

## DRAFT FSOR APPENDIX B – SUMMARIES AND RESPONSES TO 15-DAY COMMENTS

### ARTICLE 2. DEFINITIONS AND REGISTRATION REQUIREMENTS

Section of Regulation	Comment Numbers	Summary of Comments 15-Day Comment Period	Agency Response
7601(g), 7613(a)(1)(A)(i) i)(1)	114	Commenter requests clarification of the term “extraneous or special characters” in § 7601(g) and § 7613(a)(1)(A)(ii)(1) because commenter states that the term “non-alphabetic or non-numeric characters” is vague. The commenter suggests specifying the alphabet (e.g., Latin) and clarifying that diacritics (e.g., in names like “Björn”) should be removed rather than replaced with “closest English character.”	The Agency agrees that clarity in data standardization requirements is important. The regulations define “extraneous or special characters,” in § 7601(g), to include non-alphabetic or non-numeric characters, such as punctuation, math symbols, emojis, extra spaces, and foreign language characters. The originally proposed text was revised such that § 7613(a)(1)(A)(ii)(1) further clarifies that non-English characters must be converted to their closest matching English character and provides an example (e.g., “Björn O’Connor-López” becomes “bjornoconnorlopez”). The Agency believes the revised regulations are sufficiently clear and that additional revisions are not necessary at this time.

### ARTICLE 3. DELETE REQUEST AND OPT-OUT PLATFORM REQUIREMENTS

Section of Regulation	Comment Numbers	Summary of Comments 15-Day Comment Period	Agency Response
7613(a)(1)	8, 10, 19, 20, 21, 23, 25, 49, 94, 96	Commenter asserts that the standardization requirements are impractical, overly prescriptive, risk reducing accuracy, and create operational burdens. Commenter argues that limiting standardization obligations to compliance purposes, still imposes burdensome restructuring of internal systems. Commenter asserts that data brokers will have to create and maintain multiple databases to comply with the requirement. This will create significant costs to build and maintain these databases while being able to preserve their ability to communicate with customers in the manner they choose.	The Agency disagrees with this comment. First, the Agency’s modifications were limited to how to standardize certain pieces of information in § 7613(a)(1)(A) and that data brokers are only required to standardize their data for purposes of compliance with the regulations as indicated in new subsection (a)(1)(C). The requirement to standardize data was not modified from the original proposed text.  As indicated in the responses to 45-day comments, standardization of data formats is necessary to enhance the accuracy and reliability of data matching, which is crucial for

		<p>Commenter asserts this requirement is particularly burdensome for small and mid-sized data brokers.</p> <p>Commenter requests guidance on how to format personal identifier values when submitting deletion and opt-out requests to maximize the number of matches. While another commenter asserts that reformatting their data in a standardized manner could create data security issues because hackers will have a clear understanding of how data is structured within data brokers which makes them susceptible to attacks.</p> <p>Commenter further argues that reformatting data in a standardized manner raises First Amendment concerns. Commenter asserts that the data standardization required by the regulations affects data brokers' ability to convey their message to consumers because it requires data brokers to substantively alter the contents of their databases. Specifically, where formatting affects how information is stored, categorized, or expressed, or the products and services offered. Commenter states requiring altering the database to "increase the likelihood of a match" may have downstream effects on the reports and data compilations data brokers provide to customers, which could also burden their ability to communicate with consumers in the manner they choose.</p>	<p>the effective implementation of the right to delete under the Delete Act. Data brokers may choose to keep their data in any format they choose for all other purposes than complying with the Delete Act and regulations. The Agency notes that the regulations clarify that data broker data sets only need to be standardized to compare identifiers within deletion lists, but otherwise do not need to be retained in such formats. This means a data broker could feasibly standardize certain identifiers on a temporary basis and not maintain personal information in standardized formats after completing the required deletion list comparisons, reducing security risks. If data brokers are not required to standardize data for purposes of matching the information from DROP, data brokers would likely have to conduct the matching manually or convert the DROP data, both of which would be extremely onerous, especially for small and mid-sized businesses that may not have the staffing or other resources to do so.</p> <p>The standardization measures do not inherently increase data security risks. Instead, they ensure consistency, reduce the likelihood of errors in data processing, and maximizes matches between the data sets while providing consumers the guidance that at least one commenter has requested though illustrating the format. Additionally, the regulations mandate that data brokers implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification, or disclosure, as outlined in § 7616(b). These combined measures address data security while achieving the objectives of the Delete Act.</p> <p>As also discussed in response to the 45-day comments, the requirement to standardize data does not violate the First Amendment and implements a valid state law. The regulation merely requires that personal information be at least</p>
--	--	---	---

