PRIVACY & DATA ETHICS

Privacy Brief

State Privacy Law Remediation – Adjustments to Acxiom Audiences

U.S. Data Privacy Landscape

Many comprehensive data privacy laws recently have been enacted and many more are in progress, making staying on top of regulatory compliance more and more challenging. By 2026, 19 comprehensive state privacy laws will go into effect.[1]

- Each new law will regulate the processing of sensitive personal information
- California, Iowa, and Utah will provide people the right to limit the use of sensitive personal information through an opt-out method
- All other states will require people's opt-in consent before processing their sensitive personal information.

The new laws all will include a definition of sensitive personal information with business obligations associated with the processing of sensitive data. A summary of the 19 states and their definition of sensitive personal information can be found in the appendix. The chart is provided as summary. For a list of sensitive data defined additional documents are available.

How is data processing defined?

"Processing" has been generally defined in the laws as "any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion or modification of personal data." The broad definition of processing would include simply storing sensitive personal information.

What adjustments will be made to Acxiom's third-party data?

To ensure compliance with state privacy laws, sensitive data is removed from all sources for opt-in affected states prior to building third-party data, including InfoBase, Audience Propensities and Personicx. Acxiom also implements logic to ensure individuals and households in the affected states are not assigned sensitive attributes during the third-party data product build process.

For opt-out states, California, Iowa and Utah Acxiom removes sensitive data from consumers who have opted out.

How does this impact Acxiom Health audiences?

Acxiom’s models do not predict whether a particular individual has a past, present, or future physical, mental, or medical condition. Clients may not use our models in a manner that would express or imply a consumer may have a past, present, or future physical, mental, or medical condition.

- Acxiom Health builds look-alike models that correlate demographic variables from InfoBase to de-identified claims data to meet desired healthcare criteria.
- The U.S. adult population is then scored based on the demographic variables from InfoBase and how much they correlate to the de-identified claims data.
- The demographic variables from InfoBase used with the seed population to create the model are already cleaned of sensitive data prior to modeling.

Privacy-By-Design

Privacy-by-design is a proactive approach to privacy that integrates data protection from the onset of the design process for any system, service, or product that handles personal information. Acxiom is committed to embedding privacy into every stage of the data management life cycle, ensuring all new products, services, or data use meet stringent privacy standards from the ground up.

For more information, visit Acxiom.com/privacy

[1] IAPP.org

For questions on this brief, please contact the Acxiom Global Data Ethics and Privacy Team at DataEthics@acxiom.com.

ACXIOM

PRIVACY & DATA ETHICS
Privacy Brief

States with Privacy Law Updates	CA	CO	CT	DE	IA	IN	KY	MD	MN	MT	NE	NH	NJ	OR	RI	TN	TX	UT	VA
Social Security, driver's license, state identification card, or passport numbers	●																		
Account log-in, financial account, debit card, or credit card number in combination with any required security codes	●												●						
Precise geolocation	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Philosophical beliefs, union memberships	●																		
Religious beliefs	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Racial and ethnic origins	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Contents of mail, email, and text messages to unintended recipients	●																		
Genetic data or biometric information if used to uniquely identify a consumer	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Personal health information	●							●											
Personal information related to a consumer's sex life		●	●	●				●				●	●		●				
Sexual orientation	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Status as transgender or nonbinary				●				●					●	●					
Citizenship or immigration status		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Information regarding an individual's medical history, mental or physical health condition, medical treatment or diagnosis		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Personal data from a known child		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Status as a victim of crime														●					