by Quantcast and embeddable on web pages or apps for implementation of the Solution, together with any fixes, updates, and upgrades provided to Customer.

"**Choice Signal**" means the indication as to whether a website visitor or app user (i.e., end user) has (a) been informed of; (b) provided, withheld, or withdrawn consent to; (c) objected or removed objections to; or (d) otherwise opted in or out of the processing of Personal Information for some or all purposes by some or all third parties in accordance with IAB Privacy Frameworks.

"**Personal Information**" has the same meaning as "personal data" or "personal information" under Applicable Privacy Laws.

2. Quantcast Transparency and Consent Management Platform.

a. **Solution.** Quantcast will provide Customer with the Choice Tag and Quantcast Choice Technical Guide in order for Customer to implement the Solution. The Solution comprises the Quantcast Choice Basic Services, the Quantcast Choice Additional Services, and the Quantcast Measure Component:

(i). "**Quantcast Choice Basic Services**" means the applicable services listed here as Quantcast Choice Basic Services, as updated from time to time.

(ii). "**Quantcast Choice Additional Services**" means the applicable services, if any, listed here as Quantcast Choice Additional

Services, as updated from time to time.

(iii). "**Quantcast Measure Component**" means the applicable services listed at https://www.quantcast.com/products/measure-audience-insights/, as updated from time to time. By using the Solution, Customer additionally agrees to be bound by, and to comply with, the Quantcast Measure and Q for Publishers Terms of Service found at https://www.quantcast.com/terms/measure-terms-service/ (the "**Measure Terms**"), and, solely for purposes of the Measure Terms, the Solution shall collectively be deemed to be a component of the Services (as defined in the Measure Terms).

b. **Quantcast Obligations and Representations.** Quantcast agrees, represents, and warrants to Customer that the Solution is compatible and compliant with the IAB Privacy Frameworks.

c. **Customer's Obligations and Representations.** Customer agrees, represents and warrants to Quantcast that Customer:

(i) has all rights, approvals, and consents necessary to implement the Solution on webpages, apps, or other digital applications;

(ii) will implement the Choice Tag only as described in the Quantcast Choice Technical Guide provided by Quantcast and the terms and conditions of this Agreement and update the Choice Tag when Quantcast notifies Customer of any fixes, updates, and upgrades;

(iii) will not interfere or attempt to interfere with the operational features of the Solution;

(iv) will not delete, or in any manner alter, the copyright, trademark, or other proprietary rights notices appearing on the Solution; and

(v) will not modify, reverse engineer, download, host on Customer's own servers, disassemble, decompile, license, or sublicense the Solution to any third parties or otherwise use the Solution, including the Quantcast Choice Technical Guide or other corresponding instruction manuals and documentation, to develop or assist in developing a product or service competitive with the Solution.

3. Indemnity. Customer agrees to defend, indemnify, and hold Quantcast harmless from any judgments, damages, loss, liability, fines, or costs (including reasonable attorneys' fees) resulting from Customer's breach of a term of this Agreement or Customer's use of the Solution if not in compliance with the terms of the Agreement. Quantcast will have no obligation or liability hereunder where the claim results from any combination with, addition to, or modification of the Choice Tag. Where pursuant to Article 82(4) of the GDPR, Quantcast is found to be liable for the entire damage arising from a breach or breaches of the GDPR relating to activities under this Agreement, in order to ensure effective compensation of one or more individuals, then Customer shall indemnify Quantcast for all claims, demands, loss, damages, or expenses (including reasonable attorneys' fees) relating to any breaches of GDPR for which Customer is wholly or partly responsible. All compensation paid to a data subject pursuant to Article 82(4) of the GDPR by Quantcast which is wholly or partly attributable to GDPR breaches by Customer shall be repaid pursuant to this indemnity and Article 82(5) immediately on receipt of a written request from Quantcast pursuant to this Section 3.

4. Warranty Disclaimer. The Solution provided "as is" without warranty or condition of any kind, either express or implied. Without limiting the foregoing, Quantcast explicitly disclaims any warranties of merchantability, fitness for a particular purpose, quiet enjoyment, or non-infringement. Quantcast assumes no liability on behalf of Customer, any of Customer's third party vendors, or any other entities for acting or not acting on Choice Signals, or if Customer or any of Customer's third party vendors or any other entities bypass or otherwise interfere with the technical restrictions included in the Solution as provided by Quantcast. Quantcast makes no warranty that the Solution, including the Choice Tag, will (a) be available on an uninterrupted, secure, or error-free basis, (b) not cause any latency or processing delays, or (c) meets any legal requirements around consent or data protection. Quantcast assumes no liability for Customer's reliance on the Solution. The foregoing exclusions and disclaimers are an essential part of this Agreement and formed a basis for enabling Quantcast to offer the Solution to Customer. Some jurisdictions do not allow exclusion of certain warranties so this disclaimer may not apply to Customer in full.

