SUCCESSFULLY NAVIGATING DATA SOURCING AND INTEGRATION

Regulators and individuals scrutinize businesses' collection and use of data every day, checking to ensure their data practices are ethical and people's privacy is being protected. Users of personal information must be diligent to create and maintain a data source credentialing program to ensure that all data collected has been permissioned appropriately and is used in a manner that is consistent with people's expectations and applicable regulatory requirements.

This document provides guidance regarding best practices for sourcing and implementing personal information in compliance with expectations and applicable laws.

DATA SOURCING RECOMMENDATIONS

1 Data is required to be collected pursuant to a privacy notice.

2 The privacy notice must be conspicuous.

3 **Notice.** The data collector's privacy notice must provide the consumer with the following notices:

- **Information Collected.** The privacy notice must disclose the specific information that is collected from and/or about the consumer.
- **Information Disclosed to Third Parties.** The privacy notice must give notice that the information is transferred to or shared with unaffiliated third parties for purposes unrelated to the original consumer transaction.
  - **Example:** "We may disclose the information collected to unaffiliated third parties for any legally permissible purpose including but not limited to ..."
  - **Note:** If secondary uses of the information are described, those descriptions should be specific.
  - **Note:** Notice that information will be provided to entities acting as an agent or partner under an agreement with the collector is insufficient; the notice must also state that the information is being shared with unaffiliated third parties.

4 **Choice:** The privacy notice must include information about a mechanism by which the consumer can exercise choice to "opt out" or prevent transfer of consumer information to third parties.

- There must be an **opt-out for each element** of consumer information collected and shared. If any personally identifiable information (PII) is collected and an opt-out mechanism is not provided, that information cannot be transferred to third-party marketers.
- The opt-out mechanism must be expressly available to **all consumers** and not on a limited basis by state (i.e., "for California residents").

5 **Transparency:** In addition to these requirements, the terms of the privacy notice must be clear to the average consumer and in no way be deceptive or misleading.

DATA INTEGRATION CONSIDERATIONS AND TOOLS

1 **Know the privacy terms of use for the data source and know your own privacy terms.**

- Can the data be used for analytic purposes, for aggregated reporting, for audience activation, or other uses that may be common to your operations?
- Is the data anonymous or pseudonymous? Can it be associated to known data or natural PII?
- Under what circumstances can the data be shared with partners or resold?

2 **Think about data minimization, and only bring in the data you need.**

3 **Establish a standard process to incorporate the information into your data inventory or data catalog.**

- The data inventory should reflect the data, the source, permissible use and restrictions, and attribute name.

4 **Leverage classification to how the data can be used internally and externally.**

- Define categories like offline and/or online use, whether the data is known, pseudonymous or anonymous, and whether the data can be used for analytical, and/or audience activation, and/or other uses specific to your business.

5 **Understand the regulatory obligations for the data.**

- Know if you are required to manage opt-out, delete, and access requests.

6 **Have an established process to research consumer inquiries and escalations.**

7 **Work toward engineering that allows for flexibility.**

- Monitor state and federal bills that push the envelope with respect to regulatory requirements for collecting and managing consumer data.

8 **Leverage tools for managing consumer data.**

- Data tagging minimizes the risk of data being misused by categorizing the data at the onset. The tag associated with the data identifies access and handling procedures.
- Data zoning is a methodology for routing data and categorizing data based on the data group and user access policies. Data zoning allows controlled logical and physical separation of data based on classification of the data.
- Data treatment is the application of encryption, hashing and obfuscation to ensure specific types of data cannot be viewed or matched unless that is allowed.
- Data access policies and controls are the policies and controls that manage authentication and authorization. Access controls also manage the warning and logging of activity with respect to users, data and applications.

acxiom

acxiom.com
info@acxiom.com