

FINAL STATEMENT OF REASONS

UPDATE OF INITIAL STATEMENT OF REASONS

As authorized by Government Code section 11346.9, subdivision (d), the OAG hereby incorporates the Initial Statement of Reasons (ISOR) prepared in this matter. Unless specifically discussed otherwise below, the ISOR's stated bases for the necessity of the proposed regulations continue to apply to the regulations as adopted.

All modifications from the initial proposed text of the regulations are summarized below. All references to regulations are to Title 11 of the California Code of Regulations.

Changes Made to Article 1. General Provisions:

A. 11 CCR § 999.301. Definitions

Subsection (a) has been modified to clarify that the phrase "a child under 13" means a child under 13 "years of age." This change is necessary to make the language consistent with other age references throughout these regulations.

Subsection (c) has been modified to clarify that the phrase "registered with the Secretary of State" means registered with the Secretary of State "to conduct business in California." This change was made in response to comments stating that it was unclear what kind of registration was required for authorized agents, such as comments asking whether authorized agents were required to register in a separate, CCPA-specific registry managed by the Secretary of State. The change is necessary to clarify that no CCPA-specific registry exists and to clarify that to be an authorized agent, a business entity must be registered with the Secretary of State to conduct business in California. Businesses receiving consumer requests through purported authorized agents, consumers, and business entities intending to act as authorized agents benefit from this clarification regarding who may act as authorized agents.

Subsection (d) has been modified to provide further guidance and clarification for the definition of "categories of sources," which is used throughout these regulations. (See Sections 999.301, subd. (q)(3), 999.308, subd. (c)(1)(e), 999.313, subd. (c)(10)(b).) "Categories of sources" has been clarified to mean "types or groupings of persons or entities" from which a business collects consumers' personal information, not just "types of entities." The definition has also been modified to require a business to describe its categories of sources "with enough particularity to provide consumers with a meaningful understanding of the type of person or entity." The following examples have also been added to the definition: advertising networks, internet service providers, data analytics providers, operating systems and platforms, social networks, and data brokers.

These modifications are necessary to provide further guidance to businesses concerning the information they are required to provide to consumers, especially when responding to a request to know. This additional guidance benefits consumers by ensuring that businesses provide

enough information for consumers to understand the business’s personal information practices. By requiring businesses to describe categories of sources in a manner that is easily understood by consumers, these modifications implement a performance-based approach. (See Schaub, et al., *A Design Space for Effective Privacy Notices* (July 22–24, 2015) Symposium on Usable Privacy and Security (SOUPS) 2015, Ottawa, Canada (hereafter Schaub); Center for Plain Language, *Privacy-policy analysis* (2015) (hereafter Center for Plain Language).) This additional guidance also benefits businesses, particularly smaller businesses, by clarifying the categories they must identify to consumers.

Subsection (e) has been modified to provide further guidance and clarification for the definition of “categories of third parties,” which is used throughout these regulations. (See Sections 999.301, subd. (q)(5), 999.308, subd. (c)(1)(g)(2), 999.313, subd. (c)(10)(d).) “Categories of third parties” has been clarified to mean types “or groupings of third parties with whom the business shares” personal information, rather than “types of entities that do not collect personal information directly from consumers.” The definition has also been modified to require a business to describe its categories of third parties “with enough particularity to provide consumers with a meaningful understanding of the type of third party.”

These modifications are necessary because entities with whom businesses share personal information may also collect personal information directly from consumers in other contexts. The CCPA’s definition of “third party” excludes *the* business that collects personal information from consumers, meaning the business that collects a consumer’s personal information in a particular context; it does not exclude *all* businesses that collect personal information directly from consumers in any context. (Civ. Code, § 1798.140, subd. (w).) An entity may in some instances be the business that collects personal information from consumers and in other instances a third party that receives personal information collected by another business. Accordingly, the definition of “categories of third parties” has been modified to clarify this point. These modifications also provide more guidance to businesses concerning the information they are required to provide to consumers, especially when responding to a request to know. This additional guidance benefits consumers by requiring that businesses provide enough information for consumers to understand their data practices. By requiring businesses to describe categories of third parties in a manner that is easily understood by consumers, these modifications implement a performance-based approach. (See Schaub, Center for Plain Language.) It also benefits businesses, particularly smaller businesses that lack privacy resources, by clarifying the information they must provide to consumers.

Subsection (g) was added to provide a definition for the acronym “COPPA,” which refers to the Children’s Online Privacy Protection Act (15 U.S.C. § 6501 et seq.; 16 C.F.R. § 312.5 (2013)) (hereafter COPPA). This acronym is used in these regulations most prominently in sections involving verifiable parental consent for minors under 13 years of age. (See Section 999.330.) This addition is necessary to streamline references to COPPA and will benefit consumers and businesses by making the regulations easier to read.

Subsection (h) was added to provide a definition of “employment benefits.” This change was made in response to the CCPA’s amendment by AB 25 (Assem. Bill No. 25, approved by

Governor, Oct. 11, 2019 (2019-2020 Reg. Sess.)) to include Civil Code section 1798.145, subdivision (h)(1)(C), which exempts from certain provisions of the CCPA personal information that is necessary for the business to retain to administer benefits in the employment context. This addition is necessary to clarify the type of benefits and personal information subject to this exemption and to avoid any confusion that may result from different understandings of the scope of the term. This definition summarizes the concept described in Civil Code section 1798.145, subdivision (h), and ensures that such information is included in the definition of “employment-related information.” This addition is also necessary to streamline references to this exemption and will benefit consumers and businesses by making the regulations easier to read.

Subsection (i) was added to provide a definition of “employment-related information.” This change was made in response to the CCPA’s amendment by AB 25 (Assem. Bill No. 25, approved by Governor, Oct. 11, 2019 (2019-2020 Reg. Sess.)) to include Civil Code section 1798.145, subdivision (h), which exempts personal information that is collected in an employment context from certain provisions of the CCPA. This addition was necessary to streamline references to this exemption and will benefit consumers and businesses by making the regulations easier to read. The addition is also necessary to clarify that collection of such information is considered a business purpose under the CCPA.

Subsection (j) was formerly subsection (g) and has been renumbered. The initial proposed definition of “financial incentive” has been modified to replace the phrase “as compensation for the disclosure, deletion, or sale of personal information” with “related to the collection, retention, or sale of personal information.” The phrase “as compensation for” was replaced with “related to” to be consistent with the definition of “price or service difference” set forth in section 999.301, subsection (o). Civil Code section 1798.125’s prohibition on discrimination addresses both financial incentives and price or service differences, and these regulations treat them comparably. This modification is necessary because financial incentives are a type of price or service difference. Financial incentives are not solely payments to consumers as compensation for certain actions related to their data; rather, they “*includ[e]* payments to consumers.” (Civ. Code, § 1798.125, subd. (b), emphasis added.)

The term “collection,” which replaces “disclosure,” more closely aligns with the language and activities described in Civil Code section 1798.125, subdivision (b)(1), which allows a business to offer a financial incentive to consumers (under specified conditions) for “the collection of personal information[.]” The word “deletion” was replaced with “retention” to provide greater clarity and to better describe the activity for which a financial incentive is likely to be offered—*i.e.*, a consumer forgoing the right to delete. “Retention,” as used here, is the opposite of what a business would do to incentivize a consumer to forego a request for “deletion” and is the correct word in this context. This change will benefit businesses and consumers by clarifying what is considered a “financial incentive,” and thus, what business practices are governed by Civil Code section 1798.125 and the regulations regarding non-discrimination and financial incentives.

Subsection (k) was formerly subsection (h) and has been renumbered. The initial proposed definition of “household” has been modified to “a person or group of people who: (1) reside at

the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier.” This change was made in response to comments that the initial proposed definition of “a person or group of people occupying a single dwelling” was overly broad. The change is necessary to ensure that the term does not encompass persons with only a transitory relationship to a dwelling or a tenuous connection to another resident. This change will benefit businesses by providing more guidance about which groups of persons to treat as a household and will benefit consumers by ensuring that those who only temporarily occupy a dwelling are not able to access or delete a consumer’s household information.

Subsection (l) was formerly subsection (i) and has been renumbered. The initial proposed definition of “notice at collection” required notice to be provided to consumers at or before the “time” of collection of personal information. The definition has been modified to state that the notice must be provided at or before the “point at which” a business collects personal information from a consumer. This change is necessary to make the definition consistent with the language used in the CCPA. (See Civ. Code, § 1798.100, subd. (b).) This change is also necessary to encompass both temporal proximity, such as in online data captures, and physical proximity, such as near a cash register at an in-store location where collection is taking place. This change will benefit businesses by providing further guidance on how to provide notice to consumers and will benefit consumers by making the notice more apparent when personal information is collected.

Subsection (m) was formerly subsection (j) and has been renumbered.

Subsection (n) was formerly subsection (k) and has been renumbered. The subsection has been modified for stylistic and citation formatting reasons. The modifications do not change the substantive meaning or purpose of the regulation.

Subsection (o) was formerly subsection (l) and has been renumbered. The initial proposed definition of “price or service difference” has been modified to specify that the difference in price or quality of the goods or service offered to the consumer must be “related to the collection, retention, or sale of personal information.” The phrase was added for three reasons: (1) to make the definition consistent with Civil Code section 1798.125, subdivision (b)(1), which allows a business to offer a financial incentive to consumers, under specified conditions, for “the collection of personal information”; (2) to make the definition consistent with the definition of “financial incentive,” which is defined in section 999.301, subsection (j) as a program, benefit, or other offering related to the collection, retention, or sale of personal information; and (3) in response to concerns that initial proposed definition was overbroad. Price or service differences and financial incentives are addressed in the same section of the CCPA and are treated comparably under these regulations. The change is necessary to clarify that the price or service differences covered by these regulations are only those related to activities that implicate consumers’ rights under the CCPA. Businesses and consumers will benefit from the modified definition because it will clarify what business practices are governed by Civil Code section 1798.125 and the regulations regarding non-discrimination and financial incentives.

Subsection (p) was formerly subsection (m) and has been renumbered. The subsection has been modified to correct the format of the Civil Code citation.

Subsection (q) was formerly subsection (n) and has been renumbered. Subsection (q) and subsection (q)(1) have been modified to provide that the definition of a “request to know” concerns access to a consumer’s personal information that a business has “collected.” This change is necessary to make the definition consistent with language in the CCPA. (See Civ. Code, §§ 1798.100, 1798.110, 1798.115.)

Subsection (r) was formerly subsection (o) and has been renumbered.

Subsection (s) was formerly subsection (p) and has been renumbered. The subsection has been modified to correct the format of the Civil Code citation.

Subsection (t) was formerly subsection (q) and has been renumbered. The subsection has been modified to correct the format of the Civil Code citation, and to make clear that it includes a consumer less than 13 “years of age” as well as “by a minor at least 13 and less than 16” years of age. These changes are necessary to address the CCPA’s amendment by AB 1355 (Assem. Bill No. 1355, approved by Governor, Oct. 11, 2019 (2019-2020 Reg. Sess.)) to insert similar language in Civil Code section 1798.120, subdivision (c).

Subsection (u) was added to provide a definition for “signed.” “Signed” is defined to mean that “the written attestation, declaration, or permission has either been physically signed or provided electronically per the Uniform Electronic Transactions Act, Civil Code section 1633.7 *et seq.*” Adding this definition is necessary because the regulations refer to signed documents: businesses may require consumers to provide authorized agents “signed” permission before allowing them to submit requests to know, delete, and opt-out on the consumer’s behalf (see Sections 999.315, subd. (g), 999.326, subd. (a)(1)) and may require consumers to verify their identity by providing a “signed” declaration under penalty of perjury (see Section 999.325, subd. (c)). This change is necessary to clarify for businesses that “signed” includes both physical and electronic signatures. The change benefits consumers by making the verification process for consumers and authorized agents easier to execute.

Subsection (v) was formerly subsection (r) and has been renumbered. The subsection has been modified to delete the term “who” and replace it with “that.” The modification does not change the substantive meaning or purpose of the regulation.

Former subsection (s), which defined “typical consumer,” and former subsection (t), which defined “URL,” have been deleted because the regulations using those terms have been deleted. Accordingly, there is no longer a need to define those terms.

Subsection (w) was added to define “value of the consumer’s data” as the “value provided to the business by the consumer’s data as calculated under section 999.337.” This definition was added in response to the CCPA’s amendment by AB 1355 (Assem. Bill No. 1355, approved by Governor, Oct. 11, 2019 (2019-2020 Reg. Sess.)) to clarify that the relevant value for determining the permissibility of price or service differences under Civil Code section 1798.125 is the “value *provided to the business* by the consumer’s data.” The definition here summarizes

the concept described in Civil Code section 1798.125 and allows a shortened phrase to be used throughout the regulations, making them more readable, and thus, easier for consumers and businesses to understand. The reference to section 999.337 of the regulations indicates which section of the regulations businesses and consumers should review to learn more about the calculation of the value of the consumer's data.

Subsection (x) was formerly subsection (u) and has been renumbered. The subsection has been modified so that the definition of “verify” also means to determine that the consumer making a request to know or request to delete “is the parent or legal guardian of that consumer who is less than 13 years of age.” This change is necessary to make the language of the regulation consistent with COPPA’s parental verification requirements, which mandate that a parent or guardian consent to the collection of the personal information of their children under the age of 13. This will benefit businesses and consumers by providing more guidance about how to manage the personal information of minors under the age of 13 and to protect these minors’ privacy by clarifying that parents need to provide verification.

Changes Made to Article 2. Notices to Consumers:

B. 11 CCR § 999.304. Overview of Required Notices

Section 999.304 was added to provide clarity and guidance regarding the notices that businesses must provide to consumers. It was drafted in response to several public comments expressing confusion about the number and type of notices that businesses are required to provide.

Subsection (a) requires that every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and these regulations, including section 999.308. **Subsection (b)** requires that a business that collects personal information from a consumer shall provide a notice at collection in accordance with the CCPA and these regulations, including section 999.305. **Subsection (c)** requires that a business that sells personal information shall provide a notice of right to opt-out in accordance with the CCPA and these regulations, including section 999.306. **Subsection (d)** requires that a business that offers financial incentives or price or service difference shall provide a notice of financial incentive in accordance with the CCPA and these regulations, including section 999.307. These subsections provide a roadmap of the different notices to consumers required by the CCPA and clarify whether a business is required to provide these notices. This section is necessary to ensure that businesses understand and abide by the notice obligations of the CCPA.

C. 11 CCR § 999.305. Notice at Collection of Personal Information

Subsection (a)(1) has been modified to state that businesses must provide consumers with “timely notice” at or before the “point” of collection about the categories of personal information to be collected and the purposes for which that information will be used. The modification is necessary to indicate the importance of providing timely notice to consumers and to encompass both temporal and physical proximity to the collection of personal information, for example through signage at or near a cash register for businesses that collect personal information at the time of in-store purchases. The modification also makes the language in the regulation

consistent with the language in Civil Code section 1798.100, subdivision (b). This change will benefit businesses by providing further guidance on how to provide notice to consumers and will benefit consumers by ensuring that notices are conspicuous so that consumers can be better informed of their rights under the CCPA prior to collection of their personal information. Additional minor changes in language and syntax were made in this subsection for clarity.