			<p>temporarily standardized for purposes of complying with the Delete Act. In addition, nothing in the regulations requires a data broker to alter or augment their original data sets. A data broker can simply duplicate certain identifier lists in their databases, standardize the duplicate copy for purposes of comparing identifiers with a deletion list, and then delete the standardized identifier list after completing all necessary deletions.</p> <p>The regulation also does not require data to be disclosed, sold, or shared in any particular manner. Instead, the regulation merely requires a data broker to temporarily format the data in a standardized format to enable the data broker to comply with its statutory obligations under the Delete Act. The data broker may maintain the data in other formats for other purposes.</p>
7613(a)(2)	117, 118	<p>Commenter states that the regulations need to clarify the definition of "matched identifiers" because it is not explicit whether a matching name alone is sufficient verification for deletion. Commenter states that businesses may interpret matching requirements differently, leading to inconsistent deletion outcomes. Commenter states that many names are common; therefore, there may be unintended data removal from false consumer identification.</p> <p>Commenter suggests a more comprehensive definition of "matched identifier", such as stating in the regulations that a "matched identifier" is an exact first and last name match combined with at least one of the following: complete email address, complete direct telephone number with area code, government issued identification number, and/or complete postal address match between the deletion list and the data broker's data set.</p> <p>Commenter requests clarification of the rule requiring data brokers to opt out all consumers associated with a matched</p>	<p>The Agency disagrees with this comment. The revised regulations clearly explain how to compare a data broker list if it is one with multiple identifiers, but does not specifically preclude the use of a deletion list with a single identifier. Moreover, the Agency removed the 50% match rate threshold for consumer deletion list identifiers to 100% to ensure a more precise match and reduce the likelihood of erroneous deletions. Further, the regulations address matches to multiple consumers in § 7613(a)(2)(B) and § 7614(b)(2)(B), which require data brokers to opt out consumers of the sale or sharing of their personal information if there are multiple matches with a given identifier. This ensures that consumers are protected even when identifiers are shared. Finally, the Agency intends to use technical safeguards, <u>such as third-party verification and multi-factor authentication, to ensure accuracy of deletion requests and identifiers transmitted to data brokers.</u> The Agency believes this approach appropriately balances privacy protection with operational feasibility.</p>

		<p>identifier when multiple individuals share that identifier because their concern is that shared identifiers—such as a central business phone number—could trigger unintended opt-outs for entire groups (e.g., all employees at a real estate firm). To mitigate this, commenter proposes that the CPPA define “personal information associated with a matched identifier” to exclude identifiers linked to more than ten individuals and to limit the rule to data not collected directly from the consumer. Commenter states that this would prevent overreach while still honoring valid deletion requests.</p>	
7613(a)(2)(A)	1	<p>Commenter supports and agrees with the Agency's modification to remove the data matching standards in 7613(a)(2)(A). Commenter states the removal of the requirement helps align with consumer expectations and avoids overly broad execution of deletion requests.</p>	<p>The Agency agrees with this comment and notes commenter's support.</p>
7613(a)(2)(A)	97	<p>Commenter asserts that even with the revised matching threshold of 100%, the regulations will likely lead to over deletion. Commenter asserts requests that, even with the removal of the 50% threshold and hashing, the deletion lists lack sufficient identifiers to allow accurate matching because a deletion list may contain a single identifier.</p> <p>Commenter states that the regulations match threshold conflicts with the CCPA requirements, which require a business to honor deletion requests if the identity of the consumer is verified to a "reasonable or reasonably high degree of certainty." Commenter states that a "reasonably high degree of certainty" under the CCPA requires matching at least 3 pieces of personal information to verify that the consumer request is legitimate. Commenter requests harmonizing the regulation to CCPA as not doing so will create significant operational challenges and may run afoul of the APA.</p>	<p>The Agency disagrees with this comment. The regulations implement the Delete Act, which is separate and distinct from the CCPA. Although some businesses may be subject to both laws, each law services specific purposes with respect to deletion rights; the CCPA addresses information collected directly from the consumer and the Delete Act addresses information not collected directly from the consumer. The match rate threshold for consumer identifiers for the purposes of fulfilling a deletion request through DROP is a separate and distinguishable standard from the verification standards for purposes of the CCPA right to delete regulations. These regulations are consistent with the Delete Act, which is the governing law for this proposal. The Agency has determined that the matching threshold is appropriate to implement the purpose and intent of the Delete Act. Furthermore, certain individual identifiers, if proven to be under the control of a consumer through technical means like multi-factor authentication, sufficiently demonstrate connection to the</p>

