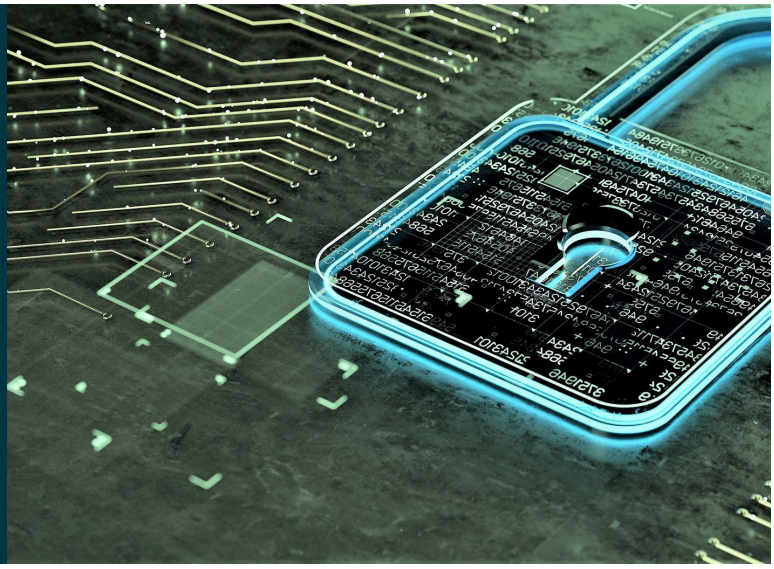
WILSON SONSINI

# CPPA Votes Out Proposed Delete Request and Opt-Out Platform (DROP) Data Broker Regulations



## CONTRIBUTORS



Tracy Shapiro


Eddie Holman


Clinton P. Oxford


Taylor Stenberg Erb


## ALERTS

*March 12, 2025*

On March 7, 2025, the California Privacy Protection Agency (CPPA) Board met to discuss its proposed data broker regulations concerning the Delete Request and Opt-Out Platform (DROP) and voted to authorize CPPA staff to advance the regulations to formal rulemaking. As mandated by the Delete Act (discussed in a previous alert), the DROP will allow California residents to submit a single request to delete all personal information held by all data brokers operating in the state via an accessible mechanism. Data brokers would be required to access the DROP for updates every 45 days and delete the personal information of any state resident that matched the data broker's records unless a deletion exception set forth in the California Consumer Privacy Act (CCPA) applies. These regulations also follow the CPPA's November 2024 meeting, during which CPPA staff provided an update on the development of the DROP.

The proposed DROP regulations further highlight data brokers as an enforcement priority for the CPPA. Beginning in October 2024, the CPPA conducted an investigative sweep of data brokers and brought several enforcement actions as a result. Most recently, in February 2025 the CPPA brought an enforcement action against a Florida-based data broker for failing to register with the CPPA and pay the associated registration fee. February's enforcement action marks the sixth in the CPPA's investigative sweep.

Below is a summary of the proposed DROP regulations and updates discussed during the board meeting:

- **Revision of "Direct Relationship":** The Delete Act requires businesses that knowingly collect and sell the personal information of a resident with whom it does not have a direct relationship to register as a data broker and comply with the Delete Act's requirements. The regulations would further revise the definition of "direct relationship" to clarify that a business does *not* have a direct relationship with a consumer simply because it has collected "personal information directly from the consumer." Rather, the regulations provide that in order to have a direct relationship, the business must not only collect personal information directly from a consumer, but also the consumer must "intend to interact with the business." In the CPPA Board meeting, CPPA staff suggested that a consumer making an online purchase may not intend to interact with cookies or reveal their geolocation information, in which case such information collection would not constitute a direct relationship. The regulations also state that merely collecting personal information directly from a consumer in one context does not categorically exempt a business from being a data broker; a business is still a data broker with respect to personal information it sells about the consumer that it collected outside of a direct, first-party relationship. These clarifications further enhance the broad scope of companies captured as data brokers under the regulations, as highlighted in a prior analysis. In one notable expansion of the definition, however, the regulations would remove the requirement that the consumer's interaction with the business have occurred within the preceding three years.

