



 ACXIOM POV

The California Delete Act: Why brands should care

ACXIOM

Privacy regulations have steadily reshaped digital marketing. Most of those regulations focus on disclosure and consent. California's Delete Act is different – it's designed to disrupt the third-party data ecosystem at scale. Starting in August 2026, the law requires covered data suppliers to process deletion requests through a single, centralized platform. For marketers, the implications are significant.

What this means

[The California Delete Act](#) (SB 362) targets companies that collect and sell personal information about consumers they don't have a direct relationship with. Instead of contacting each company separately, consumers can submit one deletion request through the [Delete Request and Opt-Out Platform](#) (DROP), managed by the California Privacy Protection Agency.

As of April, more than 550 companies were registered under the statute. Among other things, data suppliers must retrieve deletion requests, match them against their records, delete applicable data, and maintain audit-ready compliance processes. The operational requirements kick in no later than August 1, 2026.

The statute mirrors aspects of the National Do Not Call Registry but with a crucial difference: it targets participation in the third-party data ecosystem itself rather than just telemarketing outreach. That distinction matters. Centralized deletion likely means higher request volumes. If adoption accelerates, organizations that depend on third-party data face meaningful, long-term challenges.

And this will not stop in California. Connecticut has passed [similar legislation](#), with observers watching for momentum at the state and federal levels.



The immediate marketing impact

The initial effect may not seem dramatic, but the cumulative impact could be material. Marketers relying on third-party data for audience segmentation, CRM enrichment, identity resolution, and personalization may see:

- Lower match rates over time
- Reduced enrichment availability
- Smaller addressable audiences for certain campaigns
- Increased pressure on first-party data strategies

But here's what matters most: consumers benefit from personalization that actually serves them, not marketing noise. Privacy regulations like the Delete Act help ensure that trust remains intact.

The brands best positioned to compete aren't necessarily those with the largest data assets – they're those investing now in governance and responsible data practices. These organizations will work with partners who understand how to maximize available data while maintaining privacy standards. In other words, brands prioritizing data stewardship today gain a competitive advantage as the market evolves.

Data governance is now a marketing imperative

The Delete Act underscores a broader reality: privacy, governance, and marketing operations are inseparable. Historically, marketing, legal, privacy, and analytics teams operated independently. That separation becomes harder to maintain.

Here's the critical insight: strong data governance is not merely a compliance requirement – it is the foundation that enables responsible personalization. When brands understand where data comes from, how it's used, and how it's protected, they build consumer trust while delivering the relevant, preference-based experiences they expect.

Areas requiring greater focus:

- Data lineage visibility
- Vendor and partner oversight
- Consumer rights management workflows
- Audit readiness and deletion governance
- Privacy-aware data architecture

Organizations should also evaluate whether their data practices fall within the statute's scope, particularly when consumer information is enriched, shared, or licensed across ecosystems.

This isn't just compliance. It's business resilience.

What to do now

While regulatory details continue evolving, marketers should start preparing:

Assess your current position. Evaluate third-party data dependencies, review vendor relationships, and understand how consumer deletion requirements affect downstream workflows and audience strategies.

Strengthen first-party data strategies. First-party relationships are your most durable asset in a privacy-centric environment. Invest in collection, governance, and activation capabilities now.

Align internally. Marketing and privacy leaders should establish clarity around:

- How consumer data is used
- Deletion and suppression processes
- Vendor accountability
- Governance ownership

Build the right partnerships. Working with partners built to navigate these regulations responsibly – protecting your brand while enabling data-driven personalization – becomes invaluable.

The companies best positioned aren't those with the most data. They're those with the strongest ability to adapt responsibly.

The path forward

As privacy regulations reshape the marketing landscape, trust increasingly becomes a competitive asset. Organizations that combine responsible data practices with marketing performance gain distinct advantages.

Axiom helps brands assess their data practices, governance frameworks, and operational readiness to create a privacy-centric marketing environment. Our compliance-first approach ensures you safeguard your data while maximizing marketing performance, delivering personalization consumers value without sacrificing brand trust.



ACXIOM

For more information, please
contact Acxiom at acxiom.com
or email info@acxiom.com.