			consumer for purposes of verification under the Delete Act. The Agency will monitor the DROP to determine whether modifications to the regulations are necessary in the future.
7613(a)(2)(A)	51, 115	<p>Commenter requests a list of every possible combination of multiple hashed identifiers used for comparison so they can increase the odds of positive matches.</p> <p>Commenter requests clarification of the hashing process in § 7613(a)(2)(A) because commenter states that the regulation lacks detail on how identifiers should be “combined” before hashing. The commenter asks whether this means concatenating hashed values or hashing the concatenated string, and recommends explicitly stating the algorithm used.</p>	The Agency disagrees with this comment, but understands commenter’s interest in maximizing match accuracy. However, § 7613(a)(2)(A) provides a clear method for how data brokers must process multiple identifiers: each identifier must be hashed individually, then concatenated, and hashed again using the same algorithm provided in the consumer deletion list. This approach ensures consistency while protecting consumer privacy and is stated clearly in the regulations.
7613(b)(1)(C)	84	Commenter requests to know which personal data elements were processed by internal or vendor systems to confirm whether data was de-identified or aggregated.	The Agency disagrees with this comment. The Delete Act and § 7613(d) require data brokers to direct their service providers and contractors to delete records associated with a matched identifier in the data broker’s records; data brokers must also report the status of deletion requests. The Delete Act does not contain a provision treating contractors and service providers as separate entities from the data broker for the purposes of the delete request, nor does it contain a requirement to report what was processed by the data broker as compared to the service provider or contractor.
7613(b)(1)(C)	105, 108	Commenter requests clarification of data retention requirements under § 7613 because commenter states that the regulation does not specify what data must be retained or deleted, or for how long. This creates compliance uncertainty and inconsistency across data brokers. Commenter also requests further clarity on the requirements for “deletion” and whether it allows data brokers to retain deidentified or aggregated information. Commenter recommends requiring data brokers to delete all de-identified and aggregated consumer information.	The Agency disagrees with this comment. The Delete Act clearly states that data brokers delete all consumer personal information as incorporated by reference under Civil Code § 1798.140, and regulations clearly indicate that data brokers are to delete all personal information associated with a matched identifier, unless it is exempt under Civil Code § 1798.99.86 or was collected directly from the consumer in a “first party” interaction. The regulations do not impose specific retention periods but require that any retained data be the minimum necessary to comply with the law, which requires permanent

			prohibition of sale and retention of consumer data for all active deletion requests. This approach ensures compliance while allowing flexibility for operational needs.
7613(c)	22, 24, 95	<p>Commenter asserts the requirement for data brokers to save and maintain a consumer deletion list is operationally burdensome and unnecessary. Commenter asserts this rule is unnecessary because any newly collected data will be subject to deletion once a data brokers accesses the DROP.</p> <p>Commenter asserts the requirement under the Delete Act is 45-days which is two times as fast as the requirements under the CCPA and creates conflicting compliance duties with CCPA rules. Commenter requests the removal of this rule.</p>	<p>The Agency disagrees with the comment. The requirement ensures that a data broker that processes a DROP deletion request for a consumer – whether or not they initially find a match - will still honor a DROP deletion request in the event that it acquires a database or new set of personal information that includes personal information about that consumer. This ensures that data brokers can't collect and sell personal information about consumers who have previously submitted deletion requests during the 45 days between DROP access sessions. This also ensures that a consumer DROP request is honored until the consumer changes their preference. The Agency believes this approach is narrowly tailored to the purpose of preventing re-collection of deleted data. Moreover, the 45-day time period is contained in the Delete Act. The Agency cannot amend the Delete Act or adopt regulations inconsistent with the Delete Act.</p>
7613(c), 7614(a)(1)	73	<p>Commenter requests to know what personal information could not be matched and was retained for future comparison so they can assess compliance.</p>	<p>The Agency disagrees with this comment. The regulations require the data broker to maintain the consumer deletion list containing requests that did not match with the data broker's records and compare it before new personal information is sold or shared.</p>
7613(d) & (e) [formerly 7613(b)(2)]	74, 85, 106	<p>Commenter requests to know what authorization exists for third-party processing with or without consent to evaluate legal compliance.</p> <p>Commenter also requests requiring data brokers to forward deletion requests to other entities that may have sold or shared information, such as research organization or other data aggregators.</p>	<p>The Agency agrees with the comment in part. The Delete Act requires that data brokers direct all service providers and contractors associated with the data broker to delete all personal information in accordance with a DROP request. There is no purpose for this provision to be included within in Delete Act if data brokers are not authorized to utilize third-parties for processing activities.</p>