Subsection (a)(2) has been modified in two ways. First, the phrase “to the consumer” was deleted because it was not necessary. Second, the phrase “understandable to an average consumer” was changed to “understandable to consumers.” This change was made because several public comments expressed confusion about the meaning of the term “average consumer.” Because subsections (a)(2)(a) through (a)(2)(d) provide sufficient guidance on how to make the notice at collection easy to read and understandable to consumers, the word “average” has been deleted.

Subsection (a)(2)(c) has been modified to add “in California” after “consumers.” This change is necessary to clarify that businesses must provide the notice at collection in the languages in which they provide contracts and other information to consumers *in California*. Businesses expressed confusion on this issue because Civil Code § 1798.140 only defines “consumer” to mean a natural person who is a California resident, but businesses may operate in different languages in different states or countries and California residents may interact with them while traveling or overseas. This change benefits businesses by providing guidance regarding how to determine in what languages notices must be made available.

Subsection (a)(2)(d) has been modified in two ways. First, it adjusted the requirement that the notice be “accessible” to “reasonably accessible” to consumers with disabilities. This adjustment is necessary to address public concerns that “accessible” is an overly broad term that goes beyond what may be reasonable in some circumstances, particularly for smaller businesses.

The subsection was also modified to add that for online notices, businesses must follow generally recognized industry standards, such as the Web Content Accessibility Guidelines (World Wide Web Consortium, *Web Content Accessibility Guidelines (WCAG) 2.1* (June 5, 2018) <<https://www.w3.org/TR/WCAG21/>> [as of May 21, 2020]) (hereafter WCAG). This standard for making web content accessible by desktops, laptops, tablets, and mobile devices was developed through the cooperation of individuals and organizations around the world, with a goal of providing a shared standard for Web content accessibility that meets the needs of individuals, organizations, and governments internationally. Since the issuance of the first version in 1999, the WCAG has become the dominant standard for web accessibility in the United States. This change is necessary to address several public comments asking for additional more specific guidance regarding what would be considered accessible to consumers with disabilities.

Former subsection (a)(2)(e) has been renumbered and is now **subsection (a)(3)**. This subsection, which sets forth the requirements for making the notice at collection available to consumers, has been modified to provide further guidance and examples of how to provide notice in various circumstances, as requested by several public comments. The subsection now states that the

notice at collection “shall be made readily available where consumers will encounter it at or before the point of collection of any personal information.” The change is necessary to encompass a variety of contexts in which the notice at collection may be provided. It includes temporal proximity, such as notices delivered online regarding online collection or orally when information is collected by telephone, and physical proximity, such as notices delivered by signage in retail environments. The phrase “shall be made readily available” is used to avoid confusion with the accessibility requirements set forth in subsection (a)(2)(d) regarding consumers with disabilities. The use of the word “encounter” is intended to include both sighted and visually-impaired consumers. The phrase “at or before the point of collection” makes the language in the regulation consistent with the language in Civil Code section 1798.100, subdivision (b).

Subsections (a)(3)(a) through (a)(3)(d) provide examples that illustrate some of the ways in which businesses can make the notice readily available to consumers in a variety of contexts. **Subsection (a)(3)(a)** provides an example of how a business that collects personal information online can post the notice at collection through a conspicuous link on the introductory page of its website and on all webpages where personal information is collected. **Subsection (a)(3)(b)** provides an example of how a business that collects personal information through a mobile application can provide the notice through a link on the mobile application download page and within the application, such as through the application’s settings menu. **Subsection (a)(3)(c)** provides an example of how a business that collects personal information offline can provide the notice on printed forms that collect personal information, through a paper version of the notice, or through prominent signage directing consumers to where the notice can be found online. The language “directing consumers to where the notice can be found online” responds to comments noting that the prior language was overly prescriptive and that the OAG should allow for a QR code or other ways to direct the consumer to the text of the notice. Finally, **subsection (a)(3)(d)** states that where a business collects personal information over the telephone or in person, the notice can be provided orally. This particular example was added in response to comments requesting guidance on how to provide the notice when personal information is collected over the phone.

Subsection (a)(4) was added to address instances in which a business collects personal information from a consumer’s mobile device for purposes that the consumer would not reasonably expect. In those instances, the business must provide a just-in-time notice summarizing those categories of information that a consumer would not reasonably expect to be collected and a link to the full notice at collection. The subsection also includes an example that illustrates this requirement and provides guidance as to what may be considered a purpose that a consumer would not reasonably expect. This subsection is necessary to provide transparency into business practices that defy consumers’ reasonable expectations, particularly when those uses are not reasonably related to an application’s basic functionality. The requirement benefits consumers by making notices more conspicuous in instances in which their personal information is being collected for purposes not reasonably expected. Subsection (a)(4) is consistent with the language, intent, and purpose of the CCPA to meaningfully give notice to consumers about what information is collected from and about them and to give them control over how businesses use

this information. The CCPA provides the OAG with the authority to adopt regulations as necessary to further the purposes of the CCPA. (Civ. Code, § 1798.185, subd. (b)(2).) Inherent in this authority is the ability to adopt regulations that fill in details not specifically addressed by the CCPA, but fall within the scope of the CCPA. This just-in-time notice allows consumers to make an informed decision about how to interact with the business at or before the point of collection of their information, in furtherance of Civil Code § 1798.100, subdivision (b). The regulation also benefits businesses by providing clear guidance regarding when they must provide a just-in-time notice on a consumer's mobile device.

Former subsection (a)(3) has been renumbered and is now **subsection (a)(5)**. **Subsection (a)(5)** concerns restrictions on a business's use of a consumer's personal information for purposes other than those disclosed in the notice at collection. These restrictions are necessary because the consumer could have reasonably relied on the notice when interacting with the business and allowing it to collect their personal information. The subsection has been modified by changing "other than" to "materially different than." This change was made in response to numerous comments urging that the restrictions be limited to uses that are "materially different" from those disclosed in the notice and is necessary to make the language of the regulation consistent with privacy best practices. For example, the FTC has long expected that companies should obtain affirmative express consent before using consumer data in a materially different manner than claimed when the data was collected. (See Fed. Trade Com., *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, (2012), p. viii, 57-58.) This change benefits businesses because businesses will not be required to inform consumers of immaterial changes. The change also benefits consumers by not overwhelming them with notices for every minor change, which may result in notice fatigue. The subsection also adds the term "previously collected." This change is necessary to clarify that the subsection applies when a business seeks to use previously collected personal information for a use that is materially different than what was previously disclosed to the consumer, not for new personal information that it seeks to collect.

In light of the comments received from the public, the OAG further supplements its statement of reasons in support of subsection (a)(5) as follows. (See ISOR, pp. 8-9.) Subsection (a)(5) is consistent with the language, intent, and purpose of the CCPA to provide consumers with greater control over their information and meaningful ability to exercise their CCPA rights. The CCPA provides the OAG with the authority to adopt regulations as necessary to further the purposes of the CCPA. (Civ. Code, § 1798.185, subd. (b)(2).) Inherent in this authority is the ability to adopt regulations that fill in details not specifically addressed by the CCPA, but fall within the scope of the CCPA. Specifically, Civil Code § 1798.100, subdivision (b), mandates that a business provide consumers with information before or at the point of collection and explicitly prohibits a business from collecting additional categories of personal information or using personal information collected for additional purposes without providing the consumer with notice. Subsection (a)(5) is necessary to implement Civil Code section 1798.100, subdivision (b), and to implement the purposes of the CCPA to provide consumers with greater control over their information. Just as a business must provide a notice at or before the point of collection so that the consumer may affirmatively decide whether to proceed with the interaction, subsection

(a)(5) is necessary so that the consumer may affirmatively decide whether to agree to the new use. When businesses change practices midstream, the consumer should have the opportunity to decide whether to agree to the new purpose. For example, a consumer may be comfortable allowing a business to collect their personal information to use in serving them advertisements for relevant products, but not if the business wants to use the information to conduct psychological experiments. Allowing consumers the opportunity to consent to this further use is consistent with the CCPA’s goal of fairness, choice, and control.

Some comments have interpreted Civil Code section 1798.100, subdivision (b), as only requiring an additional notice and prohibiting a consumer-consent requirement. The OAG disagrees with this interpretation. As already stated, the CCPA gives the OAG authority to promulgate regulations that further the purposes of the CCPA. Furthermore, requiring explicit consent puts the consumer in the same position they would have been had the material change been disclosed during the consumer’s first engagement with the business. It empowers the consumer to actively choose whether they want to maintain their relationship with the business. It is necessary to preserve the consumer’s ability to object to the use of their personal information for new purposes, particularly because the business already has their personal information. Without this requirement, businesses could be incentivized to minimize or delay any updated notice or to otherwise hinder a consumer’s ability to object to the new use. Thus, comments that propose simply updating an online privacy policy or providing notice without explicit consent for material changes to a business’s use of personal information would not serve the purpose of section 1798.100, subdivision (b). Such an approach would allow businesses to engage in passive notice updates without allowing consumers any agency to control how their personal information is used. Furthermore, simply putting up a new notice on a website after a consumer has already provided personal information, when that consumer may be unlikely to revisit the website (and even more unlikely to revisit the notice), is not meaningful consumer notice.

Former Subsection (a)(4) has been renumbered and is now **subsection (a)(6)**.

Former Subsection (a)(5) has been renumbered and is now **subsection (a)(7)**. Subsection (a)(7) has been modified to insert “point of.” This change is necessary to make the language used in this subsection consistent with the language in Civil Code section 1798.100, subdivision (b) and section 999.305, subsections (a)(1) and (a)(3).

Subsection (b)(2) has been modified to require that the notice at collection include “the business or commercial purpose(s) for which the categories of personal information will be used,” as opposed to the business or commercial purpose for which each category of personal information will be used. This change is necessary to make the language used in this regulation consistent with the language in Civil Code section 1798.100, subdivision (b).

Subsection (b)(3) has been modified to state that an offline notice at collection include “where the [“Do Not Sell My Personal Information”] webpage can be found online,” for the same reasons set forth in subsection (a)(3)(c) above. The modification is necessary to align this provision with subsection (a)(3)(c) and subsection (b)(4). The subsection has also been modified for citation formatting reasons (added “subsection”). Including the “Do Not Sell My Personal

Information” link in the notice at collection benefits consumers because it directs them to where they can exercise their right to opt-out of the sale of their personal information. Because the CCPA does not prohibit businesses from collecting personal information (provided that they give the appropriate notice), the primary way for consumers to control their information while maintaining their relationship with the business is to exercise their right to opt-out. Including this link in the notice gives them quick and easy access to this right, thereby furthering the purposes of the CCPA. Note, however, that the inclusion of this link in the notice at collection does not relieve a business from the explicit and separate statutorily mandated requirement to include this link on its homepage. (Civ. Code, § 1798.135, subd. (a)(1).)

Subsection (b)(4) has been modified to state that an offline notice at collection include “where the business’s privacy policy can be found online,” for the same reasons set forth in subsection (a)(3)(c) above. The modification is necessary to align this provision with subsection (a)(3)(c) and subsection (b)(3). Including a link to the business’s privacy policy in the notice at collection benefits consumers because it provides them quick and easy access to a fuller picture of the business’s privacy practices.

Former subsection (d) has been modified and split up into two subsections, subsections (d) and (e). **Subsection (d)** states that a business that does not collect personal information directly from a consumer does not need to provide a notice at collection to the consumer if the business does not sell the consumer’s personal information. This regulation is necessary to clarify how Civil Code sections 1798.100, subdivision (b), and 1798.115, subdivision (d), apply to businesses that do not collect personal information directly from the consumer. Such businesses are not required to provide a notice at collection because they cannot feasibly provide a notice “at or before the point of collection,” as required by Civil Code section 1798.100, subdivision (b); however, they cannot sell any personal information that they receive because Civil Code section 1798.115, subdivision (d), prohibits third-party businesses from selling consumers’ personal information unless the consumers were given explicit notice and an opportunity to opt-out of the sale of their information. The OAG considered and rejected alternative ways to provide the notice at collection, such as through the posting of an online privacy policy, because they would not provide consumers with meaningful notice at or before the point of collection. To the extent a business does not collect personal information directly from the consumer but intends to sell the personal information, the business can comply with subsection (e).

Subsection (e) has been added to provide that a data broker registered with the Attorney General pursuant to Civil Code section 1798.99.80 et seq. does not need to provide a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out. The data broker registry, established by Civil Code section 1798.99.80 et seq., went into effect after the filing of the Notice of Proposed Regulatory Action on October 11, 2019. It requires data brokers, defined as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship (Civ. Code, § 1798.99.80, subd. (a)), to register with the Attorney General, and requires the Attorney General to create a publicly available registry of data brokers on its website (Civ. Code, § 1798.99.84).

Subsection (e) was added in response to public comments to former subsections (d)(1) and (d)(2) that raised various operational and practical concerns for both businesses and consumers, including the inundation of unwanted communications to consumers from unknown businesses and the burden and logistical barriers to obtaining attestations from multiple levels of sources. The OAG considered alternatives raised by comments and determined that using the data broker registry to provide information about how to opt-out of the sale of personal information was a better means to accomplish the purpose and intent of the CCPA with less burden to businesses and consumers. During preliminary rulemaking activities, the OAG learned that a consumer may not know who has and could be selling their personal information, given that the CCPA does not require businesses to disclose the specific persons or entities with whom they shared the consumer's personal information. (Civ. Code, § 1798.110 [merely requires the disclosure of "categories of third parties" with whom a business shared personal information].) The data broker registry addresses this gap by publicly identifying specific businesses that may be selling the consumer's personal information. Subsection (e) thus benefits consumers by allowing them to access, in one place, the information they need to exercise the right to opt-out of the sale of personal information from data brokers selling their personal information. It benefits businesses by reinforcing and streamlining their compliance with the data broker registry law and the CCPA. Subsection (e) also encourages the development of consumer tools or services by allowing innovators to pull information about how data brokers process requests to opt-out from a centralized repository.

Subsection (f) has been added in response to the CCPA's amendment by AB 25 (Assem. Bill No. 25, approved by Governor, Oct. 11, 2019 (2019-2020 Reg. Sess.)) that employment-related information is exempt from certain provisions of the CCPA until January 1, 2021. (Civ. Code § 1798.145, subd. (h).) When collecting employment-related information, businesses must still comply with Civil Code section 1798.100, subdivision (b), but they are not required to comply with Civil Code sections 1798.115 and 1798.120. Accordingly, this subsection is necessary to make the regulations consistent with the amended law. A business collecting employment-related information shall comply with the provisions of section 999.305 except that the notice at collection of employment-related information does not need to include the "Do Not Sell My Personal Information" link or a link to the business's privacy policy.

Subsection (g) has been added to state that subsection (f) shall become inoperative on January 1, 2021, unless the CCPA is amended otherwise. This change is necessary to make the regulations consistent with AB 25's (Assem. Bill No. 25, approved by Governor, Oct. 11, 2019 (2019-2020 Reg. Sess.)) amendment to the CCPA that sunsets the exemption for employment-related information. (See Civ. Code, § 1798.145, subd. (h)(4).)

The Reference section citing statutory authority has been amended to add Civil Code section 1798.99.82. This change is necessary because section 999.305 has been modified to include a reference to Civil Code section 1798.99.82.