5. Termination. Unless otherwise terminated as set forth herein, this Agreement will remain in full force and effect while Customer uses the Solution. Customer may terminate this Agreement by removing the Choice Tag from Customer's websites or apps, as applicable, or notifying Quantcast of Customer's termination of this Agreement at any time in writing. Quantcast may terminate access to the Solution or terminate this Agreement at any time, for any reason or no reason and without any liability to Customer. Quantcast

will not be liable to Customer or any third party for termination of this Agreement. Notwithstanding the above, Sections 3 and 7 to 10 will survive termination.

6. Modification of the Agreement. Quantcast reserves the right, in its sole discretion, to modify or discontinue the Solution without notice. Quantcast may also modify this Agreement from time to time. If the modified Agreement is not acceptable to Customer, Customer may terminate Customer's account within 30 days by following the procedure in Section 5. Use of the Solution, after 30 days, will constitute Customer's acceptance thereof.

7. Limitation on Liability. IN NO EVENT WILL QUANTCAST BE LIABLE TO CUSTOMER OR ANY THIRD PARTY FOR ANY CONSEQUENTIAL LOSS, EXEMPLARY DAMAGE, INCIDENTAL LOSS, SPECIAL DAMAGE OR LOSS, LOST PROFIT, OR PUNITIVE DAMAGES ARISING FROM CUSTOMER'S USE OF THE SOLUTION, EVEN IF QUANTCAST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THESE LIMITATIONS FORMED A BASIS FOR ENABLING QUANTCAST TO OFFER THE SOLUTION TO CUSTOMER. THIS PARAGRAPH WILL APPLY REGARDLESS OF ANY FAILURE OF THE EXCLUSIVE REMEDY PROVIDED IN THE FOLLOWING PARAGRAPH. EXCEPT WITH REGARD TO LIABILITY STEMMING FROM DEATH OR PERSONAL INJURY RESULTING FROM QUANTCAST'S NEGLIGENCE, OR QUANTCAST'S FRAUD, NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED HEREIN, QUANTCAST'S LIABILITY TO CUSTOMER FOR ANY CAUSE WHATSOEVER AND REGARDLESS OF THE FORM OF THE ACTION WILL AT ALL TIMES BE LIMITED TO TWO HUNDRED FIFTY DOLLARS (U.S. $250.00).

8. Notices. All notices or other communications to Quantcast from Customer will be deemed given only when received by hand delivery, electronic mail, or prepaid first class mail, at the address below or any other address provided by Quantcast to Customer for these purposes, with attention to the Legal Department.

Persons in the United States, please contact:

Quantcast Corp.
795 Folsom Street
San Francisco, CA 94107
Attn: Legal Department
Email: contact@quantcast.com

Persons outside of the United States, please contact:

Quantcast International Limited
Beaux Lane House
Lower Mercer Street, 1st Floor
Dublin 2, Ireland
Attn: Legal Department
Email: contact.dublin@quantcast.com

9. Miscellaneous. This Agreement constitutes the entire Agreement between the parties with respect to the Solution and supersedes all previous and contemporaneous agreements, proposals, and communications, written or oral, between Quantcast and Customer with respect thereto. Any waiver by either party of any violation of this Agreement will not be deemed to waive any further or future violation of the same or any other provision. If any parts or provisions of this Agreement are held to be unenforceable, then Customer and Quantcast agree that such parts or provisions will be given maximum permissible force and effect and the remainder of the Agreement will be fully enforceable. Customer and Quantcast agree that there are no third party beneficiaries of any promises, obligations, or representations made by Quantcast. Either party may assign its rights, data, and duties, under this Agreement in their entirety in connection with a sale of all (or substantially all) of its assets relating to this Agreement, a merger, or a reorganization. Nothing in this Agreement will constitute a partnership or joint venture between Customer and Quantcast. This Agreement is drafted in the English language. Any translation into another language is provided for convenience only. In the event of any inconsistency between the English language version and any translation, the English language version shall prevail.

