California Privacy Protection Agency

Initial Statement of Reasons: Data Broker Updates and DROP Audits

Title 11. Law
Division 6. California Privacy Protection Agency
Chapter 3. Data Broker Registration and Accessible Deletion Mechanism

Sections Affected: California Code of Regulations, title 11, sections 7601, 7602, 7603, 7604, 7610, 7612, 7613, 7614, 7615, 7616, 7620, 7621, 7630, 7631, 7632, and 7633.

Problem Statement

The California Privacy Protection Agency (Agency) implements and enforces the Delete Act. (Civ. Code, § 1798.99.80 et seq.) The Delete Act requires the Agency to maintain a public data broker registry and establish an accessible deletion mechanism that allows a consumer, through a single verifiable request, to require every registered data broker to delete personal information related to that consumer. (Civ. Code, § 1798.99.86(a).) Every data broker is required to access the deletion mechanism at least once every 45 days, retrieve and process deletion requests, and continue to delete newly collected personal information for consumers who have submitted requests. (Civ. Code, § 1798.99.86(c), (d).) Civil Code section 1798.99.87(a) authorizes the Agency to adopt regulations to implement these statutory requirements.

The Agency adopted regulations implementing the data broker registry, which became effective on January 1, 2025, and regulations governing the accessible deletion mechanism, which became effective on January 1, 2026. (Cal. Code Regs., tit. 11, §§ 7601–7622.) The Agency launched the accessible deletion mechanism, known as the Delete Request and Opt-out Platform (DROP) on January 1, 2026, and consumers immediately began submitting deletion requests through the DROP (DROP request). As of November 1, 2026, more than a half million consumers have submitted DROP requests containing almost three million individual consumer identifiers to 680 data brokers with active accounts in the DROP.

Since the DROP has become operational, the Agency identified several areas where the existing regulations could better align with the platform's functionality or with data brokers' operational realities. Because the initial regulations were adopted before the DROP was operational, certain provisions do not account for the more fully developed functionality of the DROP or issues that have come to the Agency's attention as consumers and data brokers use the system.

Data brokers have also raised recurring questions about definitions, scope of obligations, hashing and matching procedures, deletion requirements, suppression-list maintenance, and reporting. These issues reveal areas of confusion that could interfere with consistent and privacy-protective processing of DROP requests.

Separately, the Delete Act requires data brokers to undergo an independent third-party audit every three years beginning January 1, 2028. (Civ. Code, § 1798.99.86(e).) The statute does not specify essential audit parameters, including timing, scope, the qualifications and independence of auditors, the evidence required, or the contents of the audit report. Without regulations, audits would vary widely in rigor, comparability, and value, providing little assurance to consumers or useful information to the Agency and leaving data brokers uncertain about compliance expectations.

The Agency issued an Invitation for Preliminary Comments related to DROP audits and received 12 written comments consisting of 77 pages of input from data brokers, ad-tech companies, trade associations, nonprofits, individuals, and small businesses. Commenters emphasized auditor qualifications and independence, the importance of evidence over assertion, backups and downstream deletion requirements, and scope discipline. Agency staff also conducted comparative research, consulted academics, and engaged other agencies. The proposed regulations were developed after careful consideration of that information and input.

The Agency proposes to amend section 7601 through 7604, 7610, 7612 through 7616, 7620, and 7621 to better align the regulations to DROP and data broker operations, define terms, and to clarify data brokers' ongoing obligations. The Agency also proposes adopting proposed Article 5, consisting of sections 7630 through 7633, which establishes the timing, auditor qualifications and independence standard, scope, evidence standard, and report contents for the audits required by Civil Code section 1798.99.86, subdivision (e).

Anticipated Benefits

The proposed amendments to sections 7600 through 7622, together with the proposed adoption of Article 5, update the regulatory framework governing data broker registration, DROP access, DROP deletion request processing, and the statutory requirement that data brokers undergo periodic compliance audits. When the Agency first adopted regulations implementing the Delete Act, the DROP had not yet been fully developed, and several provisions reflected early assumptions about how the system would function. Since the DROP's launch, the Agency has gained substantial experience operating the system, responding to data broker inquiries, and observing where the regulatory text could more closely align with the DROP's more fully developed functionality. The proposed amendments to Articles 2, 3, and 4 address those issues by clarifying definitions, correcting outdated terminology, improving internal consistency, and ensuring that the requirements governing registration, DROP account creation, deletion list selection, access obligations, processing, suppression list maintenance, and status reporting account for progress in implementation, data broker operational realities, and issues that have arisen since the regulations were initially adopted.

Proposed Article 5 implements Civil Code section 1798.99.86, subdivision (e), which requires data brokers to undergo an independent third-party audit of their compliance

with deletion processing obligations beginning January 1, 2028, and every three years thereafter. Because the statute mandates audits but does not specify how they must be conducted, who is qualified to perform them, what specific components of processing they must evaluate, or what the audit report must contain, regulations are necessary to provide this structure. The proposed regulations establish predictable timing rules for the first audit cycle and the subsequent three-year cycles, set qualification and independence standards to ensure competent and objective auditors, and identify the key elements of deletion processing that every audit must assess, including deletion list selection, DROP access timeliness, standardization and hashing procedures, matching accuracy, deletion and opt-out actions, status reporting, suppression list maintenance, and instructions to service providers. These requirements ensure that audits evaluate actual performance rather than internal policies alone. The regulations also specify the required contents of the audit report, including findings, documentation of noncompliance, and certifications by both the auditor and executive management. Together, these provisions create a comprehensive audit framework that supports accountability, transparency, and enforceability.

The combined proposed amendments and new regulations create a clearer, more accurate framework that advances the Delete Act's purpose. Consumers benefit by gaining more reliable deletion processing, stronger data minimization protections, and independent verification of data broker compliance. Data brokers benefit by receiving clearer, system-aligned requirements. The Agency benefits from regulations that strengthen enforcement, improve communication, and provide the definitional and structural foundation needed for DROP audits beginning in 2028. Together, these proposed changes produce a coherent, workable regulatory scheme that reflects operational experience, incorporates stakeholder feedback, and fulfills the Delete Act's statutory mandates.

Specific Purpose, Necessity, and Rationale of Each Proposed Change

The Agency proposes amending sections 7601, 7602, 7603, 7604, 7610, 7612, 7613, 7614, 7615, 7616, 7620, 7621 and adopting sections 7630, 7631, 7632, and 7633 of Division 6, of Title 11, of the California Code of Regulations.[1]

Amend § 7601. Definitions.

The proposed amendments to section 7601 add eleven definitions, amend three existing definitions, and re-letter the remaining subsections. The new definitions are necessary because proposed Article 5 and amendments to Article 3 use terms that describe how the DROP operates and how audits will be conducted, and several existing provisions depend on concepts that the current regulations use without defining. Providing definitions makes the regulations clearer and more readable, thus, leading to increased compliance.

[1] All further references are to Title 11 of the California Code of Regulations, unless otherwise indicated.

Proposed amendments to subsection (b) revise the definition of “access session” to replace “communicates a status” with “reports a status,” “deletion request” with “DROP request,” and delete “logs out of its DROP account or.” The first change conforms the definition to the terminology of section 7614. The second uses the newly defined term “DROP request,” which excludes requests a consumer has cancelled and creates a shorter method for referring to a consumer deletion request made through the DROP, which creates greater consistency and precision throughout the regulations. These changes do not alter the substance of the definition. The final change ensures that account activity, such as logging in and out, is separate from completing an upload or download as required by the law.

Proposed subsection (c) defines “auditor” as the third party conducting the audit of the data broker who meets the requirements of section 7613 subsection (a), ensuring independence, competence, and uniformity across audits as required under Civil Code section 1798.99.86, subsection (e)(1). Without this definition, the regulations would lack clarity regarding who is authorized to conduct DROP audits, increasing the risk of inadequate or non-compliant audit practices. It additionally makes clear that a person who does not meet the qualification requirements is not an “auditor” for the purposes of a Delete Act audit.

Proposed subsection (d) defines “audit period” as the period of time assessed for purposes of the audit required by Civil Code section 1798.99.86. Without this definition, data brokers and auditors could apply inconsistent audit periods, undermining comparability and enforcement. A defined term also avoids confusion between the period being audited and the period during which the audit work is performed.

Proposed subsection (e) defines “batch” as the consumer deletion list or lists that a data broker downloads during a single access session. This definition is necessary because the DROP operates on batch-based retrieval and reporting, meaning that the DROP delivers all of a data broker's selected lists as part of a single download. For example, a data broker that has selected email address and phone lists retrieves one batch that contains both lists and must report on the status of every identifier in their downloaded lists within a mandated number of 30 days. Without this definition, the batch-based structure of the DROP could be misinterpreted, leading to inconsistent compliance, processing, and audits.

Proposed amendments to subsection (f), formerly subdivision (c), revise the definition of “consumer deletion list” to describe the list as including the applicable identifier in hashed format and the work item ID. The replacement of “transactional identifier” with “work item ID” is necessary because the DROP assigns a unique value to each hashed identifier and each ID must be separately processed. The definition updates the regulations with the term that appears in the system and its technical documentation and thus eliminates a source of confusion that the Agency observed during sandbox testing. The reference to “identifier” uses the new defined term in the proposed subsection (o) for clarity.

Proposed subsection (g) defines “data broker ID” as a unique identifier for each data broker within the DROP, which supports audit tracking, reporting, and enforcement. Without this definition, the regulations would lack a standardized mechanism for identifying data brokers across the DROP operations.

Proposed subsection (h), defines “Delete Request and Opt-out Platform” or “DROP” and moves this definition formerly found in subsection (e) without regulatory effect. This re-lettering is necessary to place it within the definitions alphabetically.

Proposed amendments to subsection (i), formerly subsection (d), re-letter the subsection without regulatory effect. This re-lettering is necessary to accommodate the incorporation of earlier definitions alphabetically.

Subsection (e) is proposed to be repealed as the definition contained in original subsection (e) has been moved to proposed subsection (h) to place it within the definitions alphabetically and the definition of “batch” is proposed to be subsection (e) to accommodate the incorporation of it alphabetically.

Proposed amendments to subsection (i), formerly subsection (e), re-letter subsection without regulatory effect. This re-lettering is necessary to accommodate the incorporation of earlier definitions alphabetically.

Proposed amendments to subsection (j), formerly subsection (f), revise the definition of “DROP account” by striking “DROP system” and replacing it with “DROP.” This amendment is necessary to eliminate redundant phrasing because DROP stands for the “Delete Request and Opt-Out Platform” and adding “system” after platform is redundant.