D. 11 CCR § 999.306. Notice of Right to Opt-Out of Sale of Personal Information

Subsection (a)(1) has been modified to delete three parts of the text. First, the phrase “of sale of personal information,” was deleted because it was unnecessary in light of the defined term “notice of right to opt-out.” (See Section 999.301, subd. (m).) Second, the phrase “(or may in the future sell)” was deleted in response to public comments that it was too speculative for businesses to make assertions about what they would do with consumer personal information in the future. Although the OAG does not agree with such an interpretation of the initial proposed language or that assessment, the phrase has been removed to clarify that the notice should refer to a business’s current practices regarding the sale of personal information. Third, the phrase “and to refrain from doing so in the future” was deleted as unnecessary because subsection (a)(1) already provides that the purpose of the notice of right to opt-out is to inform consumers of the right to prospectively prohibit a business from selling their personal information.

Subsection (a)(2) has been modified in the same way and for the same reasons that Section 999.305, subsection (a)(2), has been modified. The phrase “to the consumer” was deleted because it was not necessary, and the phrase “average” was deleted because subsections (a)(2)(a) through (a)(2)(d) provide sufficient guidance on how to make the notice easy to read and understandable to consumers.

Subsection (a)(2)(c) has been modified in the same way and for the same reasons that section 999.305, subsection (a)(2)(c), has been modified. The words “in California” have been added in response to public comments to clarify that businesses are to provide the notice in the languages in which the business provides contracts and other information to consumers *in California*. The change benefits business by providing guidance regarding how to determine in what languages notices must be available.

Subsection (a)(2)(d) has been modified in the same way and for the same reasons that section 999.305, subsection (a)(2)(d), has been modified. The word “reasonably” has been added in response to public comments that the term “accessible” was overly broad, and an example of an online standard for accessibility has also been added to provide further guidance to businesses regarding what would be reasonably accessible to consumers with disabilities.

Subsection (b) has been modified stylistically to refer to consumers in the plural rather than singular form and to replace the word “a” with “the.”

Subsection (b)(1) has been modified to add that a business that collects personal information through a mobile application may provide a link to the notice within the application, such as through the application’s settings menu. This language was added in response to public comments seeking guidance on whether businesses could include this link through their mobile application’s settings menu. This modification is necessary to clarify that a business has discretion to provide a link directing consumers to the notice in lieu of including the actual language of the notice in the application’s settings menu. It benefits businesses by clarifying requirements for businesses and giving them the flexibility to shorten the language included in the actual application. This modification is not intended to speak to whether a business can

provide the notice through its mobile application's settings menu *in lieu* of providing it on the application's download page. In the context of an online service, such as a mobile application, the CCPA defines "homepage" as "the application's platform page or download page, a link within the application, such as from the application configuration, 'About,' 'Information,' or settings page, *and* any other location that allows consumers to review the notice . . . including, but not limited to, before downloading the application." (Civ. Code, § 1798.140, subd. (1) (emphasis added).) This requires that the business provide the required information on both the download page *and* within the application itself, such as through the application's setting page.

Subsection (b)(2) has been modified to clarify that a business that substantially interacts with consumers offline may satisfy the requirement that it use an offline method to provide notice to consumers by posting signage directing consumers to "where the notice can be found online." This modification was made for the same reasons the change was made in section 999.305, subsection (a)(3)(c), above. The modification is necessary to align this provision with section 999.305, subsections (a)(3)(c), (b)(3), and (b)(4).

Subsection (b)(3) has been modified to replace the word "a" with "the" to clarify that the regulation is referring to the business that does not operate a website.

Subsection (c)(2) has been modified to replace the term "webform" with "interactive form." This change is necessary because the term "webform" was too restrictive and did not account for non-web-based methods like mobile applications or local network forms, which could also serve as a means for consumers to opt-out of sale. This broader term benefits consumers and businesses by allowing for more options in setting up opt-out methods. The subsection has also been modified to correct the citation to section 999.315, subsection (a), and to add the conjunction "and" at the end because it had become the penultimate subsection in a series as a result of other modifications.

Subsection (c)(4), which required a notice to opt-out to include proof requirements for authorized agents, and **subsection (c)(5)**, which required a notice to opt-out to include a link to a business's privacy policy, have been deleted. These changes were made in response to some comments' concerns that the regulations required too much information and thus caused the notice to be too lengthy and repetitive.

Subsection (d) has been amended to delete references to whether a business would sell consumer personal information in the future. Comments asserted that it was too speculative for businesses to make assertions about what they would do with consumer personal information in the future. Although the OAG does not agree with such an interpretation of the initial proposed language or that assessment, **subsections (d), (d)(1), and (d)(2)** have been modified to state that a business need not provide a notice to opt-out if they do not sell personal information and state so in their privacy policy. This benefits businesses by providing clear guidance about what information they must provide in their privacy policy to comply with the CCPA. The regulations also benefits consumers because it requires businesses to inform them in a straightforward manner about whether they are selling their personal information.

Subsections (d)(1) and (d)(2) have also been modified to delete references to when the personal information was collected because they are no longer necessary in light of the addition of new **subsection (e)**.

Subsection (e) was added to state that a business cannot sell personal information it collected during any time it did not have a notice of right to opt-out posted unless it obtains the consumer's affirmative authorization for the sale. Because Civil Code section 1798.120, subdivision (b), requires a business that sells consumers' personal information to third parties to provide consumers with notice of their right to opt-out of the sale of their personal information, the converse is also true: if the consumer has not been provided with notice of their right to opt-out when the business collected their personal information, the business cannot sell that consumer's personal information. Subsection (e) is necessary to prevent a business from unilaterally and retroactively changing its policy to sell personal information that it collected during a time period when it expressly assured consumers that it did not sell such information. If a business decides to change their practice midstream, the business must obtain affirmative consent.

The OAG considered alternative ways to address this situation and determined that requiring businesses to obtain affirmative authorization is the most effective way to carry out the purpose and intent of the CCPA to give consumers notice and control, at the point of collection, over the sale of their personal information. While the alternative of allowing a subsequently posted notice of right to opt-out to apply retroactively would be less burdensome to businesses, it would not be as effective in informing the consumer of their right at the point of collection, when the consumer may be most aware of what personal information the business is collecting from them. Such an approach would allow businesses to engage in passive notice updates without allowing consumers any agency to control how their personal information is used, including when it was collected under false pretenses. Furthermore, simply putting up a new notice on a website after a consumer has already provided personal information, when that consumer may be unlikely to revisit the website (and even more unlikely to revisit the notice), is not meaningful consumer notice.

Former subsection (f), regarding the proposed opt-out button, has been deleted in response to the various comments received during the public comment period. The OAG has removed this subsection in order to further develop and evaluate a uniform opt-out logo or button for use by all businesses to promote consumer awareness of how to easily opt-out of the sale of personal information.

E. 11 CCR § 999.307. Notice of Financial Incentive

Subsection (a)(1) has been amended to simplify this subsection, to conform with modifications to the definitions of "financial incentive" and "price or service difference," and to clarify when a notice of financial incentive is required.

The first sentence of this subsection has been modified to state that the purpose of the notice of financial incentive is to explain "the materials terms" of a financial incentive, price difference, or service difference that a business "is offering." The phrase "may offer in exchange for the retention or sale of a consumer's personal information" has been deleted. The modifications are

necessary to make the language consistent with the language used in the CCPA, which requires a notice that “clearly describes the material terms of the financial incentive program.” (Civ. Code, § 1798.125, subd. (b)(3).) They also clarify that a business need only provide a notice of financial incentive if it currently offers a financial incentive or price or service difference, not if it *may* make such an offering at some point in the future.

Subsection (a)(1) has also been modified to add the sentence, “A business that does not offer a financial incentive or price or service difference related to the collection, retention, disclosure, deletion, or sale of personal information is not required to provide a notice of financial incentive.” This sentence responds to public comments by businesses that appear to misunderstand the regulation to require a notice of financial incentive for any price or service difference, even when the difference is not related to the collection, retention, or sale of personal information. The definitions of the terms “financial incentive” and “price or service difference” state that the offering or difference in price or service be related to the collection, retention, or sale of personal information, in furtherance of and as consistent with the CCPA’s framework in Civil Code section 1798.125. (See Section 999.301, subs. (j) and (o).) Therefore, if an incentive or difference is not related to the collection, retention, or sale of personal information, it is not a “financial incentive” or “price or service difference” as those terms are used in these regulations. For example, a business may offer a 10 percent discount to all customers in connection with the opening of new store location, but if this is unrelated to the collection, retention, or sale of personal information, this discount is not considered a “financial incentive” or a “price or service difference” for purposes of the CCPA and these regulations. This subsection has been modified to reiterate this point so that businesses do not provide (and consumers do not receive) unnecessary notices.

Subsection (a)(2) has been modified in the same way and for the same reasons that section 999.305, subsection (a)(2), has been modified. The phrase “to the consumer” was deleted because it was not necessary, and the phrase “average” was deleted because subsections (a)(2)(a) through (a)(2)(d) provide sufficient guidance on how to make the notice easy to read and understandable to consumers.

Subsection (a)(2)(c) has been modified in the same way and for the same reasons that section 999.305, subsection (a)(2)(c), has been modified. The words “in California” have been added in response to public comments to clarify that businesses are to provide the notice in the languages in which the business provides contracts and other information to consumers *in California*. The change benefits business by providing guidance regarding how to determine to in what languages notices must be available.

Subsection (a)(2)(d) has been modified in the same way and for the same reasons that section 999.305, subsection (a)(2)(d), has been modified. The word “reasonably” has been added in response to public comments that the term “accessible” was overly broad, and an example of an online standard for accessibility has also been added to provide further guidance to businesses regarding what would be reasonably accessible to consumers with disabilities.

Subsection (a)(2)(e) has been modified to require the notice of financial incentive to be “readily available where consumers will encounter it” before opting in. These modifications are necessary to make the language in this subsection consistent with the similar provision for the notice at collection. (See Section 999.305, subd. (a)(3).) The changes are also necessary to encompass a variety of contexts in which the notice of financial incentive may be provided. It includes temporal proximity, such as notices delivered online, and physical proximity, such as notices delivered by signage in retail environments. The word “encounter” is intended to include both sighted and visually-impaired consumers.

Subsection (a)(3) has been modified to correct a typographical error in its first line, replacing the word “of” with “or.”

Subsection (b)(2) has been modified to correct a typographical error in its first line, replacing the word “of” with “or.” The subsection has also been modified to add the words “and the value of the consumer’s data” to clarify that “the value of the consumer’s data” is a material term of any financial incentive or price or service difference. This change is necessary because some public comments appear to mistakenly believe that businesses may operate financial incentive programs without performing a valuation of consumer data. This is incorrect because the CCPA requires any business offering a financial incentive program to provide a notice that “clearly describes the material terms” of the program. (See Civ. Code, § 1798.125, subd. (b)(3).) The value of the consumer’s data is always a material term of such a financial incentive program, given the statutory design of the CCPA: businesses cannot offer any price or service difference, including financial incentives, unless that difference or incentive is reasonably related to the value of the consumer’s data. The addition of the words “and the value of the consumer’s data” benefits consumers and businesses by providing clarity and certainty that such value is always among the “material terms” of any financial incentive or price or service difference, as those terms are defined in these regulations.

Subsection (b)(4) has been modified to replace “Notification” with the phrase “A statement.” This change is necessary in order to clarify that this subsection only requires a statement of the consumer’s right to withdraw from the financial incentive, rather than a separate and additional notification. This change will benefit businesses by providing additional clarity and reducing the perceived burden of an additional notification.

Subsection (b)(5) has been modified to require an explanation of “how” the financial incentive or price or service difference is “reasonably related to the value of the consumer’s data,” rather than “permitted under the CCPA.” This modification is necessary to address public comments that raised concerns that the initial proposed language could implicate the disclosure of privileged information. The modification clarifies that the regulation requires a factual disclosure of how the financial incentive or price or service difference is reasonably related to the value of the consumer’s data, which is required by Civil Code section 1798.125, subdivision (a)(2), and not any legal opinion of why it complies with the CCPA. The subsection benefits businesses and consumers by clarifying what is required in the notice of financial incentive so that consumers can provide informed consent when participating in the financial incentive or price or service difference.

F. 11 CCR § 999.308. Privacy Policy

Subsection (a)(1) has been modified to delete the last sentence, which stated that the privacy policy shall not contain specific pieces of personal information about individual consumers and need not be personalized for each consumer. As explained in the ISOR, the sentence had been included because there was a concern that Civil Code section 1798.110, subdivision (c), could be interpreted to mean that a business had to include specific pieces of consumers' personal information in a business's privacy policy, rather than in response to a consumer's request. This sentence is no longer necessary because AB 1355 (Assem. Bill No. 1355, approved by Governor, Oct. 11, 2019 (2019-2020 Reg. Sess.)) amended the CCPA so that Civil Code section 1798.110, subdivision (c), now requires the privacy policy to state that a consumer has the right to request the specific pieces of personal information the business has collected about that consumer. This statutory language resolves any former ambiguity and so this regulation does not need to address it. Subsection (a)(1) has also been modified for stylistic reasons to refer to "consumers" rather than "the consumer."

Subsection (a)(2) has been modified to replace "understandable to an average consumer" with "understandable to consumers." This change was made because several public comments expressed confusion about the meaning of the term "average consumer." Because subsections (a)(2)(a) through (a)(2)(d) provide sufficient guidance on how to make the notice at collection easy to read and understandable to consumers, the word "average" has been deleted. Subsection (a)(2) has also been modified to delete the word "notice" and replace it with "policy."

Subsection (a)(2)(c) has been modified in the same way and for the same reasons that section 999.305, subsection (a)(2)(c), has been modified. The words "in California" have been added in response to public comments to clarify that businesses are to provide the privacy policy in the languages in which the business provides contracts and other information to consumers *in California*. The change benefits business by providing guidance regarding how to determine in what languages the privacy policy must be made available. The change will also help consumers by making the privacy policy more accessible.

Subsection (a)(2)(d) has been modified in the same way and for the same reasons that section 999.305, subsection (a)(2)(d), has been modified. The word "reasonably" has been added in response to public comments that the term "accessible" was overly broad, and an example of an online standard for accessibility has also been added to provide further guidance to businesses regarding what would be reasonably accessible to consumers with disabilities.

Subsection (a)(2)(e) has been modified to delete the requirements of "an additional" format and a "separate" document. These changes were made in response to comments that pointed out that if the privacy policy is already in a format that allows a consumer to print it, then there is no need to require "an additional" format or that it print as a "separate" document. The modifications lessen the burden to businesses while still providing consumers the benefit of the option to print the document. A printable version of the privacy policy is particularly useful when consumers are accessing the privacy policy from a small screen or when its length spans

multiple webpages. Printing the policy yields the option of easily reviewing the entire policy in a tangible form.

Former subsection (a)(3) has been renumbered and is now **subsection (b)**. The subsection has also been modified to add that a mobile application may include a link to the privacy policy in the application's settings menu. This language was added in response to public comments seeking guidance on whether mobile applications could include this link in their settings menu. This addition is necessary to clarify that a business has discretion to include a link in their setting menu pursuant to Civil Code § 1798.140(1), which defines "homepage" to include "a link within the application, such as from the application configuration, 'About,' 'Information,' or settings page, and any other location that allows consumers to review the notice including, but not limited to, before downloading the application." The modification benefits businesses by clarifying that they have additional locations in which to provide the privacy policy and benefits consumers by allowing the privacy policy to be accessible from the same location as other settings in a mobile application.

Former subsection (b) has been renumbered and is now **subsection (c)**. Subsection (c) sets forth the information that must be included in the privacy policy. The regulation has been modified in response to public comments received and to make the language used in the regulation consistent with language used in Civil Code sections 1798.110, 1798.115, and 1798.130.