10. Contracting Party; Choice of Law and Venue. If Customer resides in the United States, this Agreement is between Customer and Quantcast Corporation (a Delaware corporation), this Agreement and any dispute relating to this Agreement will be governed by the laws of California, and Customer and Quantcast Corporation consent and agree that jurisdiction, proper venue, and the most

convenient forum for all claims, actions, and proceedings of any kind relating to this Agreement will be exclusively in courts located in San Francisco, California. If Customer resides outside of the United States, this Agreement is between Customer and Quantcast International Limited (an Irish limited liability company), this Agreement and any dispute relating to this Agreement will be governed by the laws of Ireland, and Customer and Quantcast International Limited consent and agree that jurisdiction, proper venue, and the most convenient forum for all claims, actions, and proceedings of any kind relating to this Agreement will be exclusively in courts located in Dublin, Ireland. References in this Agreement to “Quantcast”, “us”, “we,” and “our” mean either Quantcast Corporation or Quantcast International Limited, as appropriate.

Appendix 1: Quantcast Choice Processing Terms

Quantcast and Customer have entered into the Agreement for the provision of the Quantcast Choice Basic Services.

These Quantcast Choice Processing Terms (including Appendices 2 through 4, "**Data Processing Terms**") are entered into by Quantcast and Customer and supplement the Agreement. These Data Processing Terms will be effective, and replace any previously applicable terms relating to their subject matter (including any data processing amendment or data processing addendum relating to Quantcast Choice), from the Terms Effective Date.

1. Introduction

These Data Processing Terms reflect the parties' agreement on the terms governing the processing of certain data in connection with European Data Protection Law and certain Non-European Data Protection Law.

2. Definitions and Interpretation

2.1 In these Data Processing Terms:

"**Additional Product or Service**" means a product, product functionality service, or application provided by Quantcast or a third party that: (a) is not part of the Quantcast Choice Basic Services; and (b) is accessible for use within the Quantcast Choice user portal or is otherwise integrated or used in conjunction with the Quantcast Choice Basic Services, including, without limitation, Quantcast Choice Additional Services, Quantcast Measure, Q for Publishers, Quantcast Advertise, and Q for Marketers.

"**Additional Terms for Non-European Data Protection Law**" means the additional terms referred to in Appendix 4, which reflect the parties' agreement on the terms governing the processing of certain data in connection with certain Non-European Data Protection Laws.

"**Affiliate**" means an entity that directly or indirectly controls, is controlled by, or is under common control with, a party.

"**CCPA**" means Title 1.81.5 of the California Civil Code.

"**Customer Personal Data**" means personal data that is processed by Quantcast on behalf of Customer in Quantcast's provision of the Quantcast Choice Basic Services.

"**Data Incident**" means a breach of Quantcast's security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data on systems managed by or otherwise controlled by Quantcast. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"**Data Subject Rights Tool**" means a tool (if any) made available by Quantcast to data subjects that enables Quantcast to respond directly and in a standardised manner to certain requests from data subjects in relation to Customer Personal Data.

"**EEA**" means the European Economic Area.

"**EU 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.

"**European Data Protection Law**" means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

"**European or National Laws**" means, as applicable: (a) EU or EU Member State law (if the EU GDPR applies to the processing of Customer Personal Data); and/or (b) the law of the UK or a part of the UK (if the UK GDPR applies to the processing of Customer Personal Data).

"**GDPR**" means, as applicable: (a) the EU GDPR; and/or (b) the UK GDPR.

"**Quantcast**" means the Quantcast Entity that is party to the Agreement.

"**Quantcast Affiliate Subprocessors**" has the meaning given in Section 11.1 (Authorization for Subprocessor Engagement).

"**Quantcast Entity**" means Quantcast Corporation or Quantcast International Limited, as applicable.

"**Non-European Data Protection Law**" means data protection or privacy laws in force outside the EEA, Switzerland and the UK.

"**Notification Email Address**" means the email used to create the account with which Customer accesses the Quantcast Choice user portal, and/or the email address (if any) designated by Customer, via the Quantcast Choice user portal or such other means provided by Quantcast, to receive certain notifications from Quantcast relating to these Data Processing Terms.

"**Standard Contractual Clauses**" means the standard clauses adopted by the European Commission for the lawful transfer of personal data from the EEA to jurisdictions that have not been deemed to provide an adequate level of data protection by the European Commission, and any equivalent transfer mechanism that may apply in the UK.

