Last Update: May 16, 2023

This Privacy Implementation for Quantcast Advertiser Partners documents certain privacy-related responsibilities for advertisers and agencies, which are in addition to the US State Data Privacy Addendum and the EEA/UK/Swiss Data Privacy Addendum (collectively, the "DPAs"). If there is any conflict between this document and the DPAs, the DPAs are the controlling documents.

Privacy regulation around the world is dynamic. Quantcast may update this document from time to time at its own discretion in order to keep pace with changes in privacy rules and risks, and industry best practices, as well as to ensure users' rights are honored appropriately.

Quantcast may take reasonable measures to ensure that data processed in its services is collected and processed in accordance with privacy rules and industry best practices. We may review locations where data is collected and may refuse to accept data that is not collected in a manner consistent with the approaches described in this document.

Terminology

This document uses "user" or "users" as interchangeable with "data subject" or "consumer" or other equivalent terms from various rules.

When we say rules, we mean laws, regulations, and industry self-regulatory codes that are applicable to the processing of personal data in relation to Quantcast's services. Quantcast has a global footprint, including operations in the EU, the UK, and the US (including California), so those jurisdictions' rules are applicable to Quantcast for data about users who reside in those jurisdictions.

We also will use "personal data" as interchangeable with terms such as, "personal information." Personal data processed by Quantcast's service is pseudonymous, including but not limited to IP address, cookie or device IDs, and other identifiers used for advertising-related purposes. In the case where a partner has express permission from Quantcast to use email address, phone number, or other directly identifying information, such information will be pseudonymized (usually hashed or encrypted,) according to Quantcast specifications, before transmitting to Quantcast.

Industry standards and self-regulatory programs

Quantcast supports and participates in industry self-regulatory programs, and generally implements industry standards and best practices when it comes to handling personal data. Partners and clients are responsible for ensuring their own implementation of self-regulatory rules and industry best practices, in particular related to providing transparency and choice to users in places where data is collected or used by Quantcast's services.

Controller, processor, service provider, vendor, etc.

Unfortunately, terms describing the relationships between parties sharing data are not interchangeable. Quantcast determines its role based on applicable law and the facts of its processing of personal data. In many relationships with advertiser partners or clients, Quantcast is a controller or joint controller, because of the role that Quantcast plays in defining exactly how data is used. This does not mean Quantcast has unfettered rights to use this data; rather, Quantcast's use of the data is usually restricted by contractual limitations. If you have questions about this, please consult your agreement or ask your account representative.

Advertisers: Where the EU GDPR or the UK GDPR applies, Quantcast is a joint controller of personal data collected using Quantcast tags and pixels and of other personal data introduced into Quantcast's services by the advertiser. Where US state privacy law applies, Quantcast acts as a "third party."

Notice/Transparency and Choice

Laws, self-regulatory rules, and industry best practice require users be notified about processing of personal data, and be offered a choice – either opt in or opt out — with respect to that processing.

When deploying Quantcast tags or pixels, or otherwise introducing data into Quantcast's services, partners and clients are responsible

to make sure that users are given notice and choice that is required for Quantcast to be able to collect and process the data. And, of course, partners and clients have to make sure of notice and choice for their own personal data collection and processing.

Generally, notice must include the fact that third parties are collecting and processing users' data, along with information about the data collected, the means of collection, the purposes for processing (including interest-based advertising), and how users can exercise their choices. Laws or rules in some jurisdictions would require that Quantcast be specifically identified in the notice and a link to Quantcast's privacy policy be included.

Quantcast's methods of collection include, depending on particular circumstances, cookies, pixels, JavaScript tags, probabilistic device matching and cross-device matching (using passively collected data).

Quantcast implements choice using industry standard methods and will be responsible for honoring that choice with respect to personal data within Quantcast's services.

For their part, partners and clients need to provide access to the choice using industry standard and legally compliant methods, depending on the applicable laws and rules. Usually this means providing access to choose within other privacy disclosures, including in a privacy policy.

In all cases, partners and clients should have user-facing privacy policies that are prominently linked from their homepages and from content (sites, apps, etc.) where personal data are collected or used.

Privacy policies will adhere to applicable laws, as well as industry self-regulatory requirements and industry best practices. At minimum, policies should disclose the fact that third parties are collecting personal data for advertising-related purposes, and should describe the methods of collection, as described above. Particular circumstances and applicable rules may create additional requirements.

Where consent (opt-in) is required prior to setting cookies or collecting data, such as in Europe under ePrivacy, the GDPR, and the UK GDPR, partners and clients are responsible to make sure that tags or pixels don't fire until that consent is obtained.

EU and the UK: The industry standard means for ensuring notice and choice for vendors like Quantcast in the EU and the UK is the IAB Europe Transparency and Consent Framework. Quantcast is vendor ID 11. Quantcast's required purposes and associated legal bases are viewable in the Global Vendor List. Because Quantcast is subject to European law, the TCF should be used for all users in the EU or the UK, even if the client or partner has no operations in Europe. Alternatively, such partners and clients may elect not to introduce data about EU or UK users into Quantcast's services. Quantcast Choice is a leading, and TCF compliant, Consent Management Platform. Proper use of Quantcast Choice will meet these requirements.

Partners and clients not using the TCF for EU or UK users need to use a legally compliant alternative means to ensure Quantcast's legal basis for using cookies, where applicable, and for processing the data. This includes that Quantcast must be identified as a controller of the user's personal data, and a link to Quantcast's privacy policy must be provided. Quantcast may in the future require TCF.

Privacy policies in the EU and the UK need to include a link to the European Interactive Digital Advertising Alliance (EDAA) opt out page, located at youronlinechoices.com.

US: In the US, along with other requirements laid out here, privacy policies need to include links to an industry standard opt out page, like those offered by the NAI or DAA.

California: The CCPA applies for users in California. Partners and clients need to provide users with notice of their "sale" and "share" opt-out rights and the ability to exercise such rights, as applicable.

Other US states: Applicable state privacy law applies for users in Colorado, Connecticut, Utah, and Virginia. Partners and clients need to provide users with notice of their "sale" and "targeted advertising" opt-out rights and the ability to exercise such rights, as applicable.

US State Privacy Addendum: The processing of US users' personal data in connection with Quantcast's services shall be governed by the US State Privacy Addendum, which is available here.

Access and Deletion

Under applicable law, including the EU GDPR, the UK GDPR, and the US state privacy laws, as a joint controller or third party, Quantcast will be responsible for providing users access to their personal data that is within Quantcast's services, and for deleting personal data after it receives (or is notified of) a user's request.

Other Matters

Sensitive data. Because Quantcast's services are not intended for processing data regarded as "sensitive" or "special category" under applicable law or data about children under the age of 16, partners and clients must not transmit to Quantcast or cause Quantcast to collect any such data. Quantcast tags and pixels may not be deployed on content that is directed at children under the age of 16. Sensitive or special category data includes the types of data listed in Article 9 of the EU GDPR, Section 1798.140 of the CCPA (as amended by the CPRA), or any equivalent term under applicable law.

Directly identifying personal data. Quantcast's services are not designed to process directly identifying personal data, such as names or email addresses, and partners and clients may not send such information to Quantcast or cause Quantcast to collect it. If a partner has express permission from Quantcast to use email address, phone number, or other directly identifying information, such information will be pseudonymized (usually hashed or encrypted,) according to Quantcast specifications, before transmitting to Quantcast.

Reidentification. Under no circumstances will publishers use any information collected or generated by Quantcast's services to identify an individual user.