			The original proposed text included § 7613(b)(2), now in 7613(d), requires data brokers to direct service providers and contractors to delete personal information in its possession associated with a matched identifier. Additionally, the Agency modified the regulations to add § 7613(e) to specifically allow the sharing of personal information with service providers and contractors necessary to facilitate required deletion. These provisions allow data brokers to share information with other businesses with whom they contract or receive services from to make the required deletions and prevent them from avoiding deletion obligations by contracting with another company to act for them. The Agency lacks the authority to require other entities to comply with the Delete Act.
7614(a)	29, 101	Commenter requests that the time period for DROP reporting requirements and effectuating a DROP delete request be changed to 90 days to align with the CCPA's timeline to execute a delete request.	The Agency disagrees with this comment. The Delete Act, in Civil Code § 1798.99.86(c)(1), requires a data broker to process a deletion request and delete all personal information related to the consumer making the request within 45 days of receipt. The Agency cannot adopt regulations inconsistent with the Delete Act.

#### ARTICLE 4. CONSUMER AND AUTHORIZED AGENT DELETE REQUESTS

Section of Regulation	Comment Numbers	Summary of Comments 15-Day Comment Period	Agency Response
7620(a)	11, 12, 13, 27, 98, 109	Commenter asserts residency verification is insufficient and that the regulations are focused on matching identifiers in consumer deletion lists to data maintained by data brokers instead of ensuring that deletion requests are verifiable. Commenter asserts this is contrary to the Delete Act which provides that data brokers can determine whether an individual has submitted a verifiable consumer request. Commenter asserts the term "verifiable consumer requests" comes from the CCPA and its regulations. Commenter asserts	The Agency disagrees with this comment. Specifically, after the 45-day comment period, the Agency only modified the provision that indicated residency may be verified, but instead indicating that it will be verified. The other provisions of the subsection remain as noticed in the original proposed text.  A request to delete under the CCPA is legally and functionally different from a request to delete under the Delete Act. Under the CCPA and its regulations, a "verifiable consumer request" to delete is associated only with personal information collected

		<p>the CPPA and California Attorney General have recognized that verification serves as a safeguard against the harms of unauthorized data deletion.</p> <p>Commenter states the Legislature has recognized that improper verification can cause consumer harm; the Legislature incorporated the CCPA's exception in enacting the Delete Act. Commenter indicates that the Legislature amended the CCPA in 2020 to clarify that requests to delete do not apply to household data and that the change was intended to address the concern that privacy rights were being applied beyond the data of the consumer who made the request.</p> <p>Commenter asserts that verifying consumer requests has been a safeguard built into the CCPA, CCPA regulations, and the Delete Act to protect against the harms of unauthorized deletion. Commenter argues that the regulations undermines this safeguard by focusing on data matching instead of consumer verification.</p> <p>Commenter states that mandatory verification would align with NIST 800-63-3 standards and strengthen consumer protection.</p> <p>Commenter requests consumers be required to confirm their identity and residency using reasonable verification methods.</p>	<p>directly from a consumer. In contrast, a request to delete under the Delete Act applies only to personal information collected outside of a “first party” interaction—i.e. personal information collected when a consumer does not intend to interact with the business. A consumer does not carry the same expectations or vulnerabilities with respect to personal information being deleted when that personal information was not intentionally provided to a business or collected from another source entirely. A consumer did not affirmatively give their personal information to a data broker and therefore there is not the same sensitivity to that information being deleted. Because the verification standards implement separate laws and different circumstances, the DROP regulations are not inconsistent with other provisions of law for purposes of the APA, and the level of verification carried out by the Agency is appropriate within the context of the Delete Act.</p> <p>In arguing the regulations are contrary to the Delete Act’s provision that data brokers can determine whether an individual has submitted a verifiable consumer request, the commenter’s interpretation conflates the statutory requirement for a “verifiable consumer request” with a requirement that data brokers themselves must verify the identity. However, the statute does not mandate that data brokers perform this verification directly. Instead, the Agency has designed the DROP to fulfill this verification function, thereby reducing the risk of inconsistent or duplicative verification practices and enhancing consumer privacy.</p> <p>The Agency notes commenter’s suggestion to align its verification with the NIST 800-63-3 standards; however, the Agency must adopt requirements consistent with, and appropriate for, implementing the California law. Moreover, the Delete Act states that the purpose is to allow consumers to send a single verifiable request to have their information</p>
--	--	---	---



