State Privacy Law Requirements: Instructing Vendors and Partners to Fulfill Deletion and Opt Out Privacy Rights Requests

Alysa Z. Hutnik, Laura Riposo VanDruff, Alexander I. Schneider, Meaghan M. Donahue

November 22, 2024

Under many circumstances, state privacy laws require businesses to pass a consumer's valid deletion request to any entity that processes the data on behalf of the business or otherwise is a recipient of the data. These so-called "flow-down" obligations can be challenging to unpack. Here's a look at the flow-down obligations that may be applicable, depending on the circumstances.

DELETION REQUESTS

The state privacy laws generally require a business—also known as a controller—that receives a valid deletion request to delete the personal information it holds about the consumer. Exceptions may be available depending on the state law, which can allow the business to retain personal information where necessary to combat fraud, provide products or services specifically requested by the consumer, or to comply with a legal obligation.

In addition to existing state privacy laws, the California DELETE Act will require "data brokers" to operationalize an "accessible deletion mechanism," which the California Privacy Protection Agency (CPPA) will create by January 2026. Beginning in August 2026, data brokers must delete personal information about a consumer on an ongoing basis. If a data broker is unable to verify a deletion request submitted through the deletion mechanism, the statute instructs the entity to opt the individual out instead.

These laws may require businesses to pass deletion requests to service providers, contractors, or third parties.

Service Providers

Service providers that process personal information on behalf of and at the direction of a business—also known as contractors or processors—generally have an obligation to assist the business with privacy rights requests by deleting the consumer's personal information from their records.

For example, California's CCPA regulations expressly specify that the business must "[notify] the business's service providers or contractors of the need to delete from their records the consumer's personal information that they collected…," and that the service provider must, in turn, delete the data. The regulations also obligate the service provider to notify its own service providers of the

"need to delete from their records in the same manner the consumer's personal information. . . ." Similarly, Colorado's CPA regulations require a controller to "instruct its Processors . . . to delete the Consumer's Personal Data held by the Processors."

Where state laws do not direct a business to provide deletion instructions to their service providers, most state laws obligate service providers to assist the business with a privacy rights request, including deletion or opt-out requests. For example, the Connecticut privacy law requires a processor to "fulfill the controller's obligation to respond to consumer rights requests." The California DELETE Act likewise requires data brokers to instruct "all service providers or contractors associated with the data broker to delete all personal information in their possession related to the consumers making the requests[,]" or opt that consumer out, as applicable.

The state privacy law exceptions to deletion obligations apply equally to businesses and their service providers.

Sales to Third Parties

The CCPA uniquely requires a business to notify "all third parties to whom the business has sold or shared the personal information of the need to delete the consumer's personal information unless this proves impossible or involves disproportionate effort." The CPPA requires transparency to the consumer if a business relies on the "disproportionate effort" exception, requiring a business to provide the consumer with a "detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot notify all third parties."

Operationalizing Deletion Requests

How a business notifies service providers and third parties about deletion obligations can vary widely. For some, this may be a painfully manual process, including by sending emails to vendor points of contact. Some vendors may specify particular ways they will receive and process requests, including through designated privacy-related APIs. These processes may also change over time, which may require periodic review of vendors' publicly-facing privacy materials and customer help pages. There are also some privacy compliance technology vendors that have developed direct integrations with different vendors to automate deletion and opt-out requests, so this is a topic also worth exploring with them. Finally, the IAB Tech Lab offers a Data Deletion Request Framework to facilitate deletion requests in an ad tech context.

For data brokers, the California DELETE Act has layered on additional operational considerations. These entities not only must access the state deletion mechanism at least once every 45 days and apply the available requests, but data brokers also are required to continue deleting a consumer's data on a going-forward basis. From a preparation standpoint, for those companies that purchase or license personal data from data brokers, this means that there are likely to be a higher volume of deletion requests that data brokers flow down. The result will be an operational conundrum in which companies will need to distinguish between the data they have received from the data brokers and other sources so that they can comply with their own deletion obligations as to such data. The recent expansion of the definition of a data broker (as discussed in our recent post) may expand the number of businesses subject to these obligations.

OPT-OUT REQUESTS

The state privacy laws require businesses to comply with consumer requests to opt out of the sale or sharing of personal information or the processing of personal information for targeted advertising. In

some cases, the laws may also require a business to pass an opt-out request to a third-party recipient of the data, whether that's a data buyer or an ad tech vendor.

As an illustrative example, a consumer might fill out a lead form on a lead generation website, triggering the sale of the consumer's information to other businesses. If the consumer submits an opt-out request (either during the same browsing session or soon thereafter), the lead generator may be required to notify lead buyers about the opt-out request and direct the lead buyers to comply with the request.

Further, the CCPA regulations contain language suggesting that a business and third party may enter into a contract requiring the third party to comply with a consumer's request to opt out of the sale or sharing of personal information, which was forwarded to it by the business. A third party that receives an opt-out request could either refrain from processing the data entirely or choose to become a service provider and use the data only for limited business purposes. The IAB Multi-State Privacy Agreement (MSPA) and the IAB Tech Lab's Global Privacy Platform—industry solutions for communicating and complying with consumer opt-out requests in a digital advertising context—are built around the latter approach.

CONSIDERATIONS

Companies subject to state privacy laws can work with privacy counsel to develop and update processes and procedures for accepting and fulfilling privacy rights requests, including verifying that appropriate consumer-facing notices and disclosures are in place, implementing technology solutions for privacy rights management, mapping personal information and data flows in internal and external information systems, notifying vendors, service providers, and third parties about deletion and opt-out requests, and providing for training and written policies and procedures memorializing the company's compliance program addressing these obligations. Companies can also review their vendor contracts to address state privacy law mandatory clauses and handling of privacy rights requests.

These are no longer best practices, but rather reflect minimum expectations from regulators on what companies need to have in place to comply with state laws. We have also seen a marked increase in enforcement inquiries from states over this past quarter asking companies to demonstrate how they are addressing many of these obligations. Given the current climate, where many state regulators now have larger enforcement teams and statutory mandates, it would be prudent to assume a company may need to explain the privacy compliance measures it has in place, including the specific materials it will point to for purposes of demonstrating it is in compliance. Providing a narrative about what a company is doing is helpful, but compliance documentation is critical to resolve any such inquiries.