Renumbered subsections (c)(1)(c) and (c)(2)(c) have been modified to require that the verification process be described "in general." This change was made in response to public comments requesting guidance regarding the level of detail businesses would be required to provide and raising concerns that specific descriptions would allow bad actors to evade security procedures or be onerous on businesses. Requiring a "general" description benefits consumers by providing them a high-level understanding of the verification process while reducing the burden on businesses and minimizing the risk of fraud or malicious activity.

Former subsection (b)(1)(d) has been deleted and replaced with language that is consistent with the language used in CCPA. (See Civ. Code, §§ 1798.130, subd. (a)(5)(B), 1798.110, subd. (c)(1).) **Renumbered subsection (c)(1)(d)** now requires a business to identify in its privacy policy the categories of personal information that it has collected about consumers in the preceding 12 months. It also requires that the categories be described in a manner that provides consumers a meaningful understanding of the information being collected. By requiring businesses to describe these categories in a manner that is easily understood by consumers, these modifications implement a performance-based approach. (See Schaub, Center for Plain Language.)

Subsections (c)(1)(e) and (c)(1)(f) have been added to require a business, in its privacy policy, to identify the categories of sources from which it collects personal information and the business or commercial purpose for collecting or selling personal information. These subsections implement Civil Code section 1798.110, subdivisions (c)(2) and (c)(3). This addition is necessary to ensure that the privacy policy contains all the information required by the CCPA and benefits consumers by ensuring that the privacy policy is a comprehensive picture of the business's

privacy practices. **Subsections (c)(1)(e) and (c)(1)(f)** further require that the required information be described in a manner that provides consumers a meaningful understanding of the source from which the information is collected and why the information is collected or sold. This is necessary to ensure that the information that businesses are required to provide pursuant to the CCPA are presented in a manner that is easily understood by consumers. (See Civ. Code, § 1798.185, subd. (a)(6); see also Schaub, Center for Plain Language.)

Former subsection (c)(1)(e) has been renumbered and is now **subsection (c)(1)(g)**. It has been modified to require the business to: (1) identify the categories of personal information, if any, that the business has disclosed for a business purpose or sold to third parties in the preceding 12 months (**subsection (c)(1)(g)(1)**); (2) for each category of personal information identified, provide the categories of third parties to whom the information was disclosed or sold (**subsection (c)(1)(g)(3)**); and (3) state whether the business has actual knowledge that it sells the personal information of minors under 16 years of age (**subsection (c)(1)(g)(3)**).

Subsection (c)(1)(g)(1) is necessary to make the language of the regulation consistent with the language in the CCPA (see Civ. Code, §§ 1798.115, subd. (c), 1798.130, subd. (a)(5)(C)), and **subsection (c)(1)(g)(2)** is necessary to implement Civil Code sections 1798.110, subdivisions (c)(3) and (c)(4), 1798.115, and 1798.130, subdivision (a)(4), and to ensure that the privacy policy contains all the information required by the CCPA.

Subsection (c)(1)(g)(3), which was formerly subsection (b)(1)(e)(3), has been modified to add the phrase “actual knowledge” and to delete the phrases “or not” and “without affirmative authorization.” The purpose of this disclosure is to inform consumers whether the business is subject to requirements under the CCPA that only apply to businesses with actual knowledge that they sell the personal information of consumers under 16 years of age. (Civ. Code § 1798.120, subd. (c).) Accordingly, the regulation has been modified to make the regulation consistent with the language used in the CCPA. Additionally, the phrase “without affirmative authorization” has been deleted because it is unlawful for a business to sell the personal information of minors under 16 years of age without affirmative authorization, and thus the initial proposed language would have required a business to explicitly state that it was violating the law. The modifications to this subsection are necessary to ensure that the privacy policy contains the information necessary to inform consumers of their rights under the CCPA, especially with regard to the handling of the personal information of minors under 16 years of age.

Renumbered subsection (c)(2)(a) has been modified to delete the phrase “or maintained.” This change is necessary to make the language in the regulation consistent with the language in the CCPA and other parts of the regulations. (See Civ. Code, § 1798.105, subd. (a); Section 999.301, subd. (r).)

Renumbered subsection (c)(3)(b) has been modified to require that a business state in its privacy policy whether or not the business sells personal information. If the business sells personal information, it is required to include either the contents of the notice of right to opt-out or a link to it, in accordance with section 999.306. This requirement was initially part of former subsection (b)(1)(e) but has been moved to this subsection to avoid redundancy. The subsection

includes the phrase “whether or not” because the CCPA requires a business that has neither disclosed nor sold consumers’ personal information to disclose that fact. (See Civ. Code, §§ 1798.115, subd. (c), 1798.130, subd. (a)(5)(C).) Section 999.306, subsection (d), also provides that a business that does not sell personal information does not need to provide a notice of right to opt-out if it states so in its privacy policy. Thus, the modifications make the language of the regulation consistent with the language in the CCPA and harmonize this subsection with section 999.306, subsection (d). These modifications benefit businesses and consumers by providing clarity and transparency about businesses’ baseline obligations: businesses that state that they sell personal information must post a notice of right to opt-out, and businesses that do not sell personal information will affirmatively state so.

Renumbered subsection (c)(5)(a) has been modified to require a business to “provide instructions on how an authorized agent can make a request under the CCPA on the consumer’s behalf,” rather than explain how a consumer can designate an authorized agent to do so. The change has been made in response to public comments that businesses were not in a position to know how a consumer could designate an authorized agent, as that would be an individual decision made by the consumer and may vary by the agent. Thus, the regulation has been reframed to require businesses to provide information on what they are in a position to know, *i.e.*, how an authorized agent can make requests of the business on the consumer’s behalf. The change is necessary to ensure that the privacy policy contains relevant, helpful information about how consumers can effectively exercise their CCPA rights, including their right to make requests through authorized agents.

Renumbered subsection (c)(6) has been reformatted to move its requirements into what is now **subsection (c)(6)(a)**. This change is necessary to make subsection (c)’s formatting consistent for subsections (c)(1) through (c)(6).

Renumbered subsection (c)(8) has been modified to correct a typographical error and for citation formatting reasons.

Subsection (c)(9) has been added to require a business that has actual knowledge that it sells the personal information of minor under 16 years of age to include in its privacy policy a description of the processes required by sections 999.330 and 999.331. The change is necessary to harmonize section 999.308 with section 999.332, subsection (a), which requires a business subject to sections 999.330 and 999.331 to include a description of the processes set forth in those sections in its privacy policy. The subsection benefits businesses by compiling in one place all the information that must be provided in the privacy policy, which helps businesses better understand and comply with the requirements of the CCPA and the regulations.

Changes made to Article 3. Business Practices for Handling Consumer Requests:

G. 11 CCR § 999.312. Methods for Submitting Requests to Know and Requests to Delete

Subsection (a), which governs the methods a business must provide for the submission of consumers’ requests to know, has been modified to provide that businesses operating exclusively

online and that have a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to know. The requirement that businesses operating a website must provide an interactive webform has also been deleted. These changes are necessary to make the regulations consistent with amendments to the CCPA by AB 1564 (Assem. Bill No. 1564, approved by Governor, Oct. 11, 2019 (2019-2020 Reg. Sess.)). (Civ. Code, § 1798.130, subd. (a)(1)(A).)

Subsection (c), which requires a business to consider the methods by which it interacts with consumers when determining which methods to provide for submitting requests to know and requests to delete, has been modified in four ways. First, the word “primarily” has been inserted before “interacts” to clarify the meaning of the subsection. This clarification is necessary to prevent businesses from designating obscure methods for the submission of consumer requests as a way of discouraging consumers from exercising their rights under the CCPA. Second, the sentence “At least one method offered shall reflect the manner in which the business primarily interacts with the consumer, even if it requires a business to offer three methods for submitting requests to know” has been deleted. This change is necessary so that the language used in the regulation is consistent with the language used in the CCPA. (See Civ. Code, § 1798.130, subd. (a)(1)(A)-(B).) Third, language has been added requiring businesses that primarily interact with consumers in person to consider providing an in-person method for submitting requests. The regulation provides a few examples of in-person methods: a printed form the consumer can directly submit or send by mail, a tablet or computer portal that allows the consumer to complete and submit an online form, and a telephone by which the consumer can call the business’s toll-free number. These examples provide guidance on how businesses should determine which methods to make available to consumers, including those discussed in Civil Code section 1798.130, subdivision (a)(1), while addressing situations in which consumers may need direct, in-person assistance in exercising their CCPA rights. This regulation is necessary to prevent businesses from designating obscure methods for the submission of consumer requests as a way of discouraging consumers from exercising their rights under the CCPA, while also providing businesses with flexibility to adopt methods that are compatible with their business practices. Fourth, **subsections (c)(1)** and **(c)(2)**, which consisted of examples, were deleted as unnecessary in light of the foregoing modifications.

Subsection (d) has been modified to make the two-step process for online requests to delete optional, not mandatory. The modification was made in response to comments that raised concerns that the initial proposed language may conflict with the European Union’s General Data Protection Regulation (GDPR) and its general principle of making it easy for consumers to exercise their choices. The modification reduces the burden on businesses by giving them the flexibility to make a fact-specific determination of what process to use.

Former subsection (e) has been deleted because of the CCPA’s amendment by AB 1564 (Assem. Bill No. 1564, approved by Governor, Oct. 11, 2019 (2019-2020 Reg. Sess.)). (Civ. Code, § 1798.130, subd. (a)(1)(A).)

Former subsection (f) has been renumbered **subsection (e)**. **Subsection (e)(2)** has been modified to replace “specific directions” with “information” in response to public comments that

interpreted the initial proposed language to mean that a business had to provide an individually tailored response on how each deficient request should be remedied. This modification is necessary to clarify that a business can provide a consumer with general information on how to submit their request and address deficiencies. It lessens the burden on businesses while still giving the consumer the opportunity to remedy an incorrect submission of a request.

In light of comments received from the public, the OAG further supplements its statement of reasons in support of subsection (e). (See ISOR, p. 16.) Overall, subsection (e) is necessary to further the CCPA's express purpose of providing consumers with an "effective way to control their personal information." AB 375 (Assem. Bill No. 375, approved by Governor, June 28, 2018 (2018-2019 Reg. Sess.); Stats. 2018, ch. 55, § 2.) Consistent with this legislative intent, the regulation provides guidance for instances in which a consumer's attempt to exercise their CCPA rights is not submitted through a business's designated methods or is deficient for a reason unrelated to the verification process. Businesses should provide assistance to consumers who may be unaware of the business's designated method for submitting CCPA requests or may have made a mistake by contacting the business via some other method. Furthermore, based on the OAG's technical expertise in this area and understanding of business practices, treating a consumer's request as properly received or informing the consumer of the proper method of request is not unduly burdensome. If the business treats a request as properly received, the request proceeds through its designated CCPA-request process. If the business declines to do so, the business can simply provide the consumer with a pre-formulated response with information on how to submit the request and remedy deficiencies.

H. 11 CCR § 999.313. Responding to Requests to Know and Requests to Delete

Subsection (a) has been modified in three ways. First, it has been modified to specify that the time period to confirm receipt of a request is 10 "business" days. This change was made in response to public comments seeking clarification of whether the initial proposed "10 days" constituted calendar days and expressing concern that 10 days was not enough time for a business to confirm receipt, particularly when received during business holidays. The clarification of "business days" addresses business holidays and lessens the burden on businesses. Second, the phrase "in general" has been added to clarify that a business's confirmation of receipt of request simply needs to provide a general description of the business's verification process. This change was made in response to public comments that requested guidance regarding the level of detail required and that expressed concerns that specific descriptions of a business's verification process would reveal information to bad actors that could be used to evade security procedures. This modification balances the CCPA's intent to provide rights and transparency to consumers with the burden on businesses, including potential security concerns. (Civ. Code, §§ 1798.185, subd. (a)(7), 1798.185, subd. (b)(2).) Third, two sentences have been added to clarify that confirmation of the receipt of a request may be made in the same manner in which the request was received, for example by phone. This change was made in response to public comments and is necessary to provide businesses guidance regarding how to confirm receipt of requests. It also reduces the burden on businesses by streamlining the communication methods for receiving and confirming receipt of requests.

Subsection (b) has been modified in two ways. First, the word “calendar” has been added to clarify that the time period to respond to requests to know and requests to delete is 45 calendar days. This change was made in response to comments that sought clarification on whether the time period was calendar or business days. Consumers exercising their rights to make requests under the CCPA should not be hindered by unreasonable delays, and 45 calendar days provides businesses with sufficient time to provide the required response, especially considering that they can extend the time to respond by another 45 calendar days. This change is necessary to avoid possible confusion about how to calculate the 45-day requirement. This modification ensures that businesses expediently address consumer requests and prevents excessive wait times for responses.

Second, the subsection has been modified to add that a business may deny a request if it cannot verify the consumer within the 45-day time period. Although subsections (c)(2) and (d)(1) also provide that a request may be denied if a business cannot verify the identity of the requestor, this sentence is necessary to address how the ability to verify a consumer affects the 45-day time period. It has been added in response to several public comments seeking guidance on what businesses should do if they cannot verify the consumer within the 45-day time period. Some comments by businesses requested modifying subsection (b) to start the 45-day period only after the business verifies the consumer or to otherwise extend the period of time to respond to requests. These businesses were concerned that verification in certain cases may be difficult or require follow up with consumers, thereby necessitating more than 45 days to respond. Other comments, however, contended that allowing businesses three months to respond (45-days with the optional 45-day extension) was unreasonably long and infringed upon a consumer’s CCPA right to access their personal information. The modification balances business and consumer concerns by clarifying that businesses must verify a request within the 45-day period but can deny the request if it cannot be verified within the 45-day period. Moreover, the 45-day time period is consistent with the CCPA, which provides that the verification process “shall not extend the business’ duty to disclose *and deliver* the information within 45 days of receipt of the consumer’s request.” (Civ. Code, § 1798.130, subd. (a)(2) (emphasis added).)

Subsection (c)(1) has been modified to replace the word “consumer” with “requestor.” This change is necessary to clarify that the business may be communicating with either a consumer or a consumer’s authorized agent who made the request.

In light of the comments received from the public, the OAG further supplements its statement of reasons in support of subsections (c)(1) and (c)(2) as follows. (See ISOR, pp. 17-18.) As the primary enforcer of California’s statutes related to breach notification and security of personal information (Civ. Code, §§ 17981.81.5, 1798.82), the OAG has significant expertise in the harms that can arise from the unauthorized disclosure of specific pieces of information as compared to the disclosure of general categories of personal information. First, the OAG has received and analyzed nearly two thousand security breach notifications, which list the types of personal information that were or are reasonably believed to have been accessed. The OAG has also investigated and analyzed numerous security breaches of personal information, including data breaches that have included specific pieces of personal information, such as a Californians’ HIV-

positive status. Second, the OAG has received and reviewed countless consumer complaints that contain detailed allegations of harms that have resulted from breached data. These harms range from the mere inconveniences and time-consuming nature of restoring one's identity and correcting credit files, to frustrating financial losses, to deeply personal and exploitive harms such as the publication of sexually graphic pictures. Based on this experience and expertise, the OAG drafted subsections (c)(1) and (c)(2) to balance a consumer's right to know with the risk of harms that can result from the unauthorized disclosure of the information. These subsections include references to the appropriate verification standard that businesses must apply when responding to requests to know, for further guidance.