Proposed subsection (k) defines “DROP audit” as an audit of the data broker’s deletion request processing pursuant to Civil Code section 1798.99.86 and specifies that a DROP audit begins on the first day of the audit period and concludes on the day the DROP audit report is complete. This is necessary to ensure that data brokers and auditors understand what the audit evaluates, the DROP deletion request processing, and the time period covered. The reference to “audit period” uses the new defined term in the proposed subsection (d).

Proposed subsection (l) defines “DROP audit report” as a written document that describes the DROP audit and contains all components required by section 7633. This is necessary because Civil Code section 1798.99.86, subdivision (e)(2), requires a data broker to submit “a report resulting from the audit” to the Agency within five business days of a written request and defining the report by reference to section 7633 tells data brokers what needs to be in the report.

Proposed subsection (m) defines “DROP request” as a consumer deletion request submitted through the DROP that has not been cancelled by the consumer. This is necessary to distinguish active DROP requests from cancelled ones, which is essential to tell a data broker which requests must follow the obligations for processing, reporting, and suppression list maintenance under sections 7613 and 7614. Using a single defined

term avoids repeating the qualification “that has not been cancelled” in each provision and makes clear that the regulations’ obligations only apply to active requests.

Proposed amendments to subsection (n), formerly subsection (g), re-letter subsection without regulatory effect. This re-lettering is necessary to accommodate the incorporation of earlier definitions alphabetically.

Proposed subsection (o)(1) defines “identifier” as a single piece of personal information provided by the consumer, such as a phone number or email address. This definition is necessary to clarify the simplest form of identifier used in the DROP matching and to ensure uniform hashing and comparison practices.

Proposed subsection (o)(2) defines “identifier” created from multiple pieces of personal information combined pursuant to section 7613(a), such as a combination of name, date of birth, and zip code. This is necessary because the DROP provides two kinds of lists: lists built on a single identifier and lists built on a composite of several pieces of personal information that are hashed individually and then hashed together and a data broker must match based on identifiers rather than raw personal information. The definition clarifies that, for composite lists, the identifier is the combined value created under section 7613, subsection (a), and it supports the list-selection rule in section 7610, subsection (a)(3), which now refers to the "type of identifier" in a data broker's records.

Proposed amendments to subsection (p), formerly subsection (h), re-letter the subsection without regulatory effect. This re-lettering is necessary to accommodate the incorporation of earlier definitions alphabetically.

Proposed amendments to subsection (q), formerly subsection (i), re-letter the subsection without regulatory effect. This re-lettering is necessary to accommodate the incorporation of earlier definitions alphabetically.

Proposed amendments to subsection (r), formerly subsection (j), re-letter the subsection without regulatory effect. This re-lettering is necessary to accommodate the incorporation of earlier definitions alphabetically.

Proposed subsection (s) defines “registration confirmation number” as the confirmation number provided to a data broker after it has successfully completed its annual data broker registration in January. This definition is necessary to support tracking and verification of completed registrations and to ensure that data brokers can reliably identify their registration submissions.

Proposed amendments to subsection (t), formerly subsection (k), re-letter the subsection without regulatory effect. This re-lettering is necessary to accommodate the incorporation of earlier definitions alphabetically.

Proposed amendments to subsection (u), formerly subsection (l), re-letter the subsection without regulatory effect. This re-lettering is necessary to accommodate the incorporation of earlier definitions alphabetically.

Proposed subsection (v) defines "suppression list" as the information for all consumers who have submitted a DROP request that a data broker maintains in accordance with section 7613, subsection (b), and provides that a suppression list may be comprised of multiple lists if together the lists include information for all consumers who have submitted a DROP request for the data broker. This is necessary because Civil Code section 1798.99.86, subdivision (d), requires a data broker to ensure each consumer remains deleted, and to not sell or share newly collected personal information about the consumer. A data broker can only meet that obligation if it keeps a record against which to screen incoming data. Existing section 7613, subsection (b)(1)(B) already requires that the record be kept but do not explicitly use the term "suppression list," which has created confusion for data brokers. The term "suppression list" is the term data brokers themselves use for this record, and the Agency received requests for further clarification of this requirement. The second part of the sentence is necessary because many data brokers maintain personal information in multiple systems or match on some identifier types but not others, and therefore, must maintain more than one list to accurately effectuate the requirement. This is clarifying that this practice is not only allowable or best practice but required by law.

Proposed subsection (w) defines "work item identifier" or "work item ID" as the alphanumeric character string that represents a single consumer identifier assigned by the DROP. This is necessary because the DROP assigns a unique, permanent alphanumeric identifier to each hashed consumer identifier it delivers, and a data broker must return that identifier with a status to report how it processed that request. The existing regulations call this value a "transaction identifier," but that term can be confusing because the identifier is permanent and not based on a single transaction. Adopting the system's own term is necessary to eliminate confusion and to ensure that status uploads are formatted correctly. The definition also supports the audit requirement in section 7632, section (e)(7), where the auditor assesses whether the data broker assigned and reported the correct status for each work item ID.

Amend § 7602. Registration Submission Requirements.

Proposed amendments to section 7602 repeal subsection (c), which provides that a data broker cannot amend or withdraw a completed registration after January 31 except as set forth in section 7604. This repeal is necessary because proposed section 7604, subsection (b), establishes a procedure by which a data broker that discovers after the registration period closes that its registration is inaccurate or incomplete must withdraw the deficient submission and submit an accurate and complete registration.

Amend § 7603. Registration Information Requirements.

Proposed amendments to subsection (a) replace "correct" with "accurate" to conform with the terminology used in other sections, including section 7602, subsection (b),

which references “accurate information”. This amendment is necessary to ensure consistency with terminology used throughout the Chapter. Additionally, a sentence is added providing that a data broker shall only be deemed registered in compliance with Civil Code section 1798.99.82 if the data broker has provided complete and accurate information. This is necessary to make clear that a registration that omits or misstates the required information does not provide the transparency the statute requires. Indeed, the Legislature indicated that it perceives the transparency of this law important and high priority when it passed Senate Bill (SB) 361 (2025), which increased the number of disclosures required as part of registration. This sentence tells data brokers that an incomplete or inaccurate submission does not satisfy the statutory obligation, and it works together with proposed section 7604, subsection (b), which tells data brokers how to cure a deficient submission.

Proposed amendments to subsection (d) replace “When reporting” with “When providing to the Agency” and update the statutory cross-reference to include the additional subdivision cited. The first change is a clarification that the described information is provided to the Agency as part of the registration process and to ensure that the cross-references accurately reflect the statutory provisions governing the required disclosures. The note is amended to add Civil Code section 1798.99.85 as a reference because the metrics compiled under that section are part of the registration information governed by this section.

Amend § 7604. Changes to Registration Information After Registration Period Closes.

Proposed amendments to the section title add “Removal from the Registry and” to the beginning of the title so it accurately describes subsection (a), which governs removal of an erroneously registered business from the registry. This amendment is necessary to reflect that the section governs both removal from the publicly posted registry in cases of erroneous registration and changes to registration information after the registration period closes.

Proposed subsection (b) replaces the prior text with new language providing a clear procedure for correcting a registration after the registration period closes. If a data broker determines that its registration contains inaccurate or incomplete information, it must withdraw the incorrect submission and submit an accurate and complete registration. To withdraw, the data broker must submit to the Agency a written request explaining what information is inaccurate or incomplete and provide the accurate and complete information through its DROP account. These changes are necessary to establish a clear process for correcting erroneous registrations. An inaccurate registry misinforms consumers who rely on it to understand which businesses hold their personal information. A written request is necessary so the Agency has an accurate record of what was wrong and why. Additionally, this subsection clarifies that the data broker’s registration date shall be the date the data broker submitted the registration with the accurate and complete information, which describes how the Agency determines the effective registration date when a corrected submission is required. This

change promotes the submission of accurate and complete registration information and prevents registrants from circumventing or delaying compliance with statutory requirements through incomplete filings.

Amend § 7610. Delete Request and Opt-Out Platform Creation.

Proposed amendments to the subsection title replace “Opt-Out” with “Opt-out” without regulatory effect. This amendment is necessary to ensure consistent capitalization of a defined term and a uniform appearance across the Chapter.

Proposed amendments to subsection (a) replace www.cppa.ca.gov with “privacy.ca.gov” as the Agency website because the data broker portal for DROP is hosted at privacy.ca.gov. These amendments are necessary to ensure data brokers use the correct website to create DROP accounts and to avoid confusion and misdirected web traffic.

Proposed amendments to subsection (a)(2) require the account information a data broker provides be “accurate and complete.” This conforms the account creation standard to the registration standard proposed in section 7603, subsection (a). This is necessary because the Agency relies on the account information to communicate with data brokers about compliance, and the public relies on the registry for accurate information to learn more about data brokers.

Proposed subsection (a)(2)(F) adds a new requirement that data brokers provide a link to the specific webpage required by Civil Code section 1798.99.82(b)(2)(V). This amendment is necessary to ensure the Agency can verify compliance with statutory requirements and the webpage is updated and accurate for the public throughout the year.

Proposed amendment to subsection (a)(3) replaces “delete requests” with “DROP requests” without regulatory effect. This amendment is necessary to ensure consistent use of a newly defined term across the Chapter.

Proposed amendments to subsection (a)(3)(A) require a data broker to select all consumer deletion lists that contain an identifier that matches the type of identifier within the data broker’s records. This change incorporates the newly defined term “identifier” and clarifies that list selection must correspond to the types of identifiers maintained in the data broker’s records. It is necessary because data brokers must select a list even if they hold only some of the list’s composite components to ensure the highest number of possible matches. The amendments also ensure consistent terminology that aligns with the identifier-based structure of the DROP.

Proposed amendments to subsection (a)(3)(C) strike the final sentence limiting a data broker to changing its consumer deletion list selection once every 45 calendar days. This amendment is necessary to remove obsolete timing restrictions that no longer align with the updated the DROP access and retrieval framework. Additionally, operating experience has shown the limit can work against the statute’s purpose. A data broker

that, for example, begins collecting a new type of identifier or acquires a new database would have had to wait up to 45 days to retrieve deletion requests relevant to the newly acquired personal information under the existing rule, during which time requests from consumers with that identifier type go unmatched. Removing the limit allows data brokers to align their selections with their data in real time, which the Agency expects to increase match rates and therefore the number of consumer requests honored.

Proposed subsection (b) requires a data broker to update its DROP account with accurate and complete information within 10 business days if any of the information provided under subsection (a)(2) changes. This is necessary because the Agency relies on the point-of-contact information to notify data brokers of account security issues, connection failures, registration deficiencies, and written requests for audit reports. Ten business days are consistent with California practice in privacy and data sensitive operations. For example, the Agency's CCPA regulations require businesses to acknowledge consumer requests within 10 business days (§ 7021), and financial institutions must give at least 10 business days' prior notice of an office address change to the Commissioner of Financial Protection and Innovation. (Fin. Code, § 23021; Cal, Code Regs., tit. 10, § 10.6006.) Other licensing regimes likewise use 10-day windows for contact information updates, including gambling licensees (Cal. Code Regs., tit. 4, § 12004) and Early Learning & Care contractors (Cal. Code Regs., tit. 5, § 18014).