			<p>deleted; thus, allowing data brokers to contact a consumer to separately verify a request after the Agency has verified the consumer's residency and certain personal information defeats the primary purpose of the accessible deletion mechanism and is unnecessary to carry out the Delete Act.</p> <p>Accordingly, the Agency has acted within its statutory authority and consistent with the Delete Act in designing a system that ensures verifiable consumer requests are submitted through a secure, centralized platform, without requiring data brokers to independently verify each request.</p>
--	--	--	---

## GENERAL AND OTHER TOPICS

Section of Regulation	Comment Numbers	Summary of Comments 15-Day Comment Period	Agency Response
Exemptions	61	Commenter requests to know which personal information is subject to exemptions so they can understand the limits of deletion.	The Agency agrees that consumers should know what personal information is exempt from disclosure. The regulations clarify that data brokers are not required to delete personal information that is exempt under Civil Code § 1798.99.86 or that was collected directly from the consumer in a “first party” interaction. The Agency intends to provide educational materials to assist consumers with understanding the DROP and notes commenter’s suggestion.

**NOT ON PROPOSED MODIFICATIONS**

Section of Regulation	Comment Number	Summary of Comments 15-Day Comment Period	Agency Response
7601(d), 7601(i)	62, 64, 65	Commenter requests to know what data was voluntarily submitted because they state that this may affect whether it is retained or deleted. Commenter also requests to know which personal information attributes are considered inferences. Commenter further requests to know what data was found but not deleted so that they know if they were successful in their deletion request.	While not on the proposed modifications, the Agency notes commenter’s suggestion and looks forward to continuing to work with stakeholders on future policy development.
7602(a–b), 7603(a–d)	40, 79, 113	<p>Commenter requests clarification on what authorization an agent needs to truthfully sign under penalty of perjury on behalf of the consumer to ensure legal compliance.</p> <p>Commenter requests to know which entities, brands, and products are subject to data broker regulations so they can make informed choices about engagement. Commenter requests a single, parent-level DROP registration for corporate groups rather than requiring each subsidiary to maintain a separate DROP account because commenter states that the proposed approach risks confusing consumers, unnecessarily fragmenting request processing, and creating duplicative administrative and technical burdens.</p>	While not on the proposed modifications, the Agency notes commenter’s suggestion and looks forward to continuing to work with stakeholders on future policy development.
7610(a)(1)(A–B), 7616(b)	31, 81, 82, 83	<p>Commenter requests clarification on what credentials an authorized agent needs to create a DROP account on the consumer’s behalf because their agent impersonates them using various communication channels. Commenter also requests a ledger of who accessed their personal information and for what purpose to support audits and accountability. Additionally, commenter requests to know what authorizations are required for third-party processing with and without consumer consent. Commenter further requests</p>	While not on the proposed modifications, the Agency notes commenter’s suggestion and looks forward to continuing to work with stakeholders on future policy development.