Former **subsection (c)(3)** has been deleted in response to public comments that: (1) the regulation was unnecessary in light of the other protections promulgated in the regulations, specifically the verification requirements; (2) the regulation was at risk for abuse by businesses taking a broad view of their need for secrecy; and (3) disclosure to a consumer of their specific pieces of personal information should neither create a risk to the security of a business's systems nor enable bad actors to intrude on a business's systems. The OAG agrees that this subsection is unnecessary and duplicative. The regulations already prohibit the disclosure of highly sensitive identifiers, account passwords, and security questions and answers, as well as require businesses to use reasonable security measures when transmitting personal information to a consumer. (See Section 999.313, subd. (c)(4), (c)(6), and (c)(7).) The regulations also govern verification of consumer requests, which protect consumers from unauthorized disclosure and require businesses to use reasonable security measures to protect consumers' personal information and accounts. (See Sections 999.323, 999, 324, 999.325, 999.326.)

New subsection (c)(3) has been added to set forth the conditions under which a business is not required to search for personal information in response to a request to know. This subsection was added in response to comments that were concerned about a business's burden or inability to search unstructured data for a consumer's personal information (*i.e.*, when a consumer's personal information is not maintained in a searchable format, such as the return address on a payer's check). The change is necessary to balance the goals and purposes of the CCPA while minimizing the burden on businesses searching for personal information to respond to a request to know.

To fall within this exception, a business must meet all the conditions set forth in subsections (c)(3)(a) through (d). **Subsections (c)(3)(a), (c)(3)(b), and (c)(3)(c)** are necessary to narrowly tailor the exception so that it is not abused by businesses to avoid their obligations under the CCPA. **Subsection (c)(3)(a)**, which requires that the personal information not be maintained in a searchable or reasonably accessible format, ensures that the exception is only available when searching for personal information imposes an excessive burden on a business. **Subsection (c)(3)(b)**, which requires that the business maintain the personal information solely for legal or compliance purposes, ensures that the exception is only available when the business cannot avoid the burden by opting to not maintain the personal information. By including this requirement, the exception promotes data minimization principles. Although some public comments suggested including personal information maintained for other purposes, this would allow

businesses to interpret those purposes broadly to evade their obligations under the CCPA. **Subsection (c)(3)(c)**, which requires that the business not sell the personal information or use it for any commercial purpose, applies a general fairness principle to ensure that a business that is not able or willing to disclose personal information to the consumer cannot profit or commercially benefit from that personal information. Finally, **subsection (c)(3)(d)**, which requires the business to describe to the consumer the categories of records that may contain personal information that it did not search, is necessary to provide transparency to consumers. It informs the consumer that the business may have other personal information about them but assures them that this information is only maintained by the business in an unsearchable or inaccessible format, solely for legal or compliance purposes, and is not being used for the business's commercial benefit.

Although some public comments suggested modifying the regulation to permit businesses to fall within this exception if any (rather than all) of these subsections apply, such a modification would too easily allow a business to evade its obligations under the CCPA and could incentivize behavior that would undermine a consumer's ability to exercise their CCPA rights and access what personal information the business has collected about them.

Subsection (c)(4) has been modified in three ways. First, subsection (c)(4) has been modified to delete the phrase "at any time" and to insert the phrase "in response to a request to know." This change is necessary to clarify that subsection (c)(4) is not intended as a blanket prohibition on the disclosure of the specified personal information, but rather that a business shall not disclose this information in response to a request to know. This change was made in response to public comments identifying certain instances where a business may be required to disclose this information pursuant to other laws. Second, subsection (c)(4) has been modified to add "unique biometric data generated from measurements or technical analysis of human characteristics" to the list of specific pieces of personal information that a business shall not disclose in response to a request to know. This change is necessary to balance a consumer's right to know with the harms that can result from the unauthorized disclosure of information. It is also necessary to conform the regulation with Civil Code sections 1798.81.5 and 1798.82, which was amended by AB 1130 to include "unique biometric data generated from measurements or technical analysis of human characteristics." Including this category of personal information in the regulation also benefits businesses by reducing the risk that a business will violate Civil Code § 1798.82 in attempting to comply with the CCPA. The OAG purposefully used the language from Civil Code section 1798.82(h)(1)(F) because it is narrower than the term "biometric information," as defined in the Civil Code section 1798.140, subdivision (b). Third, subsection (c)(4) has been modified to require a business to inform consumers with sufficient particularity that it has collected the type of information set forth in the regulation. It also includes a clarifying example. This change is necessary because it provides direction to businesses on what to communicate to consumers when they are prohibited from disclosing these specified pieces of personal information. It benefits consumers by providing them with information to make privacy decisions while protecting them from the harms that could result from the unauthorized disclosure of this sensitive personal information.

Subsection (c)(5) has been modified to state that a business shall explain the basis for a denial “unless prohibited from doing so by law.” This change was made in response to public comments that the initial proposed language may conflict with instances in which the business may be prohibited by law from disclosing the basis for its denial of a consumer’s request to know specific pieces of personal information. The change is necessary to avoid any conflict between this regulation and other laws.

Subsection (c)(8) has been modified to correct the format of the Civil Code citation.

Subsection (c)(10) has been modified to make the language of the regulation consistent with the language in the CCPA. (See Civ. Code, §§ 1798.110, 1798.115, 1798.130.) The regulation no longer requires that the information in former subsections (a) through (f) be provided for each identified category of personal information a business has collected about a consumer. Instead, the business must disclose, in response to a verified request to know, categories of personal information:

- The categories of personal information the business has collected about the consumer in the preceding 12 months (**subsection (c)(10)(a)**);
- The categories of sources from which the personal information was collected (**subsection (c)(10)(b)**);
- The business or commercial purpose for which it collected or sold the personal information (**subsection (c)(1)(c)**);
- The categories of third parties with which the business shares personal information (**subsection (c)(1)(d)**);
- The categories of personal information that the business sold in the preceding 12 months, and for each category identified, the categories of third parties to which it sold that particular category of personal information (**subsection (c)(1)(e)**); and
- The categories of personal information that the business disclosed for a business purpose in the preceding 12 months, and for each category identified, the categories of third parties to whom it disclosed that particular category of personal information (**subsection (c)(1)(e)**).

These changes are necessary to conform the regulation more closely to the requirements in the CCPA. Specifically, **subsection (c)(10)(a)** tracks the requirements in Civil Code sections 1798.110, subdivisions (a)(1) and (c)(1), 1798.115, subdivision (a)(1), and 1798.130, subdivision (a)(3)(B). **Subsection (c)(10)(b)** tracks the requirements in Civil Code section 1798.110, subdivisions (a)(2) and (c)(2). **Subsection (c)(10)(c)** tracks the requirements in Civil Code section 1798.110, subdivisions (a)(3) and (c)(3). **Subsection (c)(10)(d)** tracks the requirements in Civil Code section 1798.110, subdivisions (a)(4) and (c)(4). **Subsection (c)(10)(e)** tracks the requirements in Civil Code sections 1798.115, subdivisions (a)(2) and (b), 1798.130, subdivision (a)(4)(B). **Subsection (c)(10)(f)** tracks the requirements in Civil Code sections 1798.115, subdivisions (a)(3) and (b), 1798.130, subdivision (a)(4)(C). Altogether, subsections (c)(10)(a) through (c)(10)(f) are necessary because they provide clarity regarding a business’s obligations when responding to requests to know categories of information. These subsections also compile and clarify in one place the statutory requirements, and thus benefits businesses, particularly

small businesses, by making it easier for them to understand how to comply. These subsections are also necessary to protect consumers from being denied their right to know by a business responding in a generic and unspecified way.

Subsection (d)(1) has been modified to delete the requirement that a business treat an unverified request to delete as a request to opt-out of sale. This change was in response to public comments that contended that automatically treating an unverifiable request to delete as a request to opt-out of sale may be inconsistent with a consumer's intent or choice and that it would cause logistical and operational problems for businesses to implement. While the OAG does not necessarily agree with these comments, the requirement has been removed and replaced with an alternative obligation, set forth in subsection (d)(7), that the business instead provide the consumer with the opportunity to opt-out of the sale of their personal information. The last sentence has also been deleted and incorporated into subsection (d)(7). (See discussion below on subsection (d)(7) for further explanation.)

Subsection (d)(2)(b) has been modified to revise the spelling of "deidentifying." This change is necessary to make the language consistent with the term "deidentified" in the CCPA. (See Civ. Code, § 1798.140, subd. (h).)

Subsection (d)(2)(c) has been modified to replace "personal" with "consumer." This change is necessary to make the language consistent with the term "aggregate consumer information" in the CCPA. (See Civ. Code, § 1798.140, subd. (a).)

Subsection (d)(3) has been modified to allow a business to delay compliance with the consumer's request to delete only with respect to personal information stored on an archived or backup system until the archived or backup system "relating to that data is restored to an active system or next accessed or used for a sale, disclosure, or commercial purpose." This change was made in response to comments that were concerned that the initial proposed language "next accessed or used" would be burdensome because the next access or use may be for reasons unrelated to the consumer's personal information, and that it would deter businesses from implementing reasonable data security practices and procedures because routine maintenance, general testing, or testing of disaster recovery protocols could trigger a deletion obligation. The comments also contended that many archived or backup systems do not allow specific, targeted deletions, and thus it would not be technically feasible to delete a particular consumer's information when the archive or backup system was accessed or used. By modifying the regulation to limit the compliance obligation for deleting personal information on backup systems to when those systems are restored or used for a sale, disclosure, or commercial purpose, the regulation lessens the burden on businesses. The modification also preserves the consumer's right to delete when the business discloses or commercially benefits from access or use.

Former **subsection (d)(4)** has been deleted in response to public comments expressing confusion about the purpose and need for the regulation.

New subsection (d)(4) has been added to state that in responding to a request to delete, a business shall inform the consumer whether or not it has complied with the consumer's request. This change is necessary to instruct businesses on what information they must provide to the

consumer and creates a written record of whether or not the business has complied with the consumer's request. This change benefits consumers by confirming that the business received and acted upon the request or, in the event that the business denied the request, allowing the consumer to follow up or remedy any deficiencies resulting in the denial.

Subsection (d)(5) has been modified in three ways. First, the regulation now correctly cites to "section 999.317, subsection (b)," which requires a business to maintain records of consumer requests and how the business responded for 24 months. Second, subsection (d)(5) has been modified to clarify that the business only needs to inform the consumer of the record-keeping requirement if it complies with the request. Although the record-keeping requirement in section 999.317, subsection (b), applies to all requests received, including those the business denies, the disclosure to the consumer required here is necessary to dispel any assumption that granting a request to delete will also delete any record of the request. Notification that the request was denied is unlikely to lead to such an assumption. Third, language has been added to clarify that a business may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from the business's records. This change was in response to comments seeking guidance on whether businesses can maintain a suppression list. This change benefits businesses by dispelling uncertainty and benefits consumers by preventing a business from re-collecting information that the consumer had previously requested it to delete.

Subsection (d)(6)(a) has been modified to replace the phrase "statutory and regulatory exception therefor" with the phrase "conflict with federal or state law, or exception to the CCPA, unless prohibited from doing so by law." Businesses that deny a consumer's request to delete shall inform the consumer of the basis for the denial, including any conflict with law or exception to the CCPA. This change is necessary to make the language consistent with language in other requirements of the regulations. (See Section 999.313, subd. (c)(5).) The inclusion of the phrase "unless prohibited from doing so by law" was made in response to public comments that the initial proposed language may conflict with instances in which the business may be legally prohibited from disclosing the basis for its denial of a consumer's request to delete. The change is necessary to avoid any conflict between this regulation and other laws.

Subsection (d)(7) has been added to address instances in which a business that sells personal information denies a consumer's request to delete. If the consumer has not already made a request to opt-out, the regulation requires the business to ask the consumer if they would like to opt out of the sale of their personal information and to provide either the contents of, or a link to, the notice of right to opt-out. This language, some of which was initially included in subsection (d)(1), was moved to be a stand-alone subsection to clarify that the business must ask the consumer in any instance in which it denies the consumer's request to delete, not just when the denial is based on an inability to verify the requestor. The language was also modified to explicitly apply to businesses that sell personal information. This change is necessary to address concerns raised in comments that the initial proposed language applied to businesses that did not sell personal information and left those businesses unclear on how to comply. This regulation benefits consumers by providing them with an alternative to the deletion of their personal

information, if their request to delete is deny, that would at least prevent the further proliferation of their personal information in the marketplace.

Former subsection (d)(7) has been renumbered and is now **subsection (d)(8)**. The section has also been modified to delete the last sentence, which required the business to use a two-step confirmation process where the consumer confirms their selection as required by section 999.312, subsection (d). This change is necessary because the two-step confirmation process set forth in section 999.312, subsection (d), has been modified to be optional, not mandatory. (See Section 999.312, subd. (d).)

I. 11 CCR § 999.314. Service Providers

Subsection (a) has been modified to replace “a person or entity” with “business.” Neither a “person” nor an “entity,” by itself, would need to comply with the same obligations as a “business.” (Civ. Code, §§ 1798.100, 1798.105, 1798.110, 1798.115, 1798.120 [imposing obligations on a “business”, e.g., to respond to consumer requests]; see also Civ. Code, § 1798.140, subd. (c) [setting forth specific threshold requirements for what constitutes a “business”].) Therefore, it is unnecessary to extend service-provider protections to a “person or entity;” “business” is the more accurate term. Along with some minor grammatical changes, the subsection has also been modified so that businesses deemed service providers pursuant to this subsection are bound by the limitations imposed on service providers under the CCPA and section 999.314. This change is necessary to impose all obligations within the CCPA and section 999.314 on service providers, not just those set forth in the CCPA definition of “service provider.”

In light of comments received from the public, the OAG further supplements its statement of reasons in support of subsection (a). (See ISOR, p. 21.) Overall, subsection (a) is necessary to address the unintended consequences that would result from allowing consumers to access and delete personal information held on behalf of public and nonprofit entities and that would otherwise not be subject to the CCPA. Like businesses, public and nonprofit entities outsource operational needs through service providers that essentially perform tasks as if the public or nonprofit entity was doing the task in-house themselves. These public and nonprofit entities also store documents in cloud storage, use email systems provided by third parties, and employ vendors to manage data. For example, a public school district may use a service provider to secure student information, including each student’s grades and disciplinary record. Without this regulation, service providers used by public and nonprofit entities may be required to disclose or delete records in response to consumer requests because they may constitute businesses that maintain consumers’ personal information. Service providers for public and nonprofit entities could also be asked to disclose personal information maintained by a government agency, despite the fact that such files may be expressly exempt from disclosure under the Public Records Act.

Accordingly, the OAG has promulgated this regulation pursuant to its authority to adopt regulations as necessary to further the purposes of the CCPA. (See Civ. Code, § 1798.185, subd. (b)(2).) Treating a service provider for a public entity or nonprofit as a “business” would not support the purpose and intent of the CCPA because it may expose otherwise exempt personal

information to access and deletion requests or force service providers to create unnecessary and burdensome systems to respond to consumer requests. California law does not provide a right to delete information held by a public entity, nor does it provide a right to access personal information held by a nonprofit entity. The CCPA imposes obligations on “businesses,” which excludes public and nonprofit entities. (See Civ. Code, §§ 1798.100, 1798.105, 1798.110, 1798.115, 1798.120 [imposing obligations on businesses].) It is not intended to allow consumers to know or delete personal information collected by a non-business merely because the non-business outsources tasks to a service provider. In addition, California law already imposes a separate and distinct legal regime to access information held by public entities, including requirements and exceptions that differ from the CCPA. (See, e.g., Gov. Code, § 6250 et seq.) Without this regulation’s clarification, non-businesses, such as public and nonprofit entities, may not be able to employ service providers without risking disclosure or deletion of personal information or without unnecessary and burdensome costs, which may cause them to incur extra expenses to perform operations internally.