"**Quantcast Choice Basic Services**" means the applicable services listed here.

"**Security Measures**" has the meaning given in Section 7.1.1 (Quantcast's Security Measures).

"**Subprocessors**" means third parties authorised under these Data Processing Terms to have logical access to and process Customer Personal Data in order to provide parts of the Quantcast Choice Basic Services and any related technical support.

"**Supervisory Authority**" means, as applicable: (a) a "supervisory authority" as defined in the EU GDPR; and/or (b) the "Commissioner" as defined in the UK GDPR.

"**Term**" means the period from the Terms Effective Date until the end of Quantcast's provision of the Quantcast Choice Basic Services under the Agreement.

"**Terms Effective Date**" means, the date on which Customer accepted the Agreement or the parties otherwise agreed to these Data Processing Terms.

"**Third Party Subprocessors**" has the meaning given in Section 11.1 (Authorization for Subprocessor Engagement).

"**UK GDPR**" means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, if in force.

2.2 The terms "controller", "data subject", "personal data", "processing" and "processor" as used in these Data Processing Terms have the meanings given in the GDPR.

2.3 The words "include" and "including" mean "including but not limited to". Any examples in these Data Processing Terms are illustrative and not the sole examples of a particular concept.

2.4 Any reference to a legal framework, statute or other legislative enactment is a reference to it as amended or re-enacted from time to time.

2.5 If these Data Processing Terms are translated into any other language, and there is a discrepancy between the English text and the translated text, the English text will govern.

3. Duration of these Data Processing Terms

These Data Processing Terms will take effect on the Terms Effective Date and, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon, deletion of all Customer Personal Data by Quantcast as described in these Data Processing Terms.

4. Application of these Data Processing Terms

4.1 Application of European Data Protection Law.

Sections 5 (Processing of Data) to 12 (Contacting Quantcast; Processing Records) (inclusive) will only apply to the extent that European Data Protection Law applies to the processing of Customer Personal Data, including if:

(a) the processing is in the context of the activities of an establishment of Customer in the EEA or the UK; and/or

(b) Customer Personal Data is personal data relating to data subjects who are in the EEA or the UK and the processing relates to the offering to them of goods or services or the monitoring of their behaviour in the EEA or the UK.

4.2 Application to Quantcast Choice Basic Services.

These Data Processing Terms will only apply to the Quantcast Choice Basic Services for which the parties agreed to these Data Processing Terms.

4.3 Incorporation of Additional Terms for Non-European Data Protection Law.

The Additional Terms for Non-European Data Protection Legislation supplement these Data Processing Terms.

5. Processing of Data

5.1 Roles and Regulatory Compliance; Authorisation.

5.1.1 Processor and Controller Responsibilities. The parties acknowledge and agree that:

(a) Appendix 2 describes the subject matter and details of the processing of Customer Personal Data;

(b) Quantcast is a processor of Customer Personal Data under European Data Protection Law;

(c) Customer is a controller or processor, as applicable, of Customer Personal Data under European Data Protection Law; and

(d) each party will comply with the obligations applicable to it under European Data Protection Law with respect to the processing of Customer Personal Data.

5.1.2 Authorisation by Third Party Controller. If Customer is a processor, Customer warrants to Quantcast that Customer's instructions and actions with respect to Customer Personal Data, including its appointment of Quantcast as another processor, have been authorised by the relevant controller.

5.2 Customer's Instructions.

By entering into these Data Processing Terms, Customer instructs Quantcast to process Customer Personal Data only in accordance with applicable law:

(a) to provide the Quantcast Choice Basic Services and any related technical support;

(b) as further specified via Customer's use of the Quantcast Choice Basic Services (including in the settings and other functionality of the Quantcast Choice Basic) and any related technical support;

(c) as documented in the form of the Agreement, including these Data Processing Terms; and

(d) as further documented in any other written instructions given by Customer and acknowledged by Quantcast as constituting instructions for purposes of these Data Processing Terms.

5.3 Quantcast's Compliance with Instructions.

Quantcast will comply with the instructions described in Section 5.2 (Customer's Instructions) (including with regard to data transfers) unless European or National Laws to which Quantcast is subject require other processing of Customer Personal Data by Quantcast, in which case Quantcast will inform Customer (unless any such law prohibits Quantcast from doing so on important grounds of public interest).