Amend § 7612. Delete Request and Opt-out Platform Access.

Proposed amendments to subsection (a) provide that a data broker must access the DROP and retrieve the DROP requests by downloading a batch at least once every 30 calendar days. This restates the statutory 30-day access requirement that becomes effective January 1, 2027, using the newly defined terms "DROP request" and "batch," and makes it explicit that the objective of the 30-day cycle is retrieving consumers' requests, not merely logging in or downloading files. These amendments are necessary to align the subsection with the revised DROP architecture and to ensure consistent terminology throughout Article 3.

Proposed amendments to subsection (b) use "retrieve" and "batch" in place of "download its selected consumer deletion list(s)," for consistency with subsection (a) and section 7601. The substance of the requirement is unchanged. These amendments are necessary to ensure consistent terminology and to further clarify the data broker's obligations when automated access is unavailable.

Proposed subsection (b)(1) adds a new provision requiring a data broker to notify the Agency immediately when it cannot access the DROP manually or through automated means and the failure is not caused by the data broker. This is necessary because the existing regulation addressed only the failure of an automated connection and assumed that manual access remained available. This amendment ensures timely communication with the Agency to allow prompt investigation of system related access issues.

Proposed subsection (b)(2), formerly subsection (b)(1), requires a data broker whose automated connection with the DROP fails, through no error of its own, to notify the Agency if the automated connection is not restored within three business days. A three-day restoration period was chosen because it aligns with established incident-response and reporting timelines in comparable regulatory regimes. For example, New York's cybersecurity regulations require notification within 72 hours, and SEC rules require disclosure of certain cybersecurity incidents within four business days. These benchmarks demonstrate that a three-day timeframe is both reasonable and consistent with prevailing regulatory expectations. These amendments are necessary to ensure timely reporting of connection failures. If the data broker reports in three business days rather than waiting a full 45 days, the Agency and the data broker may be able to fix the issue before the compliance deadline arrives. This ensures failures come to the Agency's attention as early as is reasonable.

Proposed amendments to subsection (c) provide that subsequent downloads will contain only the DROP requests received or altered after the data broker's most recent retrieval after a data broker downloads each consumer deletion list for the first time. These amendments are necessary to align terminology with the updated DROP and to further clarify that subsequent retrievals contain only new or altered DROP requests.

Proposed amendments to subsection (c)(1) allow a data broker, upon written request through its DROP account, to re-retrieve a complete or partial consumer deletion list for purposes of ensuring compliance, reconciling internal records, or completing the audit required by Civil Code section 1798.99.86. Adding "or partial" is necessary because a data broker that needs to reconcile a single list, a defined period, or the sample selected by its auditor may be able to avoid re-downloading every request ever submitted, when technologically feasible. Permitting partial re-retrieval reduces the volume of personal information transmitted and reduces the operational burden on the Agency. It also replaces "deletion requests" with "identifiers" without regulatory effect. This amendment is necessary to ensure consistent use of a newly defined term across the Chapter.

Amend § 7613. Processing Delete Requests.

Proposed amendments to section 7613 streamline and clarify the deletion request process for data brokers and integrate it into the DROP required under Civil Code section 1798.99.86. The proposed amendments reorganize the section so the steps appear in the order in which a data broker performs them, use the defined term "identifier" in place of the varying phrases referencing consumer information ("consumer identifier information," "consumer personal information," and "consumer identifier(s),"), add examples, conform the ZIP code rule to the DROP's standardization, clarify the scope of the comparison, define the suppression list obligations with greater precision, and require data brokers to share information with, and keep records of, the service providers and contractors that must act on consumers' requests.

Proposed amendment to the subsection title replaces “Delete Requests” with “DROP requests” without regulatory effect. This amendment is necessary to ensure consistent use of a newly defined term across the Chapter.

Proposed amendment to subsection (a) replaces “delete requests” with “DROP request” without regulatory effect. This amendment is necessary to ensure consistent use of a newly defined term across the Chapter

Proposed amendments to subsection (a)(1) require a data broker to compare the identifier type contained in each consumer DROP request with the same type of identifier maintained in the data broker’s records and add an example. These amendments are necessary to align the subsection with the DROP’s identifier-based matching framework and to clarify that matching is performed on standardized identifiers rather than raw personal information. The example provides guidance to data brokers illustrating how the comparison should be done, which is important to ensure the consumer DROP requests are honored and further clarify an area of inquiry by data brokers.

Proposed amendments to subsection (a)(1)(A) require a data broker, when formatting a ZIP code, to maintain only the first five characters and then remove any leading zeros and add an example. This amendment is necessary to ensure consistent standardization of ZIP codes across data broker systems and to increase the likelihood of accurate matches between DROP identifiers and the data broker’s records. Leading zeros are frequently lost when ZIP codes are stored as numbers in a table and the identifier provided by the Agency must match the business’s identifier exactly in order for the hashed versions of the identifier to match. Thus, even a single missing zero will prevent a match and removing the leading zeros should create a higher match rate. The example provides guidance to data brokers illustrating how a standardized zip code should look, which will increase match rates and further clarify an area of inquiry by data brokers.

Proposed amendments to subsection (a)(1)(B) change “consumer personal information within” to "the same type of identifier(s)" and remove a lengthy phrase with “records”. These amendments are necessary to ensure hashing is applied consistently to the correct identifiers and to improve the clarity by using the newly defined term, “identifier,” throughout the regulations.

Proposed subsection (a)(1)(C) moves the composite hashing rule from former subsection (a)(2)(A) to the standardization and hashing steps in subsection (a)(1), where it logically belongs, and language has been added to further clarify the order of the hashing steps. This is necessary to put the rule in sequence with the other hashing steps to create greater clarity for data brokers and auditors; if the sequence is not performed in the specific order, a data broker may inaccurately determine there is not a match between a DROP request and its records. Former subsection (a)(1)(C) is re-lettered as subsection (a)(1)(D) and is amended to use the defined term.

Proposed amendments subsection (a)(1)(D), formerly subsection (a)(1)(C), re-letter from subsection (a)(1)(C) and use the defined term. This is necessary to improve clarity by using the newly defined term throughout the regulations.

Proposed amendments to subsection (a)(2) delete the current language, which has become subsection (a)(2)(A) to put the steps the data broker must take in sequential order for clarity. The proposed new language clearly states that the data broker must compare standardized, hashed identifiers in its records to the identifiers in the consumer deletion list and to perform this comparison irrespective of how or where the identifier is maintained. This is necessary because data brokers commonly hold identifiers in multiple systems such as production, database, data warehouses, marketing platforms, archived files, and service providers' environments. If comparison is limited to one system, personal information would remain undeleted in the data broker's other systems. Civil Code section 1798.99.86, subdivision (b)(1)(c) requires the deletion of "all personal information related to the consumer and the existing definition of "delete" in 7613, subsection (b)(1)(c) already reaches archived and backup systems. It is necessary to make the scope of comparison explicit so data brokers design their matching process accordingly and so auditors have a clear standard against which to test.

Proposed amendments to subsection (a)(2)(A) provide that if the identifier in the data broker's records matches the identifier in the consumer deletion list, the data broker must delete all personal information associated with the matched identifier as described in subsection (b). This is necessary to clarify this requirement that was originally included in subsection (a)(2).

Proposed amendments to subsection (a)(2)(B) provide that if the identifier in the consumer deletion list matches the identifier for multiple consumers in the data broker's records, the data broker must opt each such consumer out of the sale or sharing of their personal information in accordance with Civil Code section 1798.99.86, subdivisions (c)(1)(B) and (D) and comply with the suppression list requirements in subsection (b)(1)(B) for all such consumers. This is necessary because it adds clarity by restating the existing rule in simpler language, in the sequence in which they are applied, and does not change the substance of the obligations.

Proposed amendments to subsection (b)(1)(B) use the defined term "suppression list" and specify what the list must contain and how it may be used. As amended, a data broker must continue to maintain a suppression list containing the minimum personal information necessary to comply with Civil Code section 1798.99.86, subdivisions (c) and (d), for each consumer who has submitted a DROP request, unless the consumer later alters or cancels the request. It clarifies that the suppression list does not have to include personal information, if the business does not need it to. The proposed amendments clarify that the suppression list may only be maintained for the sole purpose of complying with Civil Code section 1798.99.86 and this Chapter. The sentence formerly prohibiting other uses "unless a statutory exemption applies" is replaced by the "sole purpose" limitation. The statutory exemption language now

appears in proposed section 7616, subsection (a). These amendments are necessary to ensure consistent terminology and to clarify the scope and purpose of the suppression list.

Proposed amendments to subsection (b)(1)(B)(i), formerly subsection (b)(1)(B), clarify that for matched consumers, the information maintained on the suppression list need not be personal information the Agency provided through the DROP. The data broker may instead use its own internal identifiers, which the Agency understands is common practice today. This amendment is necessary to clarify the permissible sources of suppression list information and to prevent unnecessary retention of the DROP-provided personal information while preserving the ability to comply with ongoing comparison obligations.

Proposed subsection (b)(1)(B)(ii) clarifies that for consumers the data broker could not match, the data broker must maintain the personal information the Agency provided through DROP on its suppression list. This amendment is necessary to ensure unmatched DROP requests remain available for future comparisons under Civil Code section 1798.99.86, subdivision (d). A data broker that found no match has no internal identifier for the consumer, and therefore, without the DROP provided identifiers, it cannot match the consumer's personal information if it later acquires it.

Proposed amendments to subsection (c) require a data broker, for DROP requests that did not match any personal information in its records at the time of comparison, to compare all newly collected records with the suppression list required by subsection (b)(1)(B) before new information is sold or shared, unless the consumer later cancels the request. The text replaces existing text with newly defined "suppression list" and replaces "any" with "all" to remove the implication that screening some, but not all newly collected records would suffice. These amendments are necessary to align the subsection with the updated suppression list framework and to clarify that all newly collected records must be compared against the suppression list to ensure ongoing compliance with Civil Code section 1798.99.86, subdivision (d).

Proposed amendments to subsection (e) replace "may" with "must," clarifying that a data broker is required to share with service providers and contractors only the minimum personal information necessary to facilitate compliance with subsection (c) as data brokers have indicated concerns about whether they could or should share this information with service providers and contractors. Additionally, they add a requirement to keep a record of all service providers and contractors with whom this information is shared for at least six years. We selected a six-year retention period because the statutory enforcement period is five years, with an additional year included to provide administrative flexibility and ensure adequate time for compliance reviews and enforcement activities. These amendments are necessary to ensure data brokers share only the minimum necessary information to support compliance, to strengthen accountability through recordkeeping, and to ensure the data broker, its auditor, and the Agency can verify that the downstream direction required by the statute was actually given.