Some comments contend that businesses providing services to public and nonprofit entities should only be considered a service provider in specific circumstances. However, none of these comments proposed any specific enumerated exceptions that would be a reasonable alternative to this regulation. Given the numerous ways in which public and nonprofit entities employ service providers, crafting exceptions would be difficult and impractical and would provide less protection than the CCPA and these regulations. (See Civ. Code, § 1798.140, subd. (v); Section 999.314, subd. (c).)

Subsection (b) has been modified to clarify that a service provider that collects personal information about or directly from consumers at the direction of a business may still qualify as a service provider under the CCPA. Specifically, the terms “first business” and “second business” have been used to clearly distinguish between the businesses being referred to in the subsection and to remove any potential ambiguity regarding which business is directing the collection of personal information. The phrase “second business” was not intended to alter the types of corporate entities that may qualify as a service provider set forth in Civil Code section 1798.140, subdivision (v), or to impose onto that statute the thresholds for a business that are set forth in Civil Code section 1798.140, subdivision (c)(1)(A)-(C). Rather, the phrase was intended to succinctly refer to service providers that collect information about or directly from consumers at the direction of a business with which it has a service-provider relationship. This subsection clarifies that these service providers do not lose their status as service providers merely because they collect consumers’ personal information if that collection is performed at the business’s direction and on behalf of that business.

The phrase “or about a consumer” has also been added to clarify that a service provider may collect personal information either directly from a consumer, or *about* a consumer, on behalf of the business. This clarification is necessary because businesses employ service providers to perform both types of data collection on their behalf. Treating such collections differently would be confusing, impair the functioning of the service-provider relationship, and potentially introduce unintended consequences. For example, a business may direct a service provider to

collect personal information from one consumer about both that consumer and their spouse; there is no logical reason to allow the first collection but prohibit the second. Finally, the words “obligations” and “the CCPA and these regulations” have been added to match the language of subsection (a), for the same reasons discussed above.

Subsection (c) has been substantially modified. The subsection now prohibits a service provider from retaining, using, or disclosing personal information obtained in the course of providing services except to provide those services in compliance with the written contract for services and in four other limited circumstances. This prohibition is consistent with how the CCPA defines and regulates the disclosure of consumer personal information to service providers and service providers’ use of that information. For the purpose of processing personal information, the CCPA contemplates service providers to be an extension of the business for which it provides services. Civil Code section 1798.140, subdivision (v), defines a “service provider” as one who “processes information on behalf of [the] business” that provided the personal information, pursuant to a contract that prohibits “retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.” Relatedly, a business does not “sell” personal information when it transfers that data to a service provider, provided that the service provider does not “collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose” of the business that provided the personal information. (Civ. Code, § 1798.140, subd. (t)(2)(C).) Thus, the intent of the CCPA is to prohibit a service provider from using personal information collected from one business for its own business purposes or to then provide services on behalf of a different business.

Many comments objected to the original text of subsection (c), claiming that the CCPA broadly authorizes service providers to retain and use personal information for any “business purpose.” But nothing in the CCPA allows a service provider to retain or use personal information for its own business purpose. Rather, as discussed above, services providers are expressly limited from retaining and using personal information. (Civil Code § 1798.140, subs. (v) and (t).) Indeed, the term “business purpose,” when used in the statutory text, contextualizes why a *business* discloses personal information to a service provider or third party, not the universe of possible ways a service provider could use that information. (See Civ. Code, §§ 1798.115, subd. (a), 1798.130, subd. (a)(4)(C).) The CCPA requires that any disclosure of personal information from a business to a service provider be “necessary to perform a business purpose.” (Civ. Code, § 1798.140, subd. (t)(2)(C).) Even in defining the term “service provider,” the CCPA makes clear that a business’s disclosure of personal information must be for a business purpose that is stated in the parties’ written contract. (Civ. Code, § 1798.140, subd. (v).) Subsection (c) thus accurately reflects the CCPA’s requirement that service providers act on behalf of a business by processing information to further the *business’s* specific business purpose and not for the service provider’s own business purposes.

Subsections (c)(1) through (c)(5) provide the limited circumstances under which service providers may retain, use, and disclose personal information. **Subsection (c)(1)** allows service providers to process and maintain personal information obtained in the course of providing services, as long as the service provider is acting on behalf of the business that provided the

personal information or directed it to collect the personal information, and the service provider is complying with the written contract with that business for services required by the CCPA. This subsection closely tracks the CCPA’s definition of the term “service provider.” (See Civ. Code, § 1798.140, subd. (v).) It makes clear that a service provider may not retain, use, or disclose personal information to provide services to a third party because such services would not be “on behalf of the business that provided the personal information.”

Subsection (c)(1) was modified to more closely track the CCPA. Public comments also raised concerns that the initial proposed version imposed too great a restriction by entirely prohibiting a service provider from using personal information obtained from one business to service another. Without the modified text, the regulation could prohibit businesses that employ a service provider to render services to a third party at the direction of and on behalf of the business. Businesses benefit from this clarification because it more closely aligns with and explains the statutory text.

Subsection (c)(1) also clarifies that the processing of personal information must be “in compliance with the written contract for services required by the CCPA.” This language has been added to clarify two requirements: (1) that service providers act pursuant to a contract and (2) that the contract meets the requirements in Civil Code section 1798.140, subdivision (v). This subsection explains the statutory text prohibiting a service provider from collecting, using, or selling personal information “for any purpose other than the specific purpose of performing the services specified in the contract *for the business*” that had provided the personal information, including for the service provider’s own commercial purposes. (Civ. Code, § 1798.140, subd. (v) (emphasis added).) The modification to this subsection also clarifies that a service provider’s breach of these requirements is a violation of the CCPA and these regulations and is thus enforceable by the OAG. This is necessary to ensure that service providers comply with these restrictions set forth in their service-provider contracts even if the business does not enforce those restrictions. This benefits consumers because businesses may not have an adequate incentive to enforce restrictions that protect consumers.

Subsection (c)(2) allows services providers to hire subcontractors provided that the subcontractors meet all the requirements for a “service provider” set forth in the CCPA and these regulations. This provision has been added in response to public comments that the initial proposed language may be interpreted to prevent service providers from using subcontractors. Although the CCPA does not explicitly speak to the issue of subcontracting, Civil Code section 1798.140, subdivision (d)(5), implies that it is allowed. (Civ. Code, § 1798.140, subd. (d)(5) [refers to “performing services on behalf of the business or service provider...”].) Requiring that a subcontractor meet all the requirements for a “service provider” extends the service provider’s obligations to protect consumer personal information to the service provider’s subcontractor. This subsection benefits businesses and service providers by providing service providers the flexibility to hire subcontractors, while preserving consumers’ rights by protecting against the misuse or inappropriate sharing of their personal information.

Subsection (c)(3) has been added to allow service providers to use personal information internally to build or improve the quality of their services provided that they do not use the

information to build or modify household or consumer profiles to use in providing services to another business, or to correct or augment data acquired from another source. This subsection has been added in response to several public comments concerned that the initial proposed regulation would have prohibited service providers from making technical improvements to their services if the improvements in any way used personal information, including personal information collected from multiple businesses. For example, a vendor offering customer relationship management software may want to analyze how one client used its software to access customers' personal information and then make improvements using that analysis. Subsection (c)(3) accordingly employs the phrase "internal use" to allow service providers to use personal information in the course of developing or improving services, and clarifies that the service provider is prohibited from using that personal information to build or modify consumer profiles to service a different business and from "correcting or augmenting data acquired from another source." These prohibitions make clear that personal information acquired from or on behalf of one business cannot be used to provide services to another business—*i.e.*, for commercial purposes. Finally, the subsection uses the term "data," instead of "personal information," to encompass the use of personal information acquired from a business to reidentify deidentified consumer information acquired from another source. The use of this term is deliberate because the definition of personal information does not include consumer information that has been deidentified. (Civ. Code, § 1798.140, subd. (o)(3).)

These modifications are necessary to ensure that a service provider's internal use of personal information does not functionally operate to make personal information available to multiple businesses. Doing so would constitute a sale, which includes "making [personal information] available" to others (Civ. Code, § 1798.140, subd. (t)(1)), and effectively usurp the consumer's right to prevent the sale of their personal information. It could also allow service providers to use personal information for a commercial purpose other than providing the services specified in their written contracts, in contravention of Civil Code section 1798.140, subdivision (v). For example, a business may provide mailing addresses to a service provider with whom it has contracted to send marketing mail to its customers. Subsection (c)(1) allows the service provider to use the personal information to perform that service, but subsection (c)(3) would prohibit the service provider from reusing the consumer's address to send mail on a different business's behalf or to internally update the consumer's address on mailing lists maintained for others. The burdens these restrictions place on businesses are limited and reasonable because together, subsections (c)(1) and (c)(3) appropriately balance allowing service providers to offer robust, innovative services to the business that has a direct relationship with the consumers while at the same time protecting consumers from having their personal information functionally made available to other businesses.

Subsection (c)(4) has been added to include the initial proposed language in subsection (c) allowing service providers to use personal information to the extent necessary to detect data security incidents or protect against fraudulent or illegal activity. As stated in the ISOR, this exception is consistent with the purposes of the CCPA and with similar exceptions in other California privacy and consumer protection laws. (See Student Online Personal Information

Protection Act, Bus. & Prof. Code, § 22584; California Financial Information Privacy Act, Fin. Code, § 4056; Consumer Credit Reporting Agencies Act, Civ. Code, § 1785.15.)

Subsection (c)(5) has been added to clarify that service providers are also afforded the exceptions set forth in Civil Code section 1798.145, subdivisions (a)(1)-(4). Some comments noted that service providers may need, for example, to exercise or defend legal claims with the business that provided the personal information. The OAG has interpreted that the phrase “as otherwise permitted by this title” in Civil Code section 1798.140, subdivision (v), was drafted to allow service providers to use personal information for the same, limited uses as those provided to businesses in Civil Code section 1798.145, subdivisions (a)(1)-(4). The subsection thus clarifies that the regulations do not restrict service providers’ retention, use, or disclosure of personal information when required to comply with federal or state law, to cooperate with legal investigations and process, and to exercise or defend legal claims. This regulation is necessary to resolve any potential conflict between subsection (c)’s general prohibition against service providers using or disclosing personal information outside of providing the specified service and the allowances to use personal information “as otherwise permitted” by Civil Code section 1798.145, subdivision (a)(1)-(4).

Subsection (d) has been added to prohibit service providers from selling data on behalf of a business when a consumer has opted out of the sale of their personal information with that business. The CCPA requires a business to inform service providers that a consumer has exercised their right to opt out of the sale of their personal information but does not expressly require the service provider to comply with that opt-out request. This regulation is necessary to resolve any potential ambiguity regarding whether a service provider must comply. It is consistent with the purpose and intent of the CCPA because there would be no reason for the business to inform the service provider of the request if the service provider was not required to comply. Additionally, the subsection prevents a business from relying on this ambiguity to ignore requests to opt-out by employing a service provider to process the sale of personal information.

Former subsection (d) has been renumbered and is now **subsection (e)**. The initial proposed language has been replaced with the requirement that a service provider that receives a request to know or a request to delete from a consumer either act on behalf of the business in responding to the request, or inform the consumer that it cannot act on the request because it is a service provider. The subsection no longer requires service providers to provide the consumer with contact information for the business on whose behalf they process the consumer’s personal information. This change was made in response to numerous public comments regarding the practical difficulties service providers face in identifying the businesses that may have submitted personal information about a consumer, particularly when a service provider provides services for many businesses that may have submitted personal information about the same consumer. The modification lessens the burden on businesses and service providers, but it allows for the service provider to respond to the request if the business directs it to do so. It also benefits consumers by requiring that the service provider tell the consumer that it cannot comply with their request. Consumers should receive a response to their request because they may not know

that the entity to whom they directed the request is a service provider and may otherwise think the request has been lost or ignored.

Former subsection (e) has been renumbered and is now **subsection (f)**.

J. 11 CCR § 999.315. Requests to Opt-Out

Subsection (a) has been modified in four ways. First, the phrase “at a minimum” has been deleted as unnecessary verbiage. Second, “webform” has been replaced with “form” to avoid potential confusion regarding the undefined term “webform.” Third, the subsection has been modified to add the word “global” before “privacy controls” to clarify that the privacy controls should apply to all online services, websites, and mobile applications, as opposed to a localized privacy setting for a specific website or mobile application. “Global privacy controls” provide a mechanism for consumers who want a comprehensive option that broadly signals the consumer’s opt-out request, as opposed to going website by website to make individual requests, which would be time-consuming, burdensome, and confusing for some consumers. Fourth, the subsection was modified to add “device settings” as an example of a global privacy control to reflect the ubiquity with which online information is collected via mobile devices.

Subsection (b) has been modified to delete the word “average.” This change was made because several public comments expressed confusion about the meaning of the term “average consumer” and the use of the word did not enhance the understanding of the regulation.

Subsection (c) has been added to require that a business’s methods to submit opt-out requests are easy for consumers to locate and use. This addition is necessary to avoid the possibility that some businesses may create confusing or complex mechanisms for consumers to exercise their rights under the CCPA. It would run counter to the intent of the CCPA if websites introduced choices that were unclear or, worse, employed deceptive dark patterns to undermine a consumer’s intended direction. (See Paternoster, *Getting round GDPR with dark patterns. A case study: Techradar* (Aug. 12, 2018) <<https://www.leonpaternoster.com/posts/techradar-gdpr/>> [as of May 21, 2020].) This addition was made in response to comments raising concerns about this issue and urging the OAG to make this modification. This regulation furthers the CCPA’s purpose and intent, and benefits consumers, by ensuring that businesses do not frustrate or subvert consumers’ ability to exercise their rights under the CCPA.

Former subsection (c) has been renumbered and is now **subsection (d)**. Subsection (d) has been modified to include the phrases “global privacy controls” and “device settings” for the same reasons those changes were made in subsection (a), discussed above. Subsection (d) has also been modified to add **subsections (d)(1)** and **(d)(2)**.

Subsection (d)(1) has been added to provide clear guidance that any privacy control designed or developed should clearly communicate or signal that a consumer intends to opt-out of the sale of personal information. This subsection addresses public comments concerned that a global privacy control may not respect consumer choice, as well as comments seeking clarification on what would constitute a privacy control that communicates the consumer’s choice to opt-out. By requiring that a privacy control be designed to clearly communicate or signal that the consumer

intends to opt-out of the sale of personal information, the regulation sets clear parameters for what the control must communicate so as to avoid any ambiguous signals. It does not prescribe a particular mechanism or technology; rather, it is technology-neutral to support innovation in privacy services to facilitate consumers' exercise of their right to opt-out. The regulation benefits both businesses and innovators who will develop such controls by providing guidance on the parameters of what must be communicated. And because the regulation mandates that the privacy control clearly communicate that the consumer intends to opt-out of the sale of personal information, the consumer's use of the control is sufficient to demonstrate that they are choosing to exercise their CCPA right.