5.4 Additional Product or Services.

If Customer uses any Additional Product or Service, the Quantcast Choice Basic Services may allow that Additional Product or Service to access Customer Personal Data as required for the interoperation of the Additional Product or Service with the Quantcast Choice Basic Services. For clarity, these Data Processing Terms do not apply to the processing of personal data in connection with the

provision of any Additional Product or Service used by Customer, including personal data transmitted to or from that Additional Product or Service.

6. Data Deletion

6.1 Deletion During Term.

6.1.1 During the Term Quantcast will comply with:

(a) any reasonable request from Customer to facilitate such deletion, insofar as this is possible taking into account the nature and functionality of the Quantcast Choice Basic Services and unless European or National Laws require storage; and

(b) the data retention practices described at www.quantcast.com/privacy.

Quantcast may charge a fee (based on Quantcast's reasonable costs) for any data deletion under Section 6.1.1. Quantcast will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such data deletion.

6.2 Deletion on Term Expiry.

On expiry of the Term, Customer instructs Quantcast to delete all Customer Personal Data (including existing copies) from Quantcast's systems in accordance with applicable law. Quantcast will comply with this instruction as soon as reasonably practicable and within a maximum period of 13 months, unless European or National Laws require storage.

7. Data Security

7.1 Quantcast's Security Measures and Assistance.

7.1.1 Quantcast's Security Measures. Quantcast will implement and maintain technical and organisational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access as described in Appendix 3 (the "Security Measures"). As described in Appendix 3, the Security Measures include measures:

(a) to encrypt personal data;

(b) to help ensure the ongoing confidentiality, integrity, availability and resilience of Quantcast's systems and services;

(c) to help restore timely access to personal data following an incident; and

(d) for regular testing of effectiveness.

Quantcast may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Quantcast Choice Basic Services.

7.1.2 Security Compliance by Quantcast Staff. Quantcast will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorised to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.2 Data Incidents.

7.2.1 Incident Notification. If Quantcast becomes aware of a Data Incident, Quantcast will:

(a) notify Customer of the Data Incident promptly and without undue delay; and

(b) promptly take reasonable steps to minimise harm and secure Customer Personal Data.

7.2.2 Details of Data Incident. Notifications made under Section 7.2.1 (Incident Notification) will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps Quantcast recommends Customer take to address the Data Incident.

7.2.3 Delivery of Notification. Quantcast will deliver its notification of any Data Incident to the Notification Email Address or, at

Quantcast's discretion (including if Customer has not provided a Notification Email Address), by other direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for providing the Notification Email Address and ensuring that the Notification Email Address is current and valid.

7.2.4 Third Party Notifications. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Data Incident.

7.2.5 No Acknowledgement of Fault by Quantcast. Quantcast's notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Quantcast of any fault or liability with respect to the Data Incident.

7.3 Customer's Security Responsibilities and Assessment.

7.3.1 Customer's Security Responsibilities. Customer agrees that, without prejudice to Quantcast's obligations under Sections 7.1 (Quantcast's Security Measures and Assistance) and 7.2 (Data Incidents):

(a) Customer is solely responsible for its use of the Quantcast Choice Basic Services, including:

(i) making appropriate use of the Quantcast Choice Basic Services to ensure a level of security appropriate to the risk in respect of Customer Personal Data; and

(ii) securing the account authentication credentials, systems and devices Customer uses to access the Quantcast Choice Basic Services; and

(b) Quantcast has no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of Quantcast's and its Subprocessors' systems.

7.3.2 Customer's Security Assessment. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by Quantcast as set out in Section 7.1.1 (Quantcast's Security Measures) provide a level of security appropriate to the risk in respect of Customer Personal Data.

7.4 Reviews and Audits of Compliance.

Reviews of security documentation. To demonstrate compliance by Quantcast with its obligations under these Data Processing Terms, Quantcast will make security documentation available for review by Customer.

8. Impact Assessments and Consultations

Customer agrees that Quantcast will (taking into account the nature of the processing and the information available to Quantcast) assist Customer in ensuring compliance with any obligations of Customer in respect of data protection impact assessments and prior consultation, including (if applicable) Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by:

(a) providing security documentation in accordance with Section 7.4 (Reviews of security documentation);

(b) providing the information contained in these Data Processing Terms; and

(c) providing or otherwise making available, in accordance with Quantcast's standard practices, other materials concerning the nature of the Quantcast Choice Basic Services and the processing of Customer Personal Data.