Amend § 7614. Reporting Status of Deletion Requests.

Proposed amendments to the subsection title replace “Deletion Requests” with “Identifiers” without regulatory effect. This amendment is necessary to ensure consistent use of a newly defined term across the Chapter.

Proposed amendments to subsection (a) require a data broker to report the status of every identifier in a batch by uploading to its DROP account within 30 days of retrieving the batch. The existing text required reporting “at each subsequent access session” of the statuses for requests “received during the previous access session,” which was ambiguous. These amendments are necessary to align the subsection with the updated batch retrieval structure of the DROP and to ensure consistent use of defined terms throughout Article 3. The 30-day timeframe aligns with the statutory requirement that a data broker must access the system at least every 30 days which becomes effective January 1, 2027. The amendments also strike obsolete language related to re-downloads, which is no longer applicable under the revised DROP architecture.

Proposed amendments to subsection (a)(1) state more directly the existing rule that a data broker that finds a matched identifier when comparing newly collected personal information against its suppression list under section 7613, subsection (c), must report the new status for that identifier during its next access session, and to conform the example to the defined terms. These amendments are necessary to clarify that status changes must be reported when newly collected personal information results in a match to an existing DROP identifier and to align the subsection with the updated identifier-matching framework.

Proposed subsection (a)(1)(A) adds a new provision clarifying that a data broker is not required to report a status change when a matched identifier is found before the data broker accepts or collects the associated personal information. This amendment is necessary to clarify the scope of reporting obligations and prevent unnecessary reporting when no personal information has been collected or processed. For example, some data brokers screen incoming data against their suppression list before they ingest data into their system and reject any matched records. In this case, the data broker has not collected the consumer’s personal information, so the previously reported status of “record not found” remains accurate, and reporting a change to “record deleted” would in inaccurate. This is also necessary to incentivize data brokers to screen at intake and, therefore, minimize the personal information collected by data brokers, which is the most privacy-protective way to comply with Civil Code section 1798.99.86, subdivision (d)(2).

Proposed subsection (a)(2) adds a new provision specifying that a data broker does not need to report statuses for DROP requests that have been cancelled. This amendment is necessary to ensure data brokers do not report statuses for requests that are no longer active, which is additional burden with little benefit.

Proposed amendments to subsection (b) replace references to “deletion requests” with “identifiers,” “transaction identifier” with “work item ID,” and “response code” with

“status.” These amendments are necessary to ensure consistent terminology throughout the DROP regulations and to reflect the updated structure of the DROP work items.

Proposed amendments to subsection (b)(1) replace “transaction identifier” with “work item ID” and “consumer deletion request” with “identifier.” These amendments are necessary to align the subsection with the defined terms used throughout Article 3.

Proposed amendments to subsection (b)(2) replace “response code” with “status,” replace “transaction identifier” and “deletion request” with “work item ID,” and revise phrasing to clarify that statuses describe the action taken with respect to each work item. These amendments are necessary to ensure consistent terminology and to clarify the reporting structure for the DROP work items.

Proposed amendments to subsection (b)(2)(A) require data brokers to report an identifier as “deleted” when any personal information associated with a matched identifier is deleted, even if some of the personal information is exempt from deletion. The amendment makes "record deleted" the correct status whenever non-exempt personal information was deleted and reserves "record exempted" (subsection (b)(2)(C)) for the case in which all of the personal information is exempt and nothing is deleted. This amendment is necessary to ensure accurate reporting when only part of the personal information associated with a matched identifier is exempt from deletion.

Proposed amendments to subsection (b)(2)(B) update terminology and clarify that the opt-out requirement must be applied to all consumers associated with a matched identifier, consistent with section 7613. This amendment is necessary to ensure consistency across the DROP regulations.

Proposed amendments to subsection (b)(2)(D) replace “match” with “matching identifier” and update cross-references. These amendments are necessary to ensure consistent terminology throughout these regulations.

Proposed amendments to subsection (c) replace references to “consumer deletion requests” with “their batch,” update terminology to reflect batch-based reporting, and revise phrasing to ensure consistency with the updated DROP structure. These amendments are necessary to align manual reporting requirements with the batch retrieval system.

Proposed amendments to subsection (c)(1) replace references to “deletion requests” with “identifiers,” replace “access session” with “batch,” and update terminology related to list retrieval. These amendments are necessary to ensure consistent terminology and to reflect the updated batch-based reporting process.

Proposed amendments to subsection (c)(2) provide that a data broker that uploads the status of its batch manually must report the status of identifiers received in its previous batch before downloading a new batch, and must report statuses in a machine-readable comma separated value (CSV) file reporting the correct status code and work item ID.

The proposed amendments clarify that within the DROP the upload file contains the work item ID and the status code, not the hashed identifier. This is necessary to ensure that manual uploads are accepted and consumers receive their statuses.

Amend § 7615. Requirements to Stop Accessing Deletion Requests from the DROP.

Proposed amendments to the subsection title replace "Deletion Requests" with "Consumer Deletion Lists" without regulatory effect. This amendment is necessary to ensure consistent use of terms across the Chapter.

Proposed amendments to subsection (a) and (a)(1) simply restructure the subsections so all of the steps a business must take when it ceases to operate as a data broker occur within 30 days of the business no longer operating as a data broker. The 30-day timeframe aligns with the statutory requirement that a data broker must access the system at least every 30 days which becomes effective January 1, 2027. Now, it applies to the same period to notice, the deletion of Agency-provided personal information, and the deactivation of the account. This is necessary for administrative clarity for the business and the Agency and to ensure the information the Agency provided does not remain with a business who no longer needs it. It eliminates the redundant phrasing "meets the definition of" data broker because "operating as" a data broker is sufficient. For clarity, "the business" is moved to replace "it" as the end of the sentence.

Proposed amendments to subsection (a)(2) require the business to delete the personal information provided by the Agency through the DROP, including all DROP requests received up to the effective date on which the business notifies the Agency that it no longer meets the definition of data broker. This replaces the existing rule, under which a business could retain that information until 30 days after completing registration for its last year as a data broker or after concluding its final audit, whichever was later. These amendments are necessary to ensure data minimization by shortening the time period for deletion of personal information by businesses that no longer have a need business need for the personal information and to align the subsection with the updated audit and DROP frameworks.

Proposed amendments to subsection (b) replace the requirement that a business that has previously deactivated its account create a new DROP account with an option for the business to request reactivation of a prior account or the creation of a new account. The revised language clarifies that the Agency may request the business's most recent audit before reactivation. This is necessary because the existing text required creation of a new account in every case, which would sever the history associated with the business's data broker ID. Allowing the Agency to preserve that history will assist the Agency in tracking registration, processing, and audit cycles across periods of data broker activity. Allowing the Agency to request the most recent audit is necessary to prevent a business from evading the audit requirement by deactivating its account before an audit is due and then reactivating it afterwards.

Amend § 7616. Additional Data Broker Requirements.

Proposed amendments to subsection (a) add references to information contained in a data broker's suppression list and clarify that personal information provided by the Agency may only be used for compliance with Civil Code section 1798.99.86 and this Chapter unless a statutory exemption applies. These amendments are necessary to clarify the scope of permissible uses of DROP-provided personal information and to ensure consistent terminology across the DROP regulations. Additionally, as the suppression list may consist of personal information that was not DROP-provided, this clarifies that data brokers may maintain this personal information to fulfill their ongoing obligation to ensure they do not add personal information into their records for a consumer who has already submitted a DROP request.

Amend § 7620. Consumer Deletion Requests.

Proposed amendments to subsection (d) replace certain terms to align the subsection with the terminology used throughout the DROP regulations and strike redundant language. The word "amend" is replaced with "alter" because the statute uses "alter" in Civil Code section 1798.99.86, subdivision (a)(4). These amendments are necessary to ensure consistent use of defined terms, improve clarity, and remove phrasing that is no longer needed because all DROP requests are necessarily submitted through the DROP. The amendments do not change the meaning or effect of the provision and do not alter consumer rights or Agency obligations.

Amend § 7621. Authorized Agents.

Proposed amendments to subsections (a), (b), and (c) replace the term used to describe the type of request with the defined term "DROP request." These amendments are necessary to ensure consistent terminology throughout Article 3 and to align the subsection with the defined terms used elsewhere in the Chapter. The amendment does not change the substance of the provisions.

Adopt Article 5. Deletion Request and Opt-out Processing Audits

Proposed Article 5 establishes the requirements for DROP audits, including audit timing, auditor qualifications and independence, audit scope and required assessments, and audit report content. These provisions are necessary to implement Civil Code section 1798.99.86, subdivision (e), which requires data brokers to undergo an independent third-party audit every three years beginning January 1, 2028. Article 5 provides clarity regarding when audits must occur, who may conduct them, what components of DROP deletion request processing must be tested, and what information must be included in the audit report. The Agency modeled the structure of Article 5 on Article 9 of Chapter 1 of this Division which addresses cybersecurity audits (§§ 7120-7124), adapting its provisions on auditor qualifications and independence, scope and thoroughness, evidence, and report contents to the narrower subject of DROP request processing. Where the two frameworks differ, the difference is to address differences in the Delete Act and the California Consumer Privacy Act (CCPA). For example, the requirements for DROP audits include that the auditor must be an independent third party rather than an internal auditor, and the cycle is triennial rather than annual. The Article's title accurately

reflects the audit requirements contained within it, which is necessary to ensure the regulations are clear, logically organized, and easily understood by data brokers, auditors, and the public.

Adopt § 7630. Timing Requirements for DROP Audits, Audit Reports, and Certifications.

Proposed section 7630 establishes when a data broker must complete its first DROP audit and each subsequent audit, as well as the period each audit must cover. The statute fixes the start of the audit requirement at January 1, 2028, and its frequency at every three years, but does not specifically state the audit period or the date by which a report must be completed. This section is necessary to provide data brokers and auditors with specificity to ensure common time frame for audits and that the audit reports are comparable.