Subsection (d)(2) has been added to clarify how a business must respond when receiving a global privacy control signal for a consumer who has previously agreed to allow the sale of their information, including through participating in a financial incentive program or through a previous business-specific setting. The subsection requires the business to respect the global privacy control signal, but allows the business to notify the consumer of the conflict and ask the consumer to confirm their business-specific privacy setting or participation in the financial incentive program. This subsection is necessary to eliminate confusion by businesses that have received conflicting manifestations of intent from a consumer. It also provides businesses guidance on how to interpret Civil Code section 1798.135, subdivision (a)(5)'s 12-month prohibition on requesting that the consumer authorize the sale of their personal information for consumers who have enabled a global privacy control. Furthermore, this modification benefits consumers by ensuring that they can make discrete choices about the sale of their personal information while still enjoying the ease and reduced friction of not having to submit separate requests to opt-out on multiple websites or applications.

In light of the comments received from the public, the OAG further supplements its statement of reasons in support of subsection (d) as follows. (See ISOR, p. 24.) Subsection (d) requires a business that collects personal information online to treat user-enabled global privacy controls as a valid request to opt-out. This subsection is forward-looking and intended to encourage innovation and the development of technological solutions to facilitate and govern the submission of requests to opt-out. Given the ease and frequency by which personal information is collected and sold when a consumer visits a website, consumers should have a similarly easy ability to request to opt-out globally. This regulation offers consumers a global choice to opt-out of the sale of personal information, as opposed to going website by website to make individual requests with each business each time they use a new browser or a new device.

As stated in the ISOR, this subsection is necessary because without it, businesses are likely to reject or ignore tools that empower consumers to effectuate their opt-out right. This is based on the OAG's expertise in this subject area. As the primary enforcer of the California Online Privacy Protection Act (Bus. & Prof. Code, § 22575 et seq.) (CalOPPA), the OAG has reviewed numerous privacy policies for compliance with CalOPPA, which requires the operator of an online service to disclose, among other things, how it responds to "Do Not Track" signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personally identifiable information about their online activities over time and across third-

party websites or online services. (Bus. & Prof. Code, § 22757, subd. (b)(5).) The majority of businesses disclose that they do not comply with those signals, meaning that they do not respond to any mechanism that provides consumers with the ability to exercise choice over how their information is collected. Accordingly, the OAG has concluded that businesses will very likely similarly ignore or reject a global privacy control if the regulation permits discretionary compliance. The regulation is thus necessary to prevent businesses from subverting or ignoring consumer tools related to their CCPA rights and, specifically, the exercise of the consumer's right to opt-out of the sale of personal information.

Contrary to public comments that the user-enabled global privacy setting is outside of the scope of the OAG's authority, subsection (d) is authorized by the CCPA because it furthers and is consistent with the language, intent, and purpose of the CCPA. Civil Code section 1798.185, subdivisions (a)(4)(A)-(B), specifically mandate that the OAG establish rules that "facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information pursuant to Section 1798.120" and "to govern business compliance with a consumer's opt-out request." The CCPA also provides the OAG with the authority to adopt regulations as necessary to further the purposes of the CCPA. (See Civ. Code, § 1798.185, subd. (b)(2).) Inherent in this authority is the ability to adopt regulations that fill in details not specifically address by the CCPA, but fall within the scope of the CCPA. The CCPA establishes the baseline that a business must provide a "Do Not Sell My Personal Information" link (see Civ. Code, § 1798.135, subd. (a)(1)), but it does not foreclose the OAG from establishing additional mechanisms to facilitate the submission of a consumer's opt-out request. Indeed, the CCPA applies to businesses that operate in both online and offline contexts. Reading the CCPA to only provide a "Do Not Sell" link as the sole method through which a consumer may exercise their right to opt-out of the sale of their personal information would foreclose or inhibit the consumer's ability to exercise this profound right with a significant portion of businesses that must comply with the CCPA.

Unlike other privacy law frameworks, such as the federal Health Insurance Portability & Accountability Act (HIPAA) or the European Union's General Data Protection Regulation (GDPR), the CCPA is the first law to vest consumers with the right to stop the sale of their personal information. Fortifying this right so that it is meaningful for consumers requires that the OAG establish a robust set of rules and procedures. Furthermore, nothing in the written legislative history indicates that the Legislature intended to limit the OAG's rulemaking related to consumer opt-out requests to the development of an opt-out logo or button. If this were the case, then Civil Code section 1798.185, subdivisions (a)(4)(A) and (B), would have been written to expressly indicate such a limitation, such as by only referring to Civil Code section 1798.135 and not to Civil Code section 1798.120.

The OAG does not believe there are reasonable alternatives to requiring a business to treat user-enabled global privacy controls that meet the requirements of subsection (d)(1) as a valid request submitted pursuant to Civil Code section 1798.120. Although some comments have proposed alternative procedures by which consumers may submit an opt-out request, these alternative methods are not as effective in carrying out Civil Code section 1798.120 on a global scale. For

example, using a business's designated methods for submitting requests to know or requests to delete for the submission of opt-out requests is insufficient because it would not be an effective method to counterbalance the ease and frequency by which personal information is collected and sold in online contexts, such as when a consumer visits a website. Moreover, requests to know and requests to delete must be verified, while requests to opt-out do not. Using a procedure that requires verifiable requests would place a barrier on a consumer's exercise of their right to opt-out, which would be contrary to the CCPA. While businesses may offer such a method as one option for consumers to submit an opt-out request, this does not absolve their obligation to honor global privacy controls crafted in accordance with these regulations.

Former subsection (d) has been renumbered and is now **subsection (e)**. Subsection (e) was modified to replace the phrase "sales of certain categories" with "sale for certain uses." This change was made in response to public comments that consumers are more likely to prefer to choose the reasons why their information is being disclosed rather than the specific categories of personal information disclosed. This change benefits consumers because it provides them with meaningful control over how their information may be used.

Former subsection (e) has been renumbered and combined with **subsection (f)**. **Subsection (f)** now states that a business shall "comply" with a request to opt-out as soon as feasibly possible but no later than 15 "business" days from the date the business receives the request. It also no longer requires a business to notify all third parties to whom it sold the consumer's personal information within 90 days prior to its receipt of the opt-out request, or to direct those third parties not to sell the consumer's information. Instead, it requires a business that sells a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request to notify those third parties that the consumer has exercised their right to opt-out and to direct those third parties not to sell that consumer's information.

The modification that a business comply with the request within 15 *business* days was made after considering public comments from many businesses and consumer advocates. Some comments called for eliminating the 15-day requirement or extending it to align with the 45-day requirement for responding to requests to know or to delete. Some comments claimed operational difficulties in complying with opt-out requests within 15 days, particularly if requests are received during the holidays, and asked that the regulation at least be modified to 15 business days, not calendar days. Other comments advocated for requiring compliance "immediately" or within 24 hours of receipt of the request due to the immediate nature of the collection and sale of personal information online. The OAG weighed these various comments and determined that 15 business days appropriately balances the right of consumers to opt out at any time with the burden on businesses to process opt-out requests. Because the CCPA applies to a wide range of industries and factual situations, immediate compliance or compliance within 24 hours may be significantly burdensome to some businesses, especially businesses that primarily interact with consumers in person. However, the modification also accounts for consumers' concerns about the further proliferation of their personal information by requiring a business to instruct any third parties to whom it sold a consumer's personal information after receiving an opt-out request, but

before the business complied with that request, that they must not sell that information. This allows the consumer's opt-out request to functionally operate as if it were complied with upon the business's receipt.

The initial proposed language requiring a business to notify third parties to whom it sold a consumer's personal information within 90 days prior to receiving the consumer's opt-out request, and the corresponding requirement to inform the consumer after the business has notified those parties, have been deleted in response to a variety of public comments opposing those requirements. Comments contended that these requirements were overly burdensome and impractical, contrary to consumers' choice, and contrary to the doctrine of prospective application of laws, among other reasons. Although the OAG does not agree with these contentions, the requirement has been removed and replaced with the framework discussed above. This modification addresses businesses' concerns while still preventing the further proliferation of a consumer's personal information after the consumer has exercised their right to opt-out. It also benefits consumers by removing any incentive a businesses may otherwise have to delay complying with an opt-out request.

Subsection (g) has been modified to clarify that a consumer's written permission to the authorized agent must be "signed by the consumer." This change is necessary to clarify that the permission may be signed physically or electronically, as the term "signed" is defined by these regulations. The change was made in response to public comments seeking clarification on whether the permission can be provided electronically and benefits consumers by making it easier for a consumer to provide permission to an authorized agent. The subsection has also been modified to include the phrases "global privacy controls" and "device settings" for the same reasons those changes were made in subsection (a), as discussed above.

Subsection (h) has been modified to replace "requesting party" with "requestor." This change is necessary to make the language in this subsection consistent with the use of the term "requestor" in other sections of the regulations.

K. 11 CCR § 999.316. Requests to Opt-In After Opting Out of the Sale of Personal Information

Subsection (b) has been modified to clarify the circumstances in which a business may inform a consumer who has opted-out that they can reverse that request and opt-in or consent to the sale their personal information. Civil Code section 1798.135, subdivision (a)(5), requires that a business respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of their personal information. The modifications clarify that, even if the 12 months have not passed, businesses may inform consumers who initiate a transaction or attempt to use a product or service that requires the sale of their personal information that they need to opt-in to the sale of personal information in order to proceed. This change is necessary because the initial proposed language only referred to transactions, not the use of products or services that required the sale of personal information. This change benefits both businesses and consumers by preventing any unwanted obstacles to interactions with the business that the consumer initiates.

L. 11 CCR § 999.317. Training; Record-Keeping

Subsection (b) has been modified to expressly state that businesses must implement and maintain reasonable security procedures and practices in maintaining the required records. The modification is necessary to ensure that businesses understand their obligation to securely maintain these required records, particularly because they must maintain these records for at least 24 months. The modification will help protect any personal information that may be included in these records from data breaches or other security risks.

Subsection (e) has been modified to narrowly authorize uses of information maintained for record-keeping purposes “as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and these regulations” and to prohibit sharing this information “with any third party except as necessary to comply with a legal obligation.” These changes were made in response to public comments that the initial proposed regulation may prohibit businesses from analyzing data that would improve their compliance processes, including how they respond to consumer requests. This regulation clarifies that businesses may use the data for this purpose but protects consumers by limiting the use of this data for other purposes and by prohibiting data-sharing with third parties except as necessary to comply with a legal obligation. The limitations are necessary to clarify allowable uses for the information and to ensure that businesses do not sell the information or interpret uses “reasonably necessary for the business to review and modify its processes for compliance” in an overly broad manner that would be inconsistent with the purposes of the CCPA. These limitations are particularly necessary given that businesses are required to maintain this information for at least 24 months. (See Section 999.317, subd. (b).)

Subsection (f) has been modified to replace the phrase “Aside from this record-keeping purpose” with the phrase “Other than as required by subsection (b).” This change is necessary to clear up any ambiguity as to which particular record-keeping purpose the subsection is referring.

Subsection (g) has been modified in three ways. First, a “knows or reasonably should know” standard has been added with regard to whether a business meets the threshold amount of consumers’ personal information. This change is necessary to clarify the requisite standard of knowledge and to respond to concerns that businesses may have to collect additional personal information from consumers, such as residence information, to determine whether the business meets the threshold. The modification applies data minimization principles in clarifying that businesses do not have to collect additional personal information for the purpose of determining whether they meet the threshold. Businesses that know or reasonably should know that they have handled the personal information of 10,000,000 or more consumers, based on consumers’ personal information and other information the business collects, are subject to the requirements in subsection (g).

Second, the threshold for the requirements set forth in subsection (g) has been modified from “4,000,000” to “10,000,000.” A business that buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes the personal information of *10,000,000 or more* consumers is subject to the requirements in subsection (g). The OAG has increased the

threshold to 10,000,000 consumers, which is approximately 25 percent of the state's total population, to address public comments that the 4,000,000 threshold would impose a substantial burden on smaller businesses. The modification lessens the burden on smaller businesses and imposes the regulation's reporting obligations only on businesses most in need of oversight (because of the amount of personal information they handle). It also benefits consumers by mandating public transparency on how businesses that acquire or sell consumer personal information respond to consumer requests.

Third, subsection (g) has been modified to clarify that the qualifying time span for calculating whether a business meets the 10,000,000 threshold is "in a calendar year" rather than "annually." This change is necessary because public comments expressed some uncertainty about when the accounting of consumer personal information needed to be conducted. This change makes clear that a business that meets the threshold in a calendar year is subject to the requirements in subsection (g).

Subsection (g)(1)(d) has been modified to allow businesses to compile either the median or mean number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out. Previously, the provision only allowed the median number of days. The change from "median number of days" to "median or mean number of days" was made in response to public comments requesting that businesses be allowed to disclose the average number of days because the median number of days may be difficult to calculate. The modification now provides businesses with this flexibility.

Subsection (g)(2) has been clarified to state that businesses must report the information required by subsection (g)(1) "by July 1 of every calendar year." This change is necessary to respond to public comments expressing concern about the limited time within which businesses would have to compile and disclose the required information after the regulations go into effect, and about the burden on businesses to process and publish that information. The annual July 1 deadline provides clarity by establishing a set date for when the disclosures must be made. The July 1 date was set to align with the date on which the Attorney General could bring an enforcement action. (Civ. Code § 1798.185, subd. (c).) Businesses subject to subsection (g) have six months to compile and disclose the required information for the prior calendar year. For example, businesses will have until July 1, 2025, to compile and disclose the required information for the calendar year 2024. This modification benefits businesses by resolving ambiguity about the regulation's timeline requirements and by providing sufficient time for businesses to process and publish the required information.

Subsection (g)(3) has been added to provide businesses the flexibility to identify the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds. This subsection was added in response to public comments that claimed that general statistics about denials, without further detail, would provide an incomplete or misleading picture about a business's response practices. For example, businesses were concerned that they would be viewed negatively for denying requests even if they had a valid basis to do so. This subsection expressly allows businesses to identify the reasons for denials, if they so choose. It also benefits

consumers by providing them with insight into the business's practices and by addressing any potentially wrong assumptions about the business's practices.

Subsection (g)(4) has been added to provide businesses the flexibility to compile and disclose the information required by subsection (g)(1) for requests received from all individuals, rather than just consumers (*i.e.*, California residents). Businesses who choose to do so must disclose that they are doing so. This subsection was added in response to public comments relaying the difficulties businesses may have in identifying which requests were made by California consumers, particularly if a business does not already collect residency information or grants CCPA requests regardless of the requestor's residency. This change reduces the burden on businesses by allowing them to publish metrics based on all requests, not just those from California consumers. The subsection requires businesses who opt to disclose information for requests received from all individuals to, upon request, compile and provide to the Attorney General the information required by subsection (g)(1) for California consumers. This is necessary to monitor and enforce compliance with the CCPA.

Former subsection (g)(3) has been renumbered and is now **subsection (g)(5)**. This subsection has been modified to clarify that the requirements apply to consumer requests "made under the CCPA" in order to resolve any ambiguity regarding the type of consumer requests to which the subsection refers.

In light of the comments received, the OAG further supplements its statement of reasons in support of section 999.317, subsection (g), as follows. (See ISOR, p 28.) For a number of reasons, the compilation and reporting metrics are reasonably necessary to measure compliance with the CCPA and to further the purpose of the CCPA to empower consumers by giving them control over their personal information. First, the metrics will assist in determining whether systematic response times to CCPA requests comply with the 45-day timeframe required by the CCPA and will provide insight into whether consumers are receiving timely responses.