9. Data Subject Rights

9.1 Responses to Data Subject Requests.

If Quantcast receives a request from a data subject in relation to Customer Personal Data, Quantcast will:

(a) if the request is made via a Data Subject Rights Tool, or if the request does not name Customer, respond directly to the data subject's request in accordance with the standard functionality of that Data Subject Rights Tool or Quantcast standard practice; or

(b) if the request is not made via a Data Subject Rights Tool and the request names Customer, advise the data subject to submit

his/her request to Customer, and Customer will be responsible for responding to such request.

9.2 Quantcast's Data Subject Request Assistance.

Customer agrees that Quantcast will (taking into account the nature of the processing of Customer Personal Data and, if applicable, Article 11 of the GDPR) assist Customer in fulfilling any obligation of Customer to respond to requests by data subjects, including (if applicable) Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by:

(a) providing the functionality of the Quantcast Choice Basic Services;

(b) complying with the commitments set out in Section 9.1 (Responses to Data Subject Requests); and

(c) if applicable to the Quantcast Choice Basic Services, making available Data Subject Rights Tools.

10. Data Transfers

10.1 Data Storage and Processing Facilities.

Customer agrees that Quantcast may, subject to Section 10.2 (Transfers of Data), store and process Customer Personal Data in the United States of America and any other country in which Quantcast or any of its Subprocessors maintains facilities.

10.2 Transfers of Data.

Quantcast will ensure that any transfers of personal data between jurisdictions between Quantcast Entities and/or Subprocessors is lawful, for example by entering into Standard Contractual Clauses.

11. Subprocessors

11.1 Authorization for Subprocessor Engagement.

Customer specifically authorises the engagement of Quantcast's Affiliates as Subprocessors ("Quantcast Affiliate Subprocessors"). In addition, Customer generally authorises the engagement of any other third parties as Subprocessors ("Third Party Subprocessors").

11.2 Information about Subprocessors.

Information about Third Party Subprocessors is available at www.quantcast.com/privacy/quantcast-partners/. Quantcast will update the information included when any new Third Party Subprocessor is engaged.

11.3 Requirements for Subprocessor Engagement.

When engaging any Subprocessor, Quantcast will:

(a) ensure via a written contract that:

(i) the Subprocessor only accesses and uses Customer Personal Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including these Data Processing Terms); and

(ii) if the GDPR applies to the processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR are imposed on the Subprocessor; and

(b) remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

11.4 Opportunity to Object to Subprocessor Changes.

When any new Third Party Subprocessor is engaged during the Term by Quantcast, Customer may object to any new Third Party Subprocessor by terminating the Agreement immediately upon written notice to Quantcast. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Third Party Subprocessor.

12. Contacting Quantcast; Processing Records

12.1 Contacting Quantcast.

Customer may contact Quantcast in relation to the exercise of its rights under these Data Processing Terms via contact@quantcast.com (for persons in the United States) or contact.dublin@quantcast.com (for other persons), or via such other means as may be provided by Quantcast from time to time.

12.2 Quantcast's Processing Records.

Customer acknowledges that Quantcast is required under the GDPR to:

(a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which Quantcast is acting and (if applicable) of such processor's or controller's local representative and data protection officer; and

(b) make such information available to any Supervisory Authority.

Accordingly, Customer will, where requested and as applicable to Customer, provide such information to Quantcast via the Quantcast Choice user portal or via such other means as may be provided by Quantcast, and will use such user portal or other means to ensure that all information provided is kept accurate and up-to-date.

13. Liability

The liability provisions in the Agreement apply equally to these Data Processing Terms.

14. Effect of these Data Processing Terms

If there is any conflict or inconsistency between the terms of the Additional Terms for Non-European Data Protection Law, the remainder of these Data Processing Terms and/or the remainder of the Agreement, then the following order of precedence will apply:

(a) the Additional Terms for Non-European Data Protection Law;

(b) the remainder of these Data Processing Terms; and

(c) the remainder of the Agreement.

Subject to the amendments in these Data Processing Terms, the Agreement remains in full force and effect.

Appendix 2: Subject Matter and Details of the Data Processing

Subject Matter

Quantcast's provision of the Quantcast Choice Basic Services and any related technical support to Customer.

Duration of the Processing

The Term plus the period from expiry of the Term until deletion of all Customer Personal Data by Quantcast in accordance with these Data Processing Terms.

Nature and Purpose of the Processing

Quantcast will process (including, as applicable to the Quantcast Choice Basic Services and the instructions described in Section 5.2 (Customer's Instructions), collecting, recording, organising, structuring, storing, altering, retrieving, using, disclosing, combining, erasing and destroying) Customer Personal Data for the purpose of providing the Quantcast Choice Basic Services and any related technical support to Customer in accordance with these Data Processing Terms.