Proposed subsection (a) establishes the timing and audit period for the first DROP audit for any business that meets the definition of "data broker" at any point between August 1, 2026, and December 31, 2027. This subsection is necessary because Civil Code section 1798.99.86, subdivision (e) requires data brokers to undergo an audit beginning January 1, 2028, but does not specify when the first audit must be completed or what period it must cover. The proposed subsection provides clarity by requiring completion of the first audit report no later than November 1, 2028, and defining the audit period as August 1, 2026, through August 1, 2028. The beginning of the audit period, August 1, 2026, is the date on which the Delete Act required data brokers to begin accessing the DROP to process requests, thus, beginning the first audit period on that date is necessary to ensure that the first audit covers the entirety of each data broker's processing. The first audit is a two-year audit period, rather than three, so that the first audits are completed during 2028, the first year in which the statute requires an audit. The 90-day interval between the end of the audit period and the report deadline is necessary to be consistent with subsections (b) and (c) and cybersecurity audit reports, provides auditors time to complete fieldwork on the final cycles of the period and to prepare the report, and ensures reports are completed within a reasonable time period after the close of the audit period. A uniform deadline for all existing data brokers is necessary so the resulting reports are comparable.

Proposed subsection (b) establishes the timing and audit period for data brokers that begin operating after December 31, 2027. This subsection is necessary because the statutory audit requirement applies to all data brokers, including those that begin operations after the initial implementation period, and the statute does not specify how the first audit cycle applies to new entrants. The subsection provides clarity by requiring a 12-month audit period beginning on the first day the business meets the definition of "data broker," and requiring completion of the audit report within 90 days after the end of that period. This ensures that new data brokers undergo an early review of their DROP deletion request processing practices and identify compliance issues to promptly correct them. The 90-day interval between the end of the audit period and the report deadline is necessary to be consistent with subsections (a) and (c) and for cybersecurity audit

reports, provides auditors time to complete fieldwork on the final cycles of the period and to prepare the report, and ensures reports are completed within a reasonable time period after the close of the audit period.

Proposed subsection (c) requires data brokers to complete a DROP audit at least every three years after completing their first audit. This subsection is necessary to implement Civil Code section 1798.99.86(e), which requires triennial audits but does not specify how subsequent audit periods should be defined or when audit reports must be completed.

Proposed subsection (c)(1) specifies that each subsequent audit period must include the three years immediately following the data broker's most recent audit period. This requirement is necessary to ensure continuity between audit cycles and to guarantee each audit covers a complete three-year period of DROP deletion request processing.

Proposed subsection (c)(2) requires all DROP audit reports to be completed no later than 90 days after the last day of the audit period. The 90-day interval between the end of the audit period and the report deadline is necessary to be consistent with subsections (b) and (c) and for cybersecurity audit reports, provides auditors time to complete fieldwork on the final cycles of the period and to prepare the report, and ensures reports are completed within a reasonable time period after the close of the audit period.

Proposed subsection (c)(3) clarifies that if a business does not meet the definition of "data broker" at the time its DROP audit report would otherwise be due, it must complete a DROP audit pursuant to subsection (b) upon again meeting the definition of "data broker." This subsection is necessary to ensure that businesses that temporarily cease data broker operations are not required to complete audits during periods when they are not subject to the Delete Act, while also ensuring that they undergo an audit promptly upon resuming data broker activities. This is necessary to prevent a business from avoiding an audit by ceasing data broker activity shortly before a report is due and resuming afterward.

Adopt § 7631. Auditor Qualifications and Independence.

Proposed section 7631 establishes who may conduct a DROP audit and the independence the auditor must maintain. The statute requires an "audit by an independent third party" but does not define either term. These provisions are necessary to give the statutory terms operational content so that data brokers know whom they may engage, auditors know what is expected of them, and the Agency can rely on the resulting reports.

Proposed subsection (a) requires a data broker to engage a qualified, objective, and independent auditor who uses procedures and standards generally accepted in the auditing profession and lists examples of standards-setting bodies. It does not prescribe a specific standard to allow for flexibility so a business may choose the type of audit firm that matches their business practices, size, and complexity while ensuring every audit is

conducted with professional rigor. This list parallels the list in the Agency's cybersecurity audit regulations (§ 7122(a)), which promotes consistency and allows auditors to apply familiar methodologies. This is necessary to ensure DROP audits are conducted with rigor, consistency, and professional competence, and auditors apply recognized auditing methodologies rather than ad hoc or informal review practices.

Proposed subsection (a)(1) requires at least one auditor conducting the DROP audit to possess knowledge of data deletion practices and how to audit a business's data retention and deletion practices, including knowledge of the Delete Act and applicable provisions of the CCPA. This requirement is necessary because DROP audits involve specialized technical and legal obligations that cannot be adequately assessed by an auditor lacking familiarity with statutory deletion requirements, hashing and matching procedures, suppression list obligations, and opt-out processing.

Proposed subsection (a)(2) requires at least one auditor conducting the audit to demonstrate competence in the data systems and technical practices relevant to DROP deletion request processing. This is necessary because verifying compliance requires examining how the data broker standardizes and hashes identifiers, executes matching logic, issues deletion commands across systems including archives and backups, and maintains suppression lists. Those are technical questions that require technical competence to test. The Agency has structured the two requirements so they may be satisfied by different members of an audit team, which reduces costs by allowing firms to staff engagements with a legal or compliance specialist and a technical specialist rather than requiring every auditor to possess both skill sets.

Proposed subsection (b) requires the auditor to exercise objective and impartial judgment, remain free from influence by the data broker, and avoid activities that compromise independence. This subsection is necessary to ensure that DROP audits satisfy Civil Code section 1798.99.86, subdivision (e)'s requirement for an "independent third party" audit and to prevent conflicts of interest that could undermine the reliability of audit findings.

Proposed subsection (b)(1) identifies the specific prohibitions necessary to preserve auditor independence. These provisions are necessary to define "independent" in a way data brokers and auditors can apply, and they reflect the independence principles that professional standards and other regulators have long recognized: an auditor who is employed by the audited business, who has a financial stake in it, or who built the systems being audited faces incentives and self-review pressures that undermine objective judgment. The prohibitions parallel those in the Agency's cybersecurity audit regulations (§ 7122(a)(1)), which ensures consistency across the Agency's audit programs and allows firms that have structured their practices to satisfy those regulations to satisfy these as well.

Proposed subsection (b)(1)(A**)** prohibits the auditor from being employed by or serving as an independent contractor for the data broker for any purpose other than conducting

the DROP audit. This is necessary to prevent financial dependence or dual-role conflicts that could compromise impartiality.

Proposed subsection (b)(1)(B) prohibits the auditor from being an officer or director of the data broker. This is necessary because individuals in such positions lack independence and cannot objectively assess the business's compliance.

Proposed subsection (b)(1)(C) prohibits the auditor from having, or being affiliated with an entity that has, a financial interest in the data broker or its affiliates. This is necessary to prevent financial incentives from influencing audit findings.

Proposed subsection (b)(1)(D) prohibits the auditor from having participated in business activities the auditor will assess, including developing procedures, preparing documents, making recommendations regarding processing operations or designing, implementing, operating, or maintaining deletion processing systems. This is particularly necessary for DROP audits because many data brokers rely on outside consultants and technology vendors to build their deletion-processing pipelines. A vendor that implemented a data broker's hashing and matching logic cannot independently determine whether that logic works. This subsection ensures auditors do not evaluate their own work or rely on systems they helped create, which would undermine the independence and credibility of the audit.

Proposed subsection (c) clarifies that nothing prohibits a data broker from using the same auditor for other audits required by law or voluntarily conducted, provided the auditor meets the independence requirements of this section. This subsection is necessary to allow businesses subject to multiple audit regimes, such as Agency cybersecurity audits, to streamline compliance and reduce costs while still ensuring DROP audits are conducted by an independent third party.

Adopt § 7632. Scope and Thoroughness of the DROP Audit.

Proposed section 7632 defines what the auditor must do and what the auditor may rely on. It is necessary because the statute requires an audit "to determine compliance with" Civil Code section 1798.99.86 but does not state how that determination is to be made. Preliminary comments received by the Agency consistently attested that an audit that reviews policies and accepts management's representations does not determine compliance. The section therefore requires testing and evidence, defines the minimum components every audit must cover, and preserves the auditor's discretion to do more.

Proposed subsection (a) requires the auditor to assess compliance with the DROP deletion request processing requirements of Civil Code section 1798.99.86 and the applicable regulations during the audit period, including compliance by the data broker's contractors and service providers to the extent they process personal information on the data broker's behalf. This subsection is necessary to ensure that audits are performed with sufficient rigor, breadth, and independence to verify compliance with Civil Code section 1798.99.86 and its implementing regulations.

Proposed subsection (a)(1) requires auditors to assess compliance with all DROP deletion request processing requirements during the audit period, including compliance by contractors and service providers. This requirement is necessary because Civil Code section 1798.99.86, subdivisions (c) and (d) impose obligations on data brokers regarding the actions of their service providers, and an audit cannot accurately determine compliance without reviewing those third-party activities.

Proposed subsection (a)(2) requires auditors to review the data broker's policies and procedures related to recordkeeping, data governance, data mapping, technical controls, monitoring, and use of technical tools, including software and artificial intelligence that are noncompliant or contributed to noncompliance with the statute and regulations. The express reference to artificial intelligence is necessary because data brokers increasingly use automated and AI-assisted tools to match, classify, and delete records, and because the Agency's preliminary comment process specifically raised the question of how such tools should be audited. Rather than establishing a separate regime for AI, the regulations treat AI as one of the technical tools whose role in any noncompliance the auditor must review, which keeps the audit focused on outcomes. This subsection is necessary because deficiencies in these areas can directly contribute to noncompliance with deletion processing requirements, and the audit must identify whether such deficiencies exist.

Proposed subsection (a)(3) requires auditors to test and evaluate the data broker's deletion processing system and to review the processing steps for all consumer deletion lists from download through status reporting and suppression list use. This subsection is necessary to ensure auditors verify the accuracy of each required processing step—standardization, hashing, matching, deletion, exemption application, and suppression list maintenance—and do not rely solely on documentation or management assertions. Additionally, the reliability of a data broker's status reports depends on a chain of automated steps, and a defect anywhere in the chain causes every downstream result to be wrong; only testing can detect such defects. For example, a hashing routine that retains leading zeros in ZIP codes, or a deletion command that omits a replica database. The subsection also permits sampling, which is necessary to allow auditors to conduct thorough reviews without requiring exhaustive testing of every record. Leaving the sampling method to the auditor's professional judgment, rather than prescribing sample sizes, is a performance standard that allows the auditor to tailor the approach to the data broker's volume, system complexity, and risk.

Proposed subsection (a)(4) requires the auditors to interview individuals directly responsible for DROP deletion request processing compliance, data system development and maintenance, and data processing programs. Interviews are necessary because documents and test results often do not reveal how a process actually operates, who can change it, or how exceptions are handled. Identifying the three required interview roles ensures the audit reaches those responsible for legal compliance, system design, and day-to-day processing, while still allowing the auditor to speak with additional personnel as needed. This subsection is necessary to ensure that

auditors obtain information about actual system behavior, operational practices, and compliance workflows that may not be evident from documentation alone.