- **Mechanics of Data Brokers' DROP Account Creation:** After creating an account, data brokers would be required to select a "consumer deletion list" that the data broker will retrieve through the DROP to process deletion requests. The regulations define a "consumer deletion list" as a list containing at least one type of consumer identifier for every consumer that has submitted a deletion request through the DROP. A consumer deletion list can include one or multiple types of identifiers. For example, a consumer deletion list can include name, date of birth, and zip code. Data brokers would be required to select all consumer deletion lists that contain a consumer identifier that matches personal data in their records; however, if the data broker collects the same personal data types for every consumer, it would only be required to select one list for one type of consumer identifier. Following account creation, a data broker could add or remove a consumer deletion list through its DROP account, but it would only be able to do so once every 45 days.
- **DROP Access:** The regulations would require data brokers to access the DROP every 45 days to download updates to the consumer deletion list(s). Access can be manual or automated, and the list(s) would only reflect new or revised consumer deletion requests after a data broker's first download.
- **Processing Deletion Requests:**
  - *Matches That Trigger the Deletion Requirement:* Before processing deletion requests, the draft regulations require that data brokers standardize personal information in their records. Such standardization methods include using lowercase letters or removing special or extraneous characters. Data brokers would then be required to compare the personal information in their records against the consumer deletion list(s) and delete all personal information associated with a matched record that is not subject to a CCPA deletion exception. If a consumer deletion list has more than one type of identifier, a majority of the identifiers would need to match the data broker's records to trigger the deletion requirement. For example, the regulations note that if a consumer deletion list with identifiers such as a name, date of birth, and zip code matched only the name and zip code for a consumer in their records, they would be required to delete all of the personal information for that consumer. In addition, if multiple consumers are matched to an identifier from a consumer deletion list, instead of deleting the consumers' data the data broker must opt out each consumer from the selling or sharing of their personal information. As written, the opt-out requirements risk being overinclusive by capturing more consumers than those who actually opted out. During the CPPA Board meeting, Board member Alastair Mactaggart asked that CPPA staff consider how a consumer could submit a request concerning their biometric information, which would not be maintained in a consumer deletion list.
  - *Data to Be Deleted:* For each triggering match, data brokers would be required to delete all personal information associated with the personal identifier in their records other than: 1) personal information that the data broker collected directly from the consumer as a "first party"; and 2) personal information that is subject to a CCPA deletion exemption. The draft regulations clarify that such information includes inferences based on information collected from third parties or from consumers in a non "first party" capacity. In addition, the draft regulations would require indefinitely maintaining the minimum personal information necessary to delete any personal information that the business may receive about the consumer in the future. During the CPPA Board meeting, CPPA staff and the Board discussed "suppression lists," or records maintained by a data broker to ensure that future data purchases do not contain information about consumers that have requested their personal information be deleted. In response to a question concerning the feasibility and enforcement of this requirement, CPPA staff noted that they plan to ensure compliance through the regular audit process.
- **Reporting Deletion Requests:** Each time that a data broker accesses the DROP (other than the first time), it would be required to report the status of each deletion request it received since the last time it accessed the platform. Data brokers would be specifically required to report the transaction identifier keyed to the deletion request and the action taken in connection with the request (e.g., record deleted, record opted out of sale, record exempted, record not found). Data brokers may report through manual or automated means.
- **Data Security:** The draft regulations require that data brokers maintain reasonable security practices to protect the personal information contained in DROP. In addition, in the event of a security breach or unauthorized use of the account, a data broker would be required to notify the CPPA in writing through its DROP account. In response to CPPA Chairperson Jennifer Urban's concern regarding how a data broker would be able to notify the CPPA through their DROP account if it had been hacked, CPPA staff confirmed that they would add an alternative method for notification.

**Next Steps**

The CPPA Board approved the motion to advance the proposed draft regulations to formal rulemaking and to authorize CPPA staff to make any necessary changes. The 45-day public comment period will begin once CPPA staff makes those changes and officially publishes the notice of proposed rulemaking for the DROP regulations in the California Regulatory Notice Register. The CPPA plans for the DROP to be accessible to consumers by January 1, 2026, and to data brokers by August 1, 2026. To accommodate this timeline, the final regulations must be approved by the first quarter of 2026.

Wilson Sonsini Goodrich & Rosati routinely helps companies navigate complex privacy and data security issues. For more information or advice concerning your CCPA compliance efforts, please contact Tracy Shapiro, Eddie Holman, Clinton Oxford, or any member of the firm's data, privacy, and cybersecurity practice.

*Taylor Stenberg Erb contributed to the preparation of this alert.*