		to know who accessed their personal information in DROP on behalf of brokers to test for unauthorized use.	
7610(a)(3)(C), 7601(C)	43, 44, 47	Commenter requests to know which consumer deletion lists are accessed in the DROP and what identifiers are contained in each list to ensure all relevant identifiers are included, and to know which identifiers each data broker uses to return the most records so they can avoid disclosing unnecessary personal information. Commenter also requests to be notified when a data broker changes its consumer deletion list selection so their agent can track when new categories of personal information are collected.	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
7612	112	Commenter states that the regulations should clarify that the deletion deadline begins 45 days from the date the data broker downloads the deletion list, and how deadlines will be impacted if the DROP is unavailable, because without these clarifications, commenter states that disputes may occur surrounding inadvertent noncompliance.	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
7612(c)(1)	48, 80	Commenter requests a way to monitor deletions daily because commenter states the 45-day cadence for broker access may delay awareness of new or amended deletion requests. Commenter also requests to know which internal systems and vendor technologies process their data so they can verify deletion across all systems.	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
7613(a)(1)(B)	9, 14, 15, 16, 17, 18, 26, 50	Commenter asserts that the modified hashing algorithm requirements creates uncertainty, potentially results in matches to data not associated with the consumer making a DROP request, and prohibits verification of delete request—which is not consistent with the Delete Act or CCPA.  Commenter asserts the regulations prevent effective verification, despite the Delete Act providing that the DROP shall allow data brokers to determine whether a deletion request is verifiable, by prohibiting a data broker from	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.

		<p>contacting consumers to verify deletion requests. Hence, commenter argues the regulations do not provide a method to verify a consumer's identity. Commenter also asserts the hashing requirements conflict with the CCPA regulations because businesses must verify consumer deletion requests to a reasonable high degree.</p> <p>Commenter indicates that the lack of verification will lead to requiring data brokers to opt out all consumer records matching to the data elements. For example, the hashing algorithm would require a combined hashed identifier with a name and zip code; which in turn, would result in the deletion of information related to all consumers with that name in that zip code, even though some of those consumers have not submitted a deletion request.</p> <p>Commenter further asserts the hashing requirements lack clarity on the identifiers that may be in a consumer deletion list. Commenter requests to know which hashing algorithm is used in the consumer deletion list so they can apply the same algorithm to identifiers in broker systems.</p> <p>Commenter requests the hashing requirements be removed and that the regulations allow verification consistent with the verification process in the CCPA regulations.</p>	
7613(a)(2)(B)	67	Commenter requests to know if the broker was required to opt out all associated consumers from sale/sharing when multiple matches occurred.	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
7613(b), 7601(d), 7601(i)	63, 68, 69, 70, 71, 86, 87	Commenter requests to know if having a direct (first-party) relationship with a broker affects deletion scope because this may limit what data is deleted and what first-party data was retained so they can understand what was excluded from deletion. Commenter also requests to know whether all personal information, including inferences and third-party data, was deleted when a match occurred.	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.

		<p>Commenter further requests to know which statutory exemptions were invoked to retain personal information so they can evaluate the broker’s justification, as well as requests to know whether brokers misinterpret or misrepresent what “delete” means because this affects whether deletion was properly executed.</p> <p>Additionally, commenter requests to know what personal information was shared with service providers and whether it was the minimum necessary.</p> <p>Commenter requests a warning that deleting or opting out of personal information may result in exclusion from datasets used for eligibility or policy decisions.</p>	
7614(a)(1)	54, 72	<p>Commenter requests the exact date and time a data broker reports the status of each deletion request to track whether status changes were reported for new or amended requests</p> <p>Commenter requests to understand how cascading deletes work across brokers and third parties stating that deletion timing may vary and affect completeness.</p>	While not on the proposed modifications, the Agency notes commenter’s suggestion and looks forward to continuing to work with stakeholders on future policy development.
7614(b)(2)	52, 53, 55, 56, 57, 58	<p>Commenter requests an explanation when a data broker cannot verify a request due to multiple consumers matching the same identifier so they can understand and potentially remedy the issue; to know if their identity has been linked to another individual to protect themselves from harm such as identity theft or data loss; and to know if a shared identifier caused their records to be deleted or opted out so they can re-opt in using a different identifier if needed.</p> <p>Commenter requests the transaction ID and response code for each deletion request to serve as proof that the request was submitted and processed. Commenter also requests access to a comprehensive asset inventory of each data broker’s records to verify whether personal information was deleted or withheld.</p>	While not on the proposed modifications, the Agency notes commenter’s suggestion and looks forward to continuing to work with stakeholders on future policy development.