Proposed subsection (b) requires data brokers to make available to the auditor all information in their possession, custody, or control that the auditor requests as relevant to the DROP audit and provides examples. This subsection is necessary to ensure auditors have access to system architecture, data mapping, service provider information, and other materials required to determine the scope of the audit and apply appropriate criteria. An auditor can be independent and competent and still be unable to determine compliance if the audited business withholds information. The examples are necessary because the scope of a DROP audit depends on the data broker's architecture: an auditor cannot decide which systems to test without knowing which systems hold personal information. This parallels section 7122, subsection (b) of the cybersecurity audit regulations.

Proposed subsection (c) requires data brokers to make good-faith efforts to disclose all facts relevant to the audit and prohibit misrepresentation of any relevant fact.

This subsection is necessary to ensure the integrity of the audit process and to prevent data brokers from withholding information that could obscure noncompliance. This parallels section 7122, subsection (b) of the cybersecurity audit regulations.

Proposed subsection (d) prohibits audit findings from relying primarily on assertions or attestations by the data broker’s management or the mere existence of a policy or procedure. This subsection is necessary to ensure audits rely on objective evidence rather than self-reported compliance.

Proposed subsection (d)(1) requires audit findings to rely primarily on specific evidence deemed appropriate by the auditor, including documents, data maps, sampling and testing results, interviews, logs, and the DROP records. This subsection is necessary to ensure audit conclusions are supported by verifiable evidence and auditors apply consistent evidentiary standards. The evidence standard mirrors the standard in the cybersecurity audit regulations (§ 7122(d), (e)) and the sufficiency-of-evidence principles of professional auditing standards. The examples of evidence are illustrative and are necessary to guide auditors and data brokers toward the kinds of records that demonstrate compliance in this context, including the records the DROP itself generates when a data broker downloads a batch or uploads statuses. Preliminary commenters, including auditors, strongly supported an evidence-over-assertions standard.

Proposed subsection (e) establishes the minimum compliance areas every DROP audit must assess. Each subsection corresponds to each step at which a consumer's request can fail to be honored, and each is tied to the regulatory provision that imposes the obligation. Prescribing minimum components is necessary so audits are complete and comparable across data brokers, which may assist with identifying systemic problems, such as whether particular identifier types consistently produce low match rates, a question the Agency posed in its preliminary comment invitation. This is also necessary

for data brokers and auditors to be able to scope and price engagements with confidence.

Proposed subsection (e)(1) requires assessing the accuracy of consumer deletion list selection, including whether the data broker selected all required lists and updated selections timely. This is necessary because a data broker that selects too few lists never receives, and therefore never processes, requests from consumers whose identifiers appear only on the unselected lists.

Proposed subsection (e)(1)(A) requires verifying the data broker selected every consumer deletion list corresponding to identifiers in its records, as required by section 7610(a)(3). This is necessary to ensure all relevant DROP requests are retrieved.

Proposed subsection (e)(1)(B) requires verifying the data broker updated list selection accurately and timely when its data practices changed, as required by section 7610(a)(3)(C). This is necessary to ensure ongoing compliance as data collection practices evolve.

Proposed subsection (e)(2) requires assessing the timeliness of DROP access, including whether the data broker downloaded consumer deletion lists at least every 30 days, as required by Civil Code section 1798.99.86, subdivision (c)(1) and section 7612, beginning January 1, 2027. This subsection is necessary because timely access is required by statute and is essential to ensure prompt deletion.

Proposed subsection (e)(3) requires assessing the accuracy of standardization, including whether the data broker standardized identifiers as required and applied standardization consistently. This is necessary because inconsistent standardization produces hashes that do not match and, therefore, can result in incomplete deletion.

Proposed subsection (e)(3)(A) requires verifying the data broker standardized identifiers according to section 7613, subsection (a)(1). This is necessary to ensure compliance with required formatting rules to ensure consistent matching once identifiers are hashed.

Proposed subsection (e)(3)(B) requires verifying standardization was applied consistently across all systems and data. This is necessary because standardization that is not applied to all systems can miss certain identifiers leading to incomplete deletion.

Proposed subsection (e)(4) requires assessing the accuracy of hashing, including whether hashing was consistently applied across all systems and data. This is necessary because a system that hashes with a different algorithm, encoding, or output format than DROP will never match. This will lead to data brokers failing to honor DROP requests even when a match exists between the DROP request and data broker record identifiers.

Proposed subsection (e)(5) requires assessing the accuracy of consumer identifier matching. This subsection is necessary because matching determines whether deletion, exemption, or opt-out actions must be taken.

Proposed subsection (e)(5)(A) requires verifying the data broker compared hashed identifiers in each batch against its own hashed identifiers as required. This is necessary to ensure correct matching methodology.

Proposed subsection (e)(5)(B) requires verifying the data broker accurately determined when DROP-provided identifiers match their own records. This is necessary to ensure data brokers maximize accurate matches, which directly drive deletion rates, and is essential because a broker cannot process a deletion without first confirming a valid match.

Proposed subsection (e)(6) requires assessing whether the data broker completed the appropriate action for matched identifiers, including deletion, opt-out, or exemption. This subsection is necessary to ensure compliance with statutory requirements for handling matched identifiers and to ensure all DROP requests are properly honored.

Proposed subsection (e)(6)(A) requires verifying each DROP request was processed correctly. This is necessary to ensure compliance with section 7613.

Proposed subsection (e)(6)(B) requires verifying the data broker properly identified and processed personal information as defined by Civil Code section 1798.150. This is necessary to ensure all relevant data is deleted or opted out.

Proposed subsection (e)(6)(C) requires verifying exemptions were applied correctly. This ensures exemptions are not used too broadly or improperly, preventing the inappropriate retention of personal information that should be deleted. In short, the provision prevents data brokers from misusing exemptions to avoid required deletions.

Proposed subsection (e)(6)(D) requires verifying deletion and opt-out were applied completely and permanently across all systems, including systems or databases holding derived data, such as inferences. This is necessary to ensure full compliance with deletion obligations as required in section 7613.

Proposed subsection (e)(6)(E) requires verifying opt-out requirements were correctly applied to all applicable consumers. This is necessary to ensure compliance with section 7613(a)(2)(B).

Proposed subsection (e)(7) requires assessing the accuracy and timeliness of status reporting. This subsection is necessary because status reporting is essential for transparency and oversight by stakeholders, such as the Agency, auditors, consumers, and the public.

Proposed subsection (e)(7)(A) requires verifying the correct status was assigned because status codes are how consumers learn the outcome of their requests as required by Civil Code section 1798.99.86, subdivision (b)(9).

Proposed subsection (e)(7)(B) requires verifying compliance with section 7614's reporting requirements. This is necessary to ensure timely and accurate status updates.

Proposed subsection (e)(8) requires assessing suppression list maintenance and use. This subsection is necessary because suppression lists prevent re-collection or re-processing of personal information for consumers who submitted DROP requests as required under Civil Code section 1798.99.86, subdivision (d).

Proposed subsection (e)(8)(A) requires verifying the suppression list included all consumers with DROP requests, other than cancelled requests. This is necessary to ensure all consumers who have requested their personal information be deleted are maintained as deleted within the data broker's system.

Proposed subsection (e)(8)(B) requires verifying only permissible personal information was included in the business's suppression list. This is necessary to ensure compliance with section 7613, subsection (b)(1)(B) and for data minimization.

Proposed subsection (e)(8)(C) requires verifying the suppression list was updated for new DROP requests. This ensures consumers who submit future requests continue to be treated as deleted.

Proposed subsection (e)(8)(D) requires verifying newly collected personal information was compared against the suppression list. This is necessary to prevent re-collection of deleted data as required in 7613, subsection (c).

Proposed subsection (e)(8)(E) requires verifying newly collected personal information matching suppression list identifiers is handled appropriately—whether through deletion, opt-out, or a valid exemption—as required by section 7613 and Civil Code section 1798.99.86, subdivision (c) and (d). This is necessary to ensure compliance with statutory deletion and opt-out requirements for new matches as they arise, for example when a business acquires new data sets.

Proposed subsection (e)(8)(F) requires verifying status updates are accurately and promptly reported for consumers whose status changes due to a suppression list match, as required by section 7614(a)(1). This ensures transparency through timely and accurate reporting to both the Agency and the consumer.

Proposed subsection (e)(9) requires assessing the data broker's direction to service providers and contractors and its recordkeeping regarding such direction. This subsection is necessary because Civil Code section 1798.99.86(c)(1)(C) and (D) require data brokers to ensure service providers delete personal information and maintain records for six years.

Proposed subsection (f) clarifies that nothing in the section prohibits an auditor from assessing or testing other components of a data broker's DROP deletion request processing and related recordkeeping. This is necessary to make clear subsection (e) is a floor rather than a ceiling, and to preserve the auditor's professional judgment to pursue issues the minimum components do not reach.

Adopt § 7633. Audit Report.

Proposed section 7633 specifies the contents of the DROP audit report. The statute requires the data broker to submit "a report resulting from the audit and any related materials" to the Agency within five business days of a written request under Civil Code section 1798.99.86, subdivision (e)(2) but does not say what the report must contain. Specifying the contents is necessary to ensure that reports are complete, the Agency can evaluate them efficiently and consistently, and data brokers and auditors know in advance what must be produced. The section is modeled on the report requirements of the cybersecurity audit regulations (§ 7123) and adapted to DROP deletion request processing.

Proposed subsection (a) establishes that the DROP audit report must be prepared by the auditor and must contain specific components necessary to demonstrate compliance with Civil Code section 1798.99.86, subdivision (e). This subsection is necessary to ensure audit reports contain uniform, complete, and verifiable information that allows the Agency to evaluate whether a data broker has complied with all statutory and regulatory obligations related to DROP deletion request processing.

Proposed subsection (a)(1) requires the audit report to identify the data broker’s business name and any trade names. This information is necessary to ensure the audit report can be accurately associated with the correct entity in the Data Broker Registry and to avoid confusion where a business operates under multiple names.

Proposed subsection (a)(2) requires the audit report to include the titles of up to three individuals responsible for the business’s DROP deletion request processing. This requirement is necessary to identify the personnel accountable for compliance and to ensure the auditor’s findings can be contextualized within the data broker’s organizational structure. Limiting the number to three minimizes the burden on data brokers while ensuring the persons with primary responsibility are identified.

Proposed subsection (a)(3) requires the audit report to include the data broker’s ID and registration confirmation number(s). This information is necessary to link the audit report to the data broker’s DROP account and registration records, ensuring accurate tracking and enforcement.

Proposed subsection (a)(4**)** requires the audit report to state the audit period. This is necessary because Civil Code section 1798.99.86(e) requires audits to cover specific periods of DROP deletion request processing, and the Agency must be able to confirm the auditor reviewed the correct timeframe under section 7630.