Types of Personal Data

Customer Personal Data may include the types of personal data described www.quantcast.com/privacy.

Categories of Data Subjects

Customer Personal Data will concern the following categories of data subjects:

- data subjects about whom Quantcast collects personal data in its provision of the Quantcast Choice Basic Services; and/or
- data subjects about whom personal data is transferred to Quantcast in connection with the Quantcast Choice Basic Services by, at the direction of, or on behalf of Customer.

Data subjects may include individuals who have visited specific websites or applications in respect of which Quantcast provides the Quantcast Choice Basic Services; and/or (c) users who access the Quantcast Choice user portal.

Appendix 3: Security Measures

As from the Terms Effective Date, Quantcast will implement and maintain the Security Measures set out in this Appendix 3. Quantcast may update or modify such Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Quantcast Choice Basic Services.

1. Data Centre & Network Security

(a) Data Centres.

Infrastructure. Quantcast maintains geographically distributed data centres. Quantcast stores all production data in physically secure data centres.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimise the impact of anticipated environmental risks. Dual circuits, switches, routers or other necessary network devices help provide this redundancy. The Quantcast Choice Basic Services are designed to allow Quantcast to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data centre equipment is scheduled through a standard process according to documented procedures.

Power. The data centre electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data centre. Backup power is provided by various mechanisms such as uninterruptible power supply (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data centre, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data centre at full capacity typically for a period of days.

Server Operating Systems. Quantcast servers use hardened operating systems which are customised for the unique server needs of the business. Data is stored using proprietary algorithms to augment data security and redundancy. Quantcast employs a code review process to increase the security of the code used to provide the Quantcast Choice Basic Services and enhance the security products in production environments.

Businesses Continuity. Quantcast replicates data over multiple systems to help to protect against accidental destruction or loss. Quantcast has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) Networks & Transmission.

Data Transmission. Data centres are typically connected via high-speed private links to provide secure and fast data transfer between data centres. This is designed to prevent data from being read, copied, altered or removed without authorisation during electronic transfer or transport or while being recorded onto data storage media. Quantcast transfers data via industry standard network protocols.

External Attack Surface. Quantcast employs multiple layers of network devices and intrusion detection to protect its external attack surface. Quantcast considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Quantcast’s intrusion detection involves:

1. Tightly controlling the size and make-up of Quantcast’s attack surface through preventative measures;

2. Employing intelligent detection controls at data entry points; and

3. Employing technologies that automatically remedy certain dangerous situations.

Incident Response. Quantcast monitors a variety of communication channels for security incidents, and Quantcast's security personnel will react promptly to known incidents.

Encryption Technologies. Quantcast makes HTTPS encryption (also referred to as SSL or TLS connection) available. Quantcast servers support ephemeral elliptic curve Diffie Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimise the impact of a compromised key, or a cryptographic breakthrough.

2. Access and Site Controls

(a) Site Controls.

On-site Data Centre Security Operation. Quantcast's data centres maintain an on-site security operation responsible for all physical data centre security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor Closed Circuit TV ("CCTV") cameras and all alarm systems. On-site security operation personnel perform internal and external patrols of the data centre regularly.

Data Centre Access Procedures. Quantcast maintains formal access procedures for allowing physical access to the data centres. The data centres are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data centre are required to identify themselves as well as show proof of identity to on-site security operations. Only authorised employees, contractors and visitors are allowed entry to the data centres. Only authorised employees and contractors are permitted to request electronic card key access to these facilities. Data centre electronic card key access requests must be made in advance and in writing, and require the approval of the requestor's manager and the data centre director. All other entrants requiring temporary data centre access must: (i) obtain approval in advance from the data centre managers for the specific data centre and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data centre access record identifying the individual as approved.

On-site Data Centre Security Devices. Quantcast's data centres employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorised activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorised access throughout the business operations and data centres is restricted based on zones and the individual's job responsibilities. The fire doors at the data centres are alarmed. CCTV cameras are in operation both inside and outside the data centres. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data centre building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centres connect the CCTV equipment. Cameras record on-site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for at least 7 days based on activity.

(b) Access Control.

Infrastructure Security Personnel. Quantcast has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Quantcast's infrastructure security personnel are responsible for the ongoing monitoring of Quantcast's security infrastructure, the review of the Quantcast Choice Basic Services, and responding to security incidents.

