

Understanding the California DELETE Act: Key Insights and Implications

WRITTEN BY

Shelby E. Dolen | Marlaina Zollinger Pinto

This article originally appeared in the September 28, 2026 issue of the [Orange County Business Journal](#). It is republished here with permission.

California continues to be at the forefront of consumer data privacy regulation. For businesses that collect and sell consumer data, the DELETE Act and its corresponding Delete Request and Opt-out Platform (DROP) regulations expand compliance obligations under the existing data broker framework. This article provides an overview of the law, highlights practical implications, and offers guidance for building a defensible compliance program.

OVERVIEW OF THE DELETE ACT AND DROP

Signed into law in October 2023, the DELETE Act builds on the California Consumer Privacy Act (CCPA) framework by creating a centralized deletion mechanism administered by the California Privacy Protection Agency (CalPrivacy). The law requires every entity that meets the definition of a “data broker” to register with CalPrivacy and participate in the newly launched DROP. Under the DELETE Act, a company is a “data broker” when it knowingly collects and sells personal information of California consumers with whom it lacks a direct relationship and meets the CCPA’s definition of a “business.”

DROP launched in 2026, allowing registered California residents to direct all registered data brokers to delete their personal information through a single request submitted on the platform. Each registered data broker must access DROP at least once every 45 days, process all applicable deletion requests, and direct any service providers or contractors that received the covered data to delete it.

In addition to fines for not registering with the state, a data broker that fails to comply with a DROP deletion request may face an administrative fine of \$200 per request for each day the information remains undeleted. As of August 25, 2026, CalPrivacy has reported that more than 500,000 Californians have registered for DROP, bringing a data broker’s potential penalties for non-compliance to over \$100,000,000 per day, with actual exposure depending on how many registrants’ data the broker holds.

After honoring a request, a data broker generally may not sell or share newly collected personal information about that consumer unless the consumer affirmatively consents to opt back in. The DELETE Act layers additional transparency and accountability requirements on top of existing CCPA obligations. Registered data brokers face enhanced disclosure and recordkeeping duties, including maintaining verifiable records of how deletion requests were processed and the timeframes for completion. Looking ahead, the law introduces independent audit

requirements beginning in 2028, requiring data brokers to undergo third-party reviews of their deletion and opt-out practices.

STRATEGIC IMPLICATIONS FOR BUSINESSES

The DELETE Act's operational requirements require affected businesses to move well beyond a check-the-box registration exercise. Several areas merit immediate attention.

Determining data broker status. Companies should evaluate whether their data practices bring them within the statutory definition of a data broker. Under the DELETE Act, personal information carries the same broad definition established under the CCPA. Importantly, publicly available information remains outside the scope of the data broker-specific law, which may be a significant exclusion for certain businesses. Businesses should not rely on the exemptions under the CCPA, however, as the DELETE Act has its own exceptions, including entities covered by the Fair Credit Reporting Act or the Gramm-Leach-Bliley Act. Businesses engaged in data aggregation, lead generation, people-search services, advertising-data licensing, or similar activities should undertake this assessment promptly.

Multi-entity registration. Critically, the data broker analysis must be performed entity by entity, not at the enterprise or brand level. A review of the California Data Broker Registry reveals that relatively few corporate groups have registered multiple legal entities. Some companies appear to register one entity while listing multiple brands, DBAs, or websites under that single registration, an approach that may or may not reflect the underlying operational and legal structure.

This divergence likely reflects two distinct strategies playing out across the industry. Some companies may be centralizing all data broker activity within a single legal entity so that affiliate entities do not independently trigger registration obligations. Others may be registering with only one entity despite potential data broker activity across affiliates.

For corporate groups navigating this question, the threshold inquiry is which legal entities, independently, collect and sell personal information of California consumers with whom they have no direct relationship. If the answer is more than one, a conservative posture may require multiple registrations. Where data broker activities are genuinely centralized within a single legal entity, a single registration may be supportable. But where affiliates independently qualify, failure to register each entity exposes the broader corporate group to penalties and enforcement scrutiny.

Registration information. Data brokers must submit certain information when registering with DROP, including describing the products and services covered by the law, the types of personal information collected and sold, and the proportion of data collected and sold that is subject to the law compared to its total data collection and sales. These disclosures require a close comparison to any public disclosures the data broker has made, including public privacy notices.

Preserve defensible records. Given the independent audit requirements starting in 2028, data brokers should establish detailed recordkeeping practices now. Demonstrating compliance during an audit will require the data broker to maintain verifiable logs showing when it received deletion requests, when it completed processing those requests, and when it passed those requests to applicable service providers or contractors. Data brokers have a

narrow but meaningful window to build processes that will withstand external scrutiny.

Vendor and contractual obligations. Data brokers relying on third-party data suppliers or downstream vendors should assess whether their existing contracts adequately address DELETE Act compliance. Contracts that predate the law may lack provisions requiring counterparties to honor deletion requests, propagate those requests downstream, or maintain the recordkeeping necessary to demonstrate compliance. Renegotiating or supplementing these agreements now reduces exposure as the deletion framework becomes fully operational.

CONCLUSION

The California DELETE Act meaningfully expands consumer privacy rights and imposes substantial new obligations and penalties on data brokers operating in California. The law is not a static compliance exercise, and organizations should resist treating it as one. Organizations that have not yet assessed their databroker status, mapped their data flows, and established operational processes for DROP should treat these steps as urgent priorities to reduce regulatory risk and position themselves for the independent audits beginning in 2028.

RELATED INDUSTRIES + PRACTICES

- [Privacy + Cyber](#)