Proposed subsection (a)(5) requires the audit report to include the date of completion of the last DROP audit, if applicable. This information is necessary to verify compliance with the three-year audit cycle required by statute and to ensure continuity between audit periods.

Proposed subsection (a)(6) requires the audit report to include the auditor's name, business affiliation, and relevant qualifications demonstrating compliance with section 7631. This requirement is necessary to identify who conducted the audit and ensure the auditor meets the independence and competency standards mandated by the Delete Act and the Agency's regulations.

Proposed subsection (a)(7) requires the audit report to describe the data broker's processing of DROP requests and identify the policies, procedures, and practices assessed; the criteria used; and the specific evidence examined, such as documents reviewed, sampling and testing performed, and interviews conducted. This subsection is necessary to ensure transparency in the auditor's methodology and to allow the Agency to evaluate whether the audit was sufficiently thorough and aligned with section 7632's required assessments.

Proposed subsection (a)(7)(A) requires identification of the policies, procedures, and practices assessed. This is necessary to ensure the audit reviewed all relevant components of the data broker's deletion processing workflow.

Proposed subsection (a)(7)(B) requires identification of the criteria used for the audit. This is necessary to ensure the auditor applied appropriate standards and the Agency can evaluate the rigor of the audit.

Proposed subsection (a)(7)(C) requires identification of the specific evidence examined, including documents, sampling, testing, and interviews. This is necessary to ensure the audit relied on objective evidence rather than simply assertions by the data broker.

Proposed subsection (a)(8) requires the audit report to include findings for all assessments required in section 7632 and any additional assessments conducted by the auditor. It must also explain why assessing those policies, procedures, and practices, using those criteria, and examining that evidence justifies the findings. This subsection is necessary so the Agency can evaluate the rigor of the audit rather than simply accept its conclusions, to ensure the audit report reflects the auditor's conclusions for each of the nine required compliance areas, and to explain how the evidence supports the findings.

Proposed subsection (a)(9) requires the audit report to describe in detail any noncompliance with Civil Code section 1798.99.86 and applicable regulations. This subsection is necessary to ensure the Agency receives complete information about the nature, scope, and impact of any deficiencies in DROP deletion request processing as well as the data broker's remediation, or planned remediation, of the gaps and weaknesses identified by the audit.

Proposed subsection (a)(9)(A) requires identification of the type of personal information affected. This is necessary to assess the severity and privacy impact of noncompliance.

Proposed subsection (a)(9)(B) requires identification of the duration of the noncompliance. This is necessary to determine whether the issue was isolated or systemic.

Proposed subsection (a)(9)(C) requires identification of any policies, procedures, system architecture, data maps, technical tools, controls, or records that are noncompliant or contributed to noncompliance. This is necessary to ensure the audit report provides actionable information for remediation and enforcement.

Proposed subsection (a)(9)(D) requires identification of remedial actions taken or planned and the timeframe for completion. This is necessary to ensure data brokers address deficiencies promptly. Together, this section provides key pieces of information a business needs to prioritize and remediate vulnerabilities that could hinder proper deletion, while enabling the Agency to determine how it has remediated or plans to remediate those issues.

Proposed subsection (a)(10) requires the audit report to identify and explain any necessary corrections or amendments to prior DROP audit reports. This is necessary to maintain continuity between audit cycles, provide accurate information, and ensure that previously identified issues are appropriately resolved.

Proposed subsection (a)(11) requires a statement, signed and dated by the highest-ranking auditor, certifying that the auditor completed an independent review of the data broker's DROP deletion request processing, complied with all requirements of section 7632, exercised objective and impartial judgment on all issues within the scope of the audit, and did not rely primarily on assertions or attestations by the data broker's management. This certification is necessary to ensure the integrity of the audit and to demonstrate compliance with the Delete Act's requirement for independent third-party review.

Proposed subsection (a)(12) requires a certification from a member of the data broker's executive management team directly responsible for DROP audit compliance. This subsection is necessary to ensure the data broker attests to the accuracy of the information provided to the auditor to establish reliability of the audit and to prevent improper influence over the audit process.

Proposed subsection (a)(12)(A) requires the certification to include a specific attestation under penalty of perjury that the certifying individual has authority to make the certification, that the auditor met the requirements of section 7631, that the auditor was provided true and correct information and access to all systems and information requested, and that the business made no attempt to influence the auditor's decisions or assessments. Requiring the executive certification under penalty of perjury is consistent with the certification data brokers already make when they register. (§ 7602(b).) This is

necessary to ensure accountability and to deter attempts to mislead the auditor or the Agency.

Proposed subsection (a)(12)(B) requires identification of the certifying individual's name, business title, and the date of certification. This is necessary to ensure traceability and accountability. The certifications in subsection (a)(11) and (a)(12) are necessary to establish personal accountability. The auditor attests to the independence and evidentiary basis of the work, and the executive attests that the business did not compromise it. The certifications parallel those required in cybersecurity audit reports under section 7123.

Proposed subsection (b) allows a data broker to utilize an audit prepared for another purpose, provided it meets all requirements of Article 5, either on its own or through supplementation. This subsection is necessary to reduce unnecessary duplication of audits and to allow businesses subject to multiple audit regimes to streamline compliance while still meeting all statutory and regulatory requirements. The provision parallels section 7123, subsection (f) of the cybersecurity audit regulations.

Incorporation by Reference

No documents have been incorporated by reference.

Economic and Fiscal Impact

Pursuant to Government Code section 11346.3, the Agency has assessed the potential economic and fiscal impacts of the proposed regulations.

Business Impact

As of November 1, 2026, 680 data brokers have active DROP accounts with the Agency, including an estimated 170 small businesses and 510 typical or larger businesses. The proposed regulations will impact all registered data brokers.

Estimated Costs to Businesses

The proposed regulations fall into two categories: updates to current data broker regulations and new provisions related to DROP audits. The most significant costs to businesses relate to the DROP audit. However, the requirements to engage an external, independent auditor and to undergo an audit triennially are imposed directly by Civil Code section 1798.99.86, subdivision (e), and therefore are not costs related to the proposed regulations. Additionally, the Agency anticipates any costs associated with the clarifying amendments to be subsumed within the ordinary costs of complying with existing regulations, as the amendments do not impose new substantive obligations.

This analysis evaluates only the incremental regulatory costs attributable to the Agency's implementing specifications. For DROP audits, these include auditor qualification and independence verification required by proposed section 7631,

minimum assessment components and evidentiary expectations contained in section 7632, and audit report contents and certifications found in section 7633. For data broker regulations updates, this includes the six-year retention of service provider notification records pursuant to section 7613, subdivision (e), and the 10-business-day account update requirements in section 7610, subdivision (b). The incremental regulatory costs vary by business size and system complexity, reflecting the documentation, evidence, and recordkeeping needed to support audits of statutory obligations.

For a small business data broker—typically a single primary system with limited service provider integrations—incremental one-time costs to align documentation, data maps, and audit-ready logging with proposed sections 7631 through 7633 are estimated at approximately $1,686. Incremental ongoing annualized costs for recordkeeping, service provider notification documentation, and audit period preparation are estimated at approximately $1,604 per year.

For a typical or larger data broker—multiple systems and service provider integrations—incremental one-time costs to align documentation and logs and to organize audit support materials are estimated at approximately $3,816. Incremental ongoing annualized costs for recordkeeping and audit-period preparation are estimated at approximately $3,181 per year.

Estimated Benefits of Regulation

The proposed regulations provide operational clarity and a uniform audit structure to support the statutory obligations set forth in Civil Code section 1798.99.86. By specifying auditor qualifications and independence, minimum assessment components and evidentiary expectations, and report contents and certifications, the proposed regulations promote consistent audits of statutory duties, improve the accuracy of identifier matching and deletion across systems, support data minimization through standardized suppression list maintenance, and enhance transparency through reliable status reporting. Consumers benefit from verified deletion and sustained suppression of personal information. Data brokers benefit from predictable, system-aligned expectations. The Agency benefits from comparable, evidence-based audit reports that strengthen oversight and enforcement.

Results of Economic Impact Assessment

Pursuant to Government Code section 11346.3, subdivision (b), the Agency has conducted an economic impact assessment and concluded:

Creation or Elimination of Jobs: The proposal would not result in the creation or elimination of jobs. However, demand for independent third-party auditors with privacy, data deletion, and information systems expertise, as well as compliance and engineering roles at data brokers and consultancies, may increase.

Creation of New Businesses or Elimination of Existing Businesses: The proposal would not result in an elimination of businesses. New audit, privacy assurance, and technical compliance service provider businesses may form to serve the data broker market.

Expansion of Businesses: Firms providing accounting, information systems audit, privacy assurance, and information technology services, including firms already serving businesses subject to the Agency's cybersecurity audit regulations, may expand their practices to conduct DROP audits in accordance with the proposed regulations.

Worker Safety: The proposal would not benefit worker safety as the provisions proposed regulations do not pertain to, nor impact, worker safety.

Environment: The proposed regulations do not pertain to the state's environment and are not expected to impact the environment.

Health, Safety, and Welfare: The proposal would benefit the health, safety, and welfare of California residents by supporting statutory privacy protections. The proposal would improve identifier match accuracy, clarify deletion actions and exemptions, ensure sustained suppression of personal information, and establish uniform, evidence-based audits of statutory obligations across systems and service providers.

Evidence Supporting Finding of No Significant Statewide Adverse Impact

Although the proposed regulations will directly impact registered data brokers statewide, including small businesses, the Agency concludes that the proposed action will not have a significant, statewide adverse economic impact directly affecting business, including the ability of California businesses to compete with businesses in other states.

Because the triennial independent audit mandate and the statutory cadence for accessing the DROP are imposed directly by statute, the costs of engaging an auditor and performing statutory processing are not attributable to the proposed regulations. Applying the estimated costs to the 680 active data broker businesses, estimated to consist of 170 small businesses and 510 typical or large businesses, equates to an estimated statewide initial one-time incremental costs of $2.2 million, and estimated statewide ongoing annualized incremental costs of $1.9 million per year. Over a complete three-year period, incremental costs attributable solely to these regulations total approximately $7.9 million, remaining well below the $50 million major regulation threshold in any 12-month period.

The Delete Act and these regulations apply uniformly to all businesses that meet the statutory definition of a data broker doing business in California, regardless of domicile. Accordingly, the proposed regulations do not place California-based businesses at a competitive disadvantage relative to out-of-state competitors.