		Commenter further requests clarification on whether response codes are being misinterpreted or misapplied because they cannot verify deletion without knowing the correct code.	
7615(a)(2)	76, 88, 93	Commenter requests assurance that agents have adequate security and governance controls for DROP information and can delete it upon revocation. Commenter also requests to know whether personal information was deleted after a broker ceased operations or completed its final audit. Commenter further requests a process for agents to delete all consumer information obtained from DROP upon revocation of authorization.	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
7616(b), 7610(a)(1)(A-D)	77	Commenter requests clarification on consumer and agent responsibilities for securing DROP data and whether the consumer is liable for agent misuse.	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
7616(c)	90, 91	Commenter requests a designated method for brokers to contact their authorized agent instead of the consumer directly.	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
7620(a-b)	30, 41, 59, 89, 92	Commenter requests more detail regarding what information will be required to create a DROP account so that they can better decide if they want to use it. Commenter further requests a way to submit deletion requests to brokers outside of DROP if they opt out of using the platform. Commenter requests a way for agents to submit deletion requests outside of DROP if the consumer opts out of using the platform. Commenter requests clarification on how consumers submit their deletion requests through the DROP so they can use the system in a manner consistent with the regulations. Commenter also requests to know what personal information can be added to deletion requests and what constraints apply so they can improve match accuracy.	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.

		Commenter further requests to be notified of any breach of security involving personal information provided through the DROP.	
7620(a) & (b), 7621(b), 7616(c)	2, 3, 4, 5, 6, 7, 28, 99	<p>Commenter asserts that the modified rules do not require verification of authorized agents to submit DROP requests on behalf of California residents, which will result in unauthorized data deletion and raise constitutional and statutory concerns.</p> <p>Commenter argues that although the revised regulations now require the Agency to verify deletion requests, they do not incorporate reasonable agent verification mechanisms and prohibit data brokers from contacting consumers to verify their requests, which arguably violates the APA and conflicts with existing law. Specifically, commenter indicates that the Delete Act incorporates the CCPA definition of "authorized agent," which includes a reference to the agency being authorized to act on the consumer's behalf subject to the requirements in the CCPA regulations. The CCPA regulations permit businesses to verify an agents' authority to act, such as signed proof, as well as confirm with delete request with the consumer. However, the DROP regulations prohibit the verifications allowed by the CCPA. Commenter states this allows agents to submit requests on behalf of consumers without authorization, which raises inconsistencies across the regulatory regimes and increases the likelihood of fraudulent requests.</p> <p>Commenter states without authorized agent safeguards, there will be no deterrent for entities to use coercive methods, dark patterns, or other tactics to persuade consumers to give authority to act or to act without the knowledge of a consumer. Additionally, there will be no way to regulate bad actors who use the DROP to gain a competitive advantage over data brokers with competing</p>	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.

		models. Commenter requests the CPPA not allow agents to self-certify their authority.	
7620(d)	60	Commenter requests a process to cancel deletion requests submitted by an agent after revoking the agent's authorization to prevent further action on their behalf.	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
7621	8, 100, 110, 111	<p>Commenter warns that failure to provide for reasonable authorized agent verification conflicts with the CCPA regulations. Failure to align DROP with CCPA verification standards could violate the California Administrative Procedure Act and raise constitutional concerns because commenter states that inconsistencies between the DROP and CCPA regulations may render the DROP rules invalid under the APA and infringe on First Amendment rights related to data processing. Commenter requests that the CPPA establish verification standards for authorized agents because commenter states that the current rules lack credentialing or proof-of-authorization requirements. Commenter recommends distinguishing between personal and commercial agents and requiring commercial agents to undergo credentialing and oversight.</p> <p>Commenter states the sale, use, and disclosure of consumer personal information is protected expression and that the regulations are content-based regulation that fails any level of scrutiny. Commenter asserts the verification standards allow authorized agents to make mass deletions, which render the regulations more extensive than necessary advance the State's privacy interests.</p> <p>Commenter states their belief that there are better-tailored and more-effective alternative approaches that better serve the state's interests. Comment asserts that privacy is not a substantial state interest to be achieved by the restriction on speech.</p>	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.



