Last Modified: January 1, 2017

OUR PRIVACY PRINCIPLES

Consumer privacy is a top priority for Claritas. We rely primarily on demographic and behavioral data from which even we cannot identify people and limit access to data about specific individuals wherever possible. Not only does our internal policy conform to laws and standards around the globe, we also follow the principle of Privacy by Design.

Our Privacy Officer and our team of internal privacy professionals review and approve new products and services.

We deploy consumer-friendly privacy controls that are easy to find and easy to use. We believe in responsible stewardship of data, and we are constantly striving to improve our own practices and maintain a high standard for our industries.

Claritas' privacy principles include:

PRIVACY BY DESIGN
While developing our products and services, we assess their potential impact on personal privacy and embed appropriate privacy protections implementing the other principles described below.

TRUST AND ACCOUNTABILITY
We are committed to being responsible stewards of the data in our control and complying with all applicable data protection laws that regulate the collection, use and disclosure of data about individual people. Claritas' internal privacy organization oversees compliance with privacy laws, self-regulatory programs that we participate in, and our policies. We use tools and methods to prevent individuals from being identifiable in our reports and insights, and we take steps to prevent the data we collect from being reused in ways that could negatively affect individuals.

Claritas works with the Research Choices Initiative. This program run under the auspices of ESOMAR (the global market research standards organization), enables consumers to make choices about participating in online or mobile research.

Through Claritas' affiliate eXelate, now part of the Nielsen Marketing Cloud, Claritas participates in:

- The Digital Advertising Alliance ("DAA"); we adhere to the DAA's self-regulatory principles for online behavioral advertising, including the DAA's application of self-regulatory principles to the mobile environment;
- The European Interactive Digital Advertising Alliance ("EDAA"), and its principles; and
- The Network Advertising Initiative (NAI) and adheres to the NAI code of conduct, including the 2013 NAI mobile application code.

You can learn more about eXelate's privacy practices here.

MEANINGFUL NOTICE AND CHOICE

We provide clear notice about what data we collect and how we use it. We offer choices about our data collection at a time and in a context that reflect the sensitivity of the data being collected. Panelists and survey respondents opt in to the collection and processing of their data, and they may withdraw their consent (opt out) at any time. Individuals also have the ability to opt out of our online and mobile measurement activities at any time. When we use third-party data solely to create statistical models that do not relate to any specific individual, we are unable to offer choices to individuals. But you may click here to learn how to exercise choices with the companies who provide us that data.

DATA QUALITY

We are constantly working to help ensure that the data we collect is complete, accurate, relevant and up to date.

DATA MINIMIZATION AND COLLECTION LIMITATION

Following the concept of privacy by design, we limit the collection of individual-level data to the extent possible while still enabling us to derive meaningful and accurate measurements and insights.

- We limit the collection of specific identifiers like names and email addresses. Rather, we mostly rely on identifiers that consumers can reset or change, including: advertising identifiers (e.g., Apple IDFA or Android Advertising ID), and identifiers we create ourselves to perform, among other things, measurement, market segmentation and Nielsen Marketing Cloud services.

- When we do use direct identifiers, we limit access to such information both internally and externally and rely on our data security measures to protect individuals' privacy.

- Before we obtain third-party data, we review the third party's data collection practices and the privacy notices that are made available to individuals to make sure that our use of the data is consistent with the promises those companies have made to individuals.

- When we have removed identifying elements from the data, we take steps to prevent them from being associated with identifiable data.

LIMITED USE AND RETENTION

We restrict internal access to and use of individual-level data to Claritas associates with a legitimate business purpose. We have established records retention policies to limit how long we keep individual-level data.

ACCESS AND CORRECTION

When we collect information that directly identifies a person (e.g., name, email or home address), we provide individuals with reasonable opportunities to access that data and correct it when it's inaccurate.

CHILDREN'S DATA

We comply with applicable laws regarding the collection of data about children. When we collect individual-level data from children, we do so with parental consent, which can be withdrawn at any time.

CROSS-BORDER TRANSFER
We respect local rules regarding cross-border transfers of and access to data.

DISCLOSURES OF DATA TO THIRD PARTIES
We do not sell data that directly identifies individuals, and we contractually prohibit our clients from re-identifying de-identified data that we provide them (e.g., audience statistics). Furthermore, we contractually prohibit recipients of our data from using our data to make decisions regarding credit, insurance, housing or employment. We contractually require service providers that have access to our data to keep it secure and to use it to perform only the services they have been hired to provide. We will provide data to government and law enforcement entities to the extent required by applicable law, to protect Claritas' legal interests, and where needed in an emergency situation to protect an individual's health or safety.

DATA SECURITY
We implement multi-layered organizational, technical and administrative measures to protect the data in our control. These include, among other things, limiting who within our organization is allowed to have access to data, using technology measures like firewalls, encryption, malware protection, and intrusion detection, maintaining policies that are aligned to a wide variety of legal requirements, and holding our associates accountable for maintaining safe data-handling practices. We have a worldwide organization of qualified data security professionals and engage in regular testing and updating of our controls to keep pace with changing technology and threats.

GLOBAL REACH, LOCAL TOUCH
We are committed to respecting the diverse cultures and local laws of the countries in which we operate.