Fiscal Effect on State Government

Pursuant to Civil Code section 1798.99.86, subdivision (e)(2), data brokers are required to submit their triennial audit reports and related materials to the Agency only upon the Agency's written request; therefore, there is not fiscal impact from the regulations, as this falls within the Agency's ongoing enforcement operations, which continue to be funded through the Data Brokers' Registry Fund via annual registration and access fees pursuant to Civil Code sections 1798.99.81 and 1798.99.87, subdivision (b), and require no additional General Fund appropriation. The proposed regulations are not expected to impose fiscal impacts on any other state agency.

Disclosures Regarding the Proposed Action

The Agency has made the following initial determinations:

Local mandate: None.

Cost to any local agency or school district requiring reimbursement pursuant to Government Code section 17500 et seq.: None.

Other non-discretionary costs or savings imposed upon local agencies: None.

Cost or savings to any state agency: Pursuant to Civil Code section 1798.99.86, subdivision (e)(2), data brokers are required to submit their triennial audit reports and related materials to the Agency only upon the Agency's written request; therefore, there is not fiscal impact from the regulations, as this falls within the Agency's ongoing enforcement operations, which continue to be funded through the Data Brokers' Registry Fund via annual registration and access fees pursuant to Civil Code sections 1798.99.81 and 1798.99.87, subdivision (b), and require no additional General Fund appropriation. The proposed regulations are not expected to impose fiscal impacts on any other state agency.

Cost or savings in federal funding to the state: None.

Effect upon housing: None.

Specific Technologies or Equipment

The proposed regulations do not require data brokers or auditors to use any particular brand, vendor, or proprietary technology. However, the regulations necessarily require the use of certain categories of technology to comply with statutory obligations under the Delete Act. Data brokers must be able to access the DROP, download consumer deletion lists, standardize and hash identifiers, compare hashed identifiers against their own records, maintain suppression lists, and upload status reports. These functions may be performed through manual processes or through automated systems of the data broker's choosing, and the regulations do not prescribe any specific software, hardware, or interface. The DROP allows data brokers to access and use the platform in

compliance with the statutory timeline, and the regulations clarify how data brokers must interact with the system without mandating a particular technological solution.

Proposed Article 5 introduces additional requirements for independent auditors. To conduct a DROP processing audit, an auditor must use tools capable of reviewing and testing the data broker's standardization, hashing, matching, deletion, suppression list maintenance, and status reporting processes. These requirements reflect the statutory mandate that audits evaluate actual compliance outcomes rather than merely reviewing internal policies. The regulations do not require auditors to use any specific software or auditing platform, and auditors may select the tools appropriate to their professional standards and the data broker's systems. The Agency determined that specifying particular technologies would be unnecessarily restrictive and could impede innovation or create barriers for small businesses. Instead, the regulations require auditors to use tools sufficient to test compliance with the Delete Act, consistent with recognized professional auditing standards.

Because the regulations allow both data brokers and auditors to choose the technologies that best suit their operations, and do not mandate any proprietary or uniquely burdensome equipment, the Agency concluded that the proposed regulations do not impose requirements for specific technologies or equipment within the meaning of Government Code section 11346.2, subdivision (b)(2).

Consideration of Alternatives to the Proposed Action

No reasonable alternative to the proposed regulations would more effectively in carrying out the purpose for which the action is proposed or would be as effective and less burdensome to affected businesses or private persons and equally effective in achieving the purposes of the proposed regulations in a manner that ensures full compliance with the law being implemented or made specific. The alternatives the Agency considered, and the reasons each was rejected, are set forth below:

Alternative 1: The first alternative considered by the Agency was to rely on the statute alone and adopt no audit regulations. This alternative would allow each data broker to determine for itself what an "audit by an independent third party" entails. The Agency rejected this alternative because it would produce audits of widely varying scope and rigor, many of which would consist of a review of policies and management representations rather than objective testing; the resulting reports would not be comparable and would not provide the assurance the Legislature intended. This alternative would also leave data brokers and auditors without clear regulatory standards, increasing rather than decreasing uncertainty and compliance costs.

Alternative 2: The second alternative considered by the Agency was to adopt reduced or tiered audit requirements, delay implementation, or allow remediation-only initial audits for smaller data brokers or those handling less sensitive information. During preliminary rulemaking activities, some commenters suggested reduced or tiered audits, delayed implementation, or limiting the first audit to remediation. The Agency evaluated these options but determined they are not permitted under the statute. The Delete Act

explicitly requires all registered data brokers to undergo an independent third-party audit beginning January 1, 2028, without exempting small businesses, and the Agency cannot waive this statutory mandate. Because each of the nine audit components in section 7632 corresponds to a point where a consumer's deletion request could fail, omitting any component would negatively impact the audit's ability to determine compliance in processing consumer DROP requests and undermine the statute. Instead of reducing statutory audit protections, the Agency minimized burdens on small businesses by permitting sampling, allowing data brokers to use or supplement audits prepared for other purposes, enabling a single qualified auditor to conduct related audits, and adopting flexible team-based auditor qualification standards, thereby lowering costs for small businesses with simpler systems.

Alternative 3: The third alternative considered by the Agency was to maintain the existing regulatory text in Articles 2, 3, and 4 without amendment. This alternative was rejected because the initial regulations were drafted before the DROP was fully developed and deployed, there have been recent statutory changes to the Delete Act, and the Agency now has the benefit of information about how the system and regulations work. Retaining outdated definitions, access provisions, and processing rules would perpetuate confusion among data brokers, reduce identifier match accuracy, and undermine the reliability of deletion processing and subsequent audits.

Performance Standard as Alternative

Pursuant to Government Code section 11346.2, subdivision (b)(4)(A), the Agency considered whether pure performance standards could be substituted for the prescriptive elements of the proposed regulations. Because the DROP deletion processing depends on uniform formatting and standardization of identifiers (such as five-digit ZIP codes without leading zeros), consistent cryptographic hashing, complete matching across systems, suppression-list maintenance, and standardized CSV status reporting, purely performance-based rules would result in incompatible hashes, lower match accuracy, and unfulfilled consumer deletion requests.

The Agency likewise found that pure performance standards could not replace the minimum audit assessment components in section 7632 or the report elements in section 7633. Civil Code section 1798.99.86, subdivision (e), requires audits to determine compliance with specific statutory duties. Without clearly defined assessment areas—such as deletion list selection, timeliness, standardization, hashing, matching accuracy, suppression list maintenance, and service provider direction—audits would vary widely and fail to reliably verify compliance. Prescribing the minimum components to be audited and reported ensures consistent evaluation of actual outcomes while preserving flexibility in audit methodology.

Consistent with Government Code section 11340.1, the proposed regulations incorporate performance standards wherever feasible: section 7631 permits auditors to apply any generally accepted professional auditing standard; section 7632 leaves test design and sample selection to the auditor's professional judgment; and Article 3

preserves data brokers' choice between manual and automated the DROP integration and allows the use of internal identifiers for matched records on suppression lists.

Technical, Theoretical, or Empirical Studies, Reports, or Similar Documents Relied Upon

The following documents were relied on for this rulemaking:

1. California Privacy Protection Agency, Invitation for Preliminary Comments: Delete Request and Opt-out Platform (DROP) Audits (Apr. 7, 2026), accessed at: https://www.cppa.ca.gov/regulations/pdf/drop_audits.pdf.

2. California Privacy Protection Agency, Preliminary Rulemaking Activities: Written Public Comments on DROP Audits (Apr. 7 through May 7, 2026), accessed at: Accessible Deletion Mechanism – Delete Request and Opt-out Platform ("DROP") System Requirements – California Privacy Protection Agency (CPPA).

3. California Privacy Protection Agency, Delete Request and Opt-out Platform (DROP) Audit Rulemaking Recommendations (Aug. 7, 2026 Board Meeting, Agenda Item 10 presentation), accessed at: https://cppa.ca.gov/meetings/materials/20260806_07_10_presentation.pdf.

4. California Privacy Protection Agency, Delete Request and Opt-out Platform (DROP) Update (Aug. 7, 2026 Board Meeting, Agenda Item 8), accessed at: https://cppa.ca.gov/meetings/materials/20260806_07_08.pdf.

5. California Privacy Protection Agency, DROP Technical and API Reference Documentation, Version 1.2.0 (July 2026), accessed at: https://privacy.ca.gov/drop-for-data-brokers/technical-specifications/, including "Working with the data" (list types, file schemas, status codes, standardization and hashing rules) and "Integration workflow."

6. California Privacy Protection Agency, Processing DROP Requests (guidance for data brokers), accessed at: https://privacy.ca.gov/drop-for-data-brokers/process-drop-requests/.

7. California Privacy Protection Agency, Account Creation, Fees, and Annual Registration (guidance for data brokers), accessed at: https://privacy.ca.gov/drop-for-data-brokers/account-creation-fees-and-annual-registration/.

8. California Privacy Protection Agency, Initial Statement of Reasons, Accessible Deletion Mechanism (Apr. 2025), accessed at: https://cppa.ca.gov/regulations/pdf/ccpa_updates_accessible_deletion_mechanism_isor.pdf, Final Statement of Reasons (Nov. 2025), https://cppa.ca.gov/regulations/pdf/drop_fosr.pdf.

9. California Privacy Protection Agency, Initial Statement of Reasons, CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology, and Insurance Regulations (Nov. 22, 2024), accessed at: https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_isor.pdf, and California Code of Regulations, title 11, sections 7120-7124 (Cybersecurity Audits).

10. Senate Bill 361 (Stats. 2025, ch. 466), Data brokers: data collection and deletion, and legislative analyses, accessed at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB361.

11. American Institute of Certified Public Accountants, Code of Professional Conduct, ET section 1.200 (Independence), https://pub.aicpa.org/codeofconduct/Ethics.aspx; accessed at: AU-C section 500 (Audit Evidence) and AU-C section 530 (Audit Sampling); Statements on Standards for Attestation Engagements.

12. International Organization for Standardization, ISO 19011:2018, Guidelines for auditing management systems, accessed at: https://www.iso.org/standard/70017.html.

13. ISACA, IT Audit Framework (ITAF): A Professional Practices Framework for IT Audit, 4th ed., accessed at: https://www.isaca.org/resources/itaf.

14. U.S. Securities and Exchange Commission, Rule 2-01 of Regulation S-X, Qualifications of Accountants, 17 C.F.R. § 210.2-01, accessed at: https://www.law.cornell.edu/cfr/text/17/210.2-01.

15. Published market estimates of third-party compliance audit fees relied on for the cost estimates below: Linford & Company LLP, SOC 2 audit cost estimates (Feb. 2026), as summarized, accessed at: https://sprinto.com/blog/soc-2-compliance-cost/; SOC2Auditors.io, How Much Does a SOC 2 Audit Cost in 2026, https://soc2auditors.io/resources/how-much-does-a-soc-2-audit-cost-in-2026; Workstreet, How Much Does a SOC 2 Audit Cost, https://www.workstreet.com/blog/soc-2-audit-cost.