		Commenter also requests a safe harbor for data brokers against liability resulting from unauthorized deletions initiated by unverified or unauthorized agents.	
7621(a-b)	32	Commenter requests confirmation that a notarized statement is sufficient to prove an agent’s authority because they cannot afford legal counsel and need a low-cost, legally valid method.	While not on the proposed modifications, the Agency notes commenter’s suggestions and looks forward to continuing to work with stakeholders on future policy development.
7621(a-b)	42	Commenter requests clarification on how authorized agents submit deletion requests through the DROP so they can instruct their agents to act in compliance with the regulations.	While not on the proposed modifications, the Agency notes commenter’s suggestions and looks forward to continuing to work with stakeholders on future policy development.
7621(b), 7616(c)	33	Commenter requests the ability to register multiple authorized agents with distinct roles, asserting that different agents specialize in different privacy rights (e.g., opt-outs vs. medical records).	While not on the proposed modifications, the Agency notes commenter’s suggestions and looks forward to continuing to work with stakeholders on future policy development.
7621(a–b), 7622	34, 35, 36, 37, 38, 39	<p>Commenter requests to prohibit their agent from accessing or sharing sensitive documents like a Real ID, driver’s license, or passport and instead use the same personal data elements and authoritative sources the Agency uses to verify identity; for authorized agents be allowed to submit residency classification review requests on behalf of consumers if the process is too complex or time-consuming; and what authorization an agent needs to truthfully sign under penalty of perjury on behalf of the consumer to ensure legal compliance; and that the Agency notify the consumer’s authorized agent directly when residency is verified because all correspondence is routed through the agent;</p> <p>Commenter also requests to use the Agency’s residency determination to correct conflicting residency data reported by data brokers, which commenter states may affect eligibility for rights or services; documentation from the Agency confirming that residency has been verified so they can push back on organizations that demand excessive verification; and clarity on what kind of documentation the Agency may</p>	While not on the proposed modifications, the Agency notes commenter’s suggestions and looks forward to continuing to work with stakeholders on future policy development.

		request to substantiate California residency to avoid being asked for irrelevant or intrusive information	
Automated Decisionmaking Technology	103	Commenter requests that the CPPA adopts its regulations for the ADMT/AI rulemaking package.	While not on the proposed modifications, the Agency notes commenter's support for its Automated Decisionmaking Technology regulations.
Assistance	102	Commenter requests help for their situation and states they cannot explain the details because of their job.	While not on the proposed modifications, the Agency notes the comment. If commenter believes a violation of the CCPA or Delete Act is occurring, commenter may wish to file a complaint with the Agency.
Contractors	78	Commenter requests to know what authorization an organization maintains to process personal information in contracts with third parties.	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
Correction of Data	45	Commenter requests the right to correct personal data, such as spelling of name, within data the records maintained by a data broker.	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
General Comment	46	Commenter requests the ability to correct misspelled names in first-party records so that identifiers can be accurately associated with both correct and incorrect data.	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
General Comment	66	Commenter requests to know how long each personal data element or attribute was retained by the data broker so they can assess whether deletion was complete and challenge violations of retention policies or claims of deletion.	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
General Comment	75	Commenter requests a way to monitor authorized use of DROP to track agent activity, detect shared identifier impacts, and prevent unauthorized use.	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
General Comment	107	Commenter requests regulations that provide more specific guidance on security measures for handling consumer deletion lists. Commenter requests clear consequences for data brokers failing to maintain the required level of security.	While not on the proposed modifications, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.

General Comment	116	<p>Commenter requests that the CPPA provide consumers with clear notice and options regarding the potential consequences of deleting professional or business-related data through the DROP because of concerns that consumers may unintentionally remove themselves from professional databases—such as those used for B2B sales or recruiting—without understanding the impact on their visibility and economic opportunities. Commenter proposes that the CPPA amend the regulations to: (a) offer deletion options for personal, professional, or both categories of data; (b) include a warning on the DROP interface stating, “This deletion may affect your visibility in professional databases”; and (c) implement a post-deletion notification and restoration mechanism.</p>	<p>While not on the proposed modifications, the Agency notes commenter’s suggestion and looks forward to continuing to work with stakeholders on future policy development.</p>
Legislation	104	<p>Commenter requests legislation to protect consumers from companies weaponizing consumer information against consumers such as doxxing, stalking, and threats.</p> <p>Commenter states the Penal Code is insufficient because law enforcement will not act unless there is a direct threat and the threshold for criminal charges is higher.</p>	<p>While not on the proposed modifications, the Agency notes commenter’s suggestion and looks forward to continuing to work with stakeholders on future policy development.</p> <p>However, the Agency does not have the authority to enact legislation, rather that authority rests with the Legislature and Governor.</p>