Access Control and Privilege Management. Customer's administrators and users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Quantcast Choice Basic Services.

Internal Data Access Processes and Policies – Access Policy. Quantcast's internal data access processes and policies are designed to prevent unauthorised persons and/or systems from gaining access to systems used to process personal data. Quantcast aims to design its systems to: (i) only allow authorised persons to access data they are authorised to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after recording. The systems are designed to detect any inappropriate access. Quantcast employs a centralised access management system to control personnel access to production servers, and only provides access to a limited number of authorised personnel. LDAP, Kerberos and a proprietary system utilising SSH certificates are designed to provide Quantcast with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Quantcast requires the use of

unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimise the potential for unauthorised account use. The granting or modification of access rights is based on: the authorised personnel's job responsibilities; job duty requirements necessary to perform authorised tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Quantcast's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g. login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength.

3. Data

(a) Data Storage, Isolation & Authentication.

Quantcast stores data in a multi-tenant cloud environment. Data, the Quantcast Choice Basic Services database and file system architecture are replicated between multiple geographically dispersed data centres. Quantcast logically isolates each customer's data. A central authentication system is used across all Quantcast Choice Basic Services to increase uniform security of data.

(b) Decommissioned Disks and Disk Destruction Guidelines.

Data Destruction: Content on drives is treated at the highest level of classification. Content is destroyed on storage devices as part of the decommissioning process in accordance with industry security standards. Where cloud servers are hosted by third parties, they are securely wiped or overwritten prior to provisioning for reuse. Any media is securely wiped or degaussed and physically destroyed prior to leaving physical or logical secure boundaries. To validate secure wipe processes and procedures, third party auditors review the guidance within the applicable media protection policy, observe degaussing equipment and secure shred bins located within physical facilities, observe historical tickets which tracked the destruction of a hard drive within a data center and the process of a device being wiped and removed from the environment.

Data Deletion for block device based storage (SSD, HDD, ephemeral drives, etc.): In order to ensure that customer content is properly erased, Quantcast ensures that underlying storage media is wiped upon re-provisioning rather than upon de-provisioning. Processes that wipe content upon release of an asset (volume, object, etc.) are less reliable than processes that only re-provision clean storage to customers. Physical servers can reboot at any time for many reasons (power outage, system process interruption or failure, etc.), which might leave a wiping procedure in an incomplete state.

4. Personnel Security

Quantcast personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Quantcast conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Quantcast's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Personal Data are required to complete additional requirements appropriate to their role. Quantcast's personnel will not process Customer Personal Data without authorisation.

5. Subprocessor Security

Before onboarding Subprocessors, Quantcast conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Quantcast has assessed the risks presented by the Subprocessor then, subject always to the requirements set out in Section 11.3 (Requirements for Subprocessor Engagement), the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

Appendix 4: Additional Terms for Non-European Data Protection Legislation

1. CCPA. Quantcast may offer and Customer may enable certain in-product settings, configurations or other functionality for the Quantcast Choice Basic Services. Subject to the terms of this Addendum and solely with respect to Customer Personal Information processed for the Quantcast Choice Basic Services, excluding any Additional Product or Service, Quantcast will act as Customer's service provider, and as such, will not retain, use or disclose Customer Personal Information, other than (a) for a business purpose under the CCPA on behalf of Customer and the specific purpose of performing the Quantcast Choice Basic Services, as updated from time to time, or as otherwise permitted under the CCPA or (b) as may otherwise be permitted for service providers or under a comparable exemption from "sale" in the CCPA.

The provisions of this section are effective solely to the extent the CCPA applies. Customer is solely liable for its compliance with the CCPA in its use of the Quantcast Choice Basic Services. In addition to Section 6 of the Agreement, in the event of changes to the CCPA or issuance of any applicable regulation or court order or governmental guidance relating to the CCPA, Quantcast may change this section, if such change does not have a material adverse impact on Customer, as reasonably determined by Quantcast, with respect to exemptions from "sales" under the CCPA. The terms "business purpose", "personal information", "sale" and "service provider" as used in this section have the meanings given in the CCPA. "Customer Personal Information" means personal information that is processed by Quantcast on behalf of Customer in Quantcast's provision of the Quantcast Choice Basic Services. If there is any conflict or inconsistency between the terms of this section and the remainder of the Agreement (including the Quantcast Choice Data Processing Terms), the terms of this section will govern.