Second, the metrics will assist in determining whether consumer requests are systematically being denied, which is a potential flag that a business may be thwarting consumers' rights. If requests are routinely denied, it could indicate that the business's notices and/or methods for submitting requests are difficult to understand or unnecessarily complicated, which could violate these regulations.

Third, reporting of the metrics will provide transparency regarding the number of CCPA requests received by businesses and their responses to those requests. The CCPA has garnered a significant amount of academic, industry, and public attention, and public disclosure of the metrics will enable academics, consumer advocates, business groups, and others to research and analyze this data. Based on the OAG's experience with other California laws, particularly privacy laws, this type of research and analysis will benefit both consumers and businesses by providing useful information that may be leveraged to improve consumers' ability to exercise their rights and businesses' compliance with the CCPA, including by assisting the OAG in its enforcement efforts. For example, as the primary enforcer of California's statutes related to breach notification and security of personal information (Civ. Code, §§ 17981.81.5, 1798.82),

the OAG has received numerous requests from academics and others for information about data breaches so that they can conduct research that ultimately benefits consumers and businesses; the OAG is also aware of other reports that analyze public information about data breaches and that may help businesses to improve their own practices. Subsection (g) facilitates such analyses and insights regarding CCPA requests and responses, including on the effectiveness and impact of the CCPA and these regulations, trends and developments regarding requests and compliance, how businesses can effectively and efficiently comply with statutory and regulatory requirements, and other related issues. They will also assist the OAG, which has exclusive enforcement authority over most of the CCPA's provisions, to learn of potential violations and compliance trends.

Finally, the metrics benefit consumers and businesses by assisting the OAG and other entities in determining whether consumer education regarding CCPA rights and requests are needed and by assisting the Legislature and the OAG in determining whether statutory or regulatory amendments are warranted. A large number of request denials may indicate that consumers do not adequately understand their CCPA rights or how to submit requests, signaling the need for consumer education, which will benefit both consumers and businesses by reducing the number of invalid or deficient requests. Metrics regarding response times, denials, and other information may also indicate that the statutory or regulatory requirements may be insufficient, overly burdensome, or otherwise should be amended.

M. 11 CCR § 999.318. Requests to Access or Delete Household Information

Subsection (a) has been modified significantly in both its structure and substance. It now states that if a household does not have a password-protected account with a business, the business shall not comply with a request to know or request to delete household information unless the conditions in **subsections (a)(1), (a)(2), and (a)(3)** are met. Syntactical and word changes have been made to make the regulation more readable and to more clearly communicate the requirements for businesses. For example, subsection (a) has been revised to specifically apply to requests to know “specific pieces of personal information about the household” and requests to delete “household personal information” to clarify that this regulation only applies to specific requests regarding household information. Substantive changes are explained below.

Subsections (a)(1) and (a)(2) include language that was part of former subsection (b) and are necessary for the reasons set forth in the ISOR. (See ISOR, p. 29.) **Subsection (a)(1)** requires that all consumers of the household jointly make the request to know or the request to delete, and **subsection (a)(2)** requires the business to individually verify all the members of the household subject to the verification requirements set forth in section 999.325. Subsection (a)(2) refers to section 999.325, instead of more generally to Article 4, because section 999.325 specifically pertains to non-password-protected accounts. **Subsection (a)(3)** has been added to require the business to verify that each consumer making the request is currently a member of the household.

These requirements are necessary to address public comments that household requests implicate privacy concerns of household members who may not want their personal information revealed

to others in response to a household request to know or may not want their personal information deleted in response to a household request to delete. Subsection (a)(1) directly addresses this concern by requiring that all members of the household consent to a household request. This prevents household requests from being improperly used to undermine the control any individual household member has over their data. Subsection (a)(2) is necessary to conform verification procedures for household requests to that of individual consumer requests. To promote security and best practices, verification procedures for household requests should not be weaker than those used for individual requests. Lastly, subsection (a)(3) is necessary to minimize the risk of fraudulent requests from persons who are not currently part of a household and are trying to obtain a household's personal information without authorization. Overall, these three subsections benefit businesses by providing guidance about how to review and verify household requests, and they benefit consumers by providing safeguards against the disclosure or deletion of their personal information without their consent.

The initial proposed requirement that businesses provide aggregate household information has been deleted in response to public comments that the term "aggregate household information" was vague. Comments expressed concern that businesses would not know what kinds of "aggregate household information" to include in response to a request. Moreover, one comment noted that the proposed requirement to provide "aggregate household information" did not make sense in the context of a household request to delete because it implied that a business should respond to a request to *delete* by *providing* the requestor "aggregate household information." In light of these concerns, the requirement was deleted.

Subsection (b) has been added to clarify that where a consumer has a password-protected account with a business that collects information about a household, the business may process requests to know and requests to delete relating to household information through the business's existing practices for accessing or deleting information and in compliance with these regulations. This addition was made in response to the CCPA's amendment by AB 1355 (Assem. Bill No. 1355, approved by Governor, Oct. 11, 2019 (2019-2020 Reg. Sess.)) to allow businesses to require the consumer to use their existing account to make consumer requests and in response to public comments seeking clarification on how to handle household requests when the consumer does have a password-protected account with the business. Subsection (b) allows businesses the flexibility to use their existing practices and to prevent any disruption to existing access to household information. For example, if a business that provides video-streaming services already gives the account holder access to information, even if that account includes information that relates to other members of the household using the service, the business does not need to create a separate method for processing household requests. This regulation benefits businesses by alleviating the need to create additional processes for handling household requests, and it benefits consumers because existing practices may provide greater access or control over information than the requirements set forth for non-account holders.

Subsection (c) has been added to specify that a business must obtain verifiable parental consent for members of a household under the age of 13 before complying with a request to know or to delete household information. This modification is necessary to make the subsection consistent

with COPPA and section 999.330, subsection (c), of these regulations, and to provide needed guidance to businesses.

Changes made to Article 4. Verification of Requests:

N. 11 CCR § 999.323. General Rules Regarding Verification

Subsections (b)(2) and (b)(3)(a) have been modified to correct the format of the Civil Code citation.

Subsection (d) has been added to prohibit a business from requiring a consumer to pay a direct or indirect fee for the verification of their request. The CCPA expressly provides that a consumer may exercise the right to know “free of charge.” (Civ. Code, §§ 1798.100, subd. (d), 1798.130, subd. (a)(2).) However, after the CCPA went into effect, some businesses began charging consumers to notarize their requests as the method for verification. Accordingly, this regulation is necessary to prevent businesses from creating fee barriers to consumers exercising their rights under the CCPA, such as by charging for verification. Notarization may be used as a method of verification if the business compensates the consumer for the cost of notarization. This regulation is not intended to require businesses to cover general transaction costs incurred by a consumer, such as the time or cost of filling out a form or making copies of identity documents, or to require a business to reimburse a consumer for the costs of notarization if the business offers alternative verification methods that are free of charge. Rather, it is intended to prevent business practices that subvert the clear mandate that businesses are to disclose and deliver the required information to consumers free of charge.

Former subsection (d) has been renumbered and is now **subsection (e)**.

Former subsection (e) has been renumbered and is now **subsection (f)**. This subsection has been modified to replace “de-identifying” with “deidentifying.” This change is necessary to make the language consistent with the term “deidentified” in the CCPA. (See Civ. Code, § 1798.140, subd. (h).)

O. 11 CCR § 999.325. Verification for Non-Accountholders

Subsection (a) has been modified to replace “the” with “a”, which is a grammatical, non-substantive change. The text “subsections (b) through (g) of” was also deleted as unnecessary because “this section” is sufficient.

Subsection (c) has been modified to clarify that only businesses that choose to verify consumers through a signed declaration under penalty of perjury are required to maintain the signed declaration as part of their record-keeping obligations. The change was made in response to public comments seeking guidance regarding whether the requirement applied only to the conditions of the previous sentence or in all instances. This change is necessary to provide guidance regarding businesses’ record-keeping obligations and to clarify that a business may use different methods to verify the identity of the consumer making a request to know specific pieces of personal information.

Subsection (d) has been modified in two ways. First, the word “only” has been added to the second sentence to emphasize that the deletion of browsing history may require “only” a reasonable degree of certainty. This change is necessary to further delineate the different standards that may apply depending on the sensitivity of the personal information and the risk of harm to the consumer. Second, the phrase “the regulations set forth in Article 4” in the last sentence has been replaced by the phrase “these regulations” because there may be other regulations other than those in Article 4 that impact the verification standard the business applies to requests.

Subsection (e) has been modified to replace the word “scenarios” with “examples” and to use “Example 1” and “Example 2” as headers for **subsections (e)(1) and (e)(2)**. These changes were made for stylistics reasons and to be consistent with language used in other sections of the regulations. (See Section 999.305, subd. (a)(3).)

The example in **subsection (e)(1)** has been modified to illustrate that a retailer that maintains a record of purchases made by a consumer may verify the consumer’s identity to a reasonable degree of certainty by requiring the consumer to identify items recently purchased from the store or the dollar amount of their most recent purchase. This change was made in response to public comments that noted that the premise of the initial proposed example—that a business maintained a record of the consumer’s name and credit card number and could require the consumer to provide the credit card’s security code—was a violation of industry standards prohibiting the retention of credit card security codes.

Subsection (e)(2) has been modified to provide an example illustrating how a business that maintains personal information not associated with a named actual person can verify a consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the non-name identifying information. It provides that a business with a mobile application that collects personal information about the consumer but does not require an account may reasonably verify the consumer by asking them to provide information that only the person using that mobile application would know or by requiring them to respond to a notification sent to their device. The example includes language noting that the business may make its verification determination based on the facts and considering factors set forth in section 999.323, subsection (b)(3). This modification was made to emphasize that determining the appropriate verification standard is fact- and scenario-specific. Indeed, while the method provided in the example may be appropriate in this particular factual circumstance, it may not be the appropriate standard if, for example, the mobile application maintains highly sensitive information that could cause harm if disclosed to an unauthorized person. The modification was made in response to public comments seeking examples and additional guidance on how to verify the identity of a consumer who does not maintain an account with the business.

Subsection (f) has been added to require a business to deny a request to know specific pieces of personal information if it cannot verify the identity of the requestor pursuant to these regulations. This subsection was added in response to comments from businesses expressing confusion on this issue. The subsection is necessary to clarify the responsibilities of a business that cannot

verify the identity of the requestor and to protect consumers from bad actors seeking to access specific pieces of personal information about them.

Former subsection (f) has been renumbered and is now **subsection (g)**. This subsection has been modified in structure to distinguish the requirements for a business's response to a specific requestor from the requirements for the business's response to all consumers. The first sentence now sets forth the business's responsibilities in responding to a consumer for which it has no reasonable method to verify their identity to the degree of certainty required by the regulations. The second sentence has been added to set forth the business's responsibilities if it has no reasonable method by which it can verify any consumer. This change is necessary to clarify the syntax and make the requirements easier to understand. The last sentence of the subsection has also been modified for syntactical, not substantive, reasons to clarify that the method referenced in the sentence is the "reasonable method" that is the subject of the subsection.

P. 11 CCR § 999.326. Authorized Agent

Subsection (a) has been modified to add the phrase "do the following" and **subsection (a)(1)** has been modified to delete the word "and." These changes are necessary to clarify that any of the subsections following—subsections (a)(1), (a)(2), and (a)(3)—are permissible options. The change, which permits a business to require that the consumer take any of the actions set forth in subsections (a)(1) through (a)(3) rather than require the consumer to take both (a)(1) and (a)(2), was made for two reasons. First, it was made in response to the addition of subsection (a)(3), which, as discussed below, allows a business to require the consumer to directly confirm with it that the consumer provided the authorized agent permission to submit the request. If a business does so, it may not be necessary for the business to also provide the authorized agent signed permission as set forth in subsection (a)(1) because, whether pursuant to subsection (a)(1) or subsection (a)(3), a business will have ascertained some form of permission that the authorized agent may make the request. Second, the change was made in response to public comments that requiring all the actions set forth in subsections (a)(1) through (a)(3) would unnecessarily burden consumers' ability to use an authorized agent. As a result of the modification, the business has discretion to determine, based on the factors set forth in Sections 999.323, subsection (b), 999.324, and 999.325 of these regulations, which of the requirements in subsections (a)(1), (a)(2), or (a)(3) are warranted. Subsection (a) has also been modified to replace "the" with "a", which is a grammatical, non-substantive change.

Subsection (a)(1) has been modified to replace "written" with "signed." This change is necessary to incorporate the defined term "signed" from section 999.301, subsection (u), which includes physical and electronic signatures. The change was made in response to public comments seeking clarification on whether permission can be provided electronically. This change benefits consumers by making the permission easier for consumers to provide to the authorized agent.

Subsection (a)(3) has been added to allow a business to require that the consumer directly confirm with it that the consumer provided the authorized agent permission to submit the request. This change was made in response to public comments raising concerns about fraud or

bad actors. By allowing a business to confirm permission with the consumer directly, a business may lessen the potential privacy and security risks of improper access to the consumer's information. As with subsections (a)(1) and (a)(2), a business has discretion to determine whether the action set forth in subsection (a)(3) is warranted based on the factors set forth in sections 999.323, subsection (b), 999.324, and 999.325 of these regulations.

Subsection (c) has been modified to insert the word "authorized" to be consistent with other sections that use the term "authorized agent."

Subsection (d) has been added to require authorized agents to implement and maintain reasonable security procedures and practices to protect the consumer's information. This change was made in response to public comments that raised concerns that authorized agents should also be responsible for protecting the consumer's information. This change is necessary to ensure that a consumer's use of an authorized agent does not put the consumer's personal information at risk, given that the use of an authorized agent is an additional link in the chain transmitting specific pieces of information from the business to the consumer. This change also benefits consumers because it allows them to securely use an authorized agent to exercise the rights the CCPA confers on them.

Subsection (e) has been added to state that an authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purpose other than to fulfill the consumer's requests for verification, or for fraud prevention. This change was made in response to comments that raised concerns that authorized agents should be strictly limited in their ability to use the information they obtain from a consumer. This change is necessary to make clear that authorized agents shall not take advantage of their position or exploit information they obtain from a consumer. This change benefits consumers because it allows them to securely use an authorized agent to exercise the rights the CCPA confers on them.

Changes made to Article 5. Special Rules Regarding Minors:

Q. 11 CCR § 999.330. Minors Under 13 Years of Age

Subsection (a)(1) has been modified in two ways. First, the phrase "collects or maintains" has been replaced with the word "sells." This change is necessary to make the language consistent with the CCPA. (See Civ. Code, § 1798.120, subd. (c).) Second, the phrase "the Children's Online Privacy Protection Act, 15 U.S.C. sections 6501, et seq." has been replaced with the term "COPPA." This change is necessary to make the regulation more readable now that "COPPA" is defined in the regulations. (See Section 999.301, subd. (g).)

Subsection (a)(2) has been modified to add the phrase "but are not limited to." This change is necessary to clarify that the acceptable methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian are not limited to the ones listed in subsection (a)(2). The change provides businesses greater flexibility in determining how to verify the identity of a parent or guardian. This change was made in response to comments questioning whether the list was exclusive, and clarifies that it is not.

Subsection (a)(2)(a) has been modified to add the phrase “physically or electronically.” This change was made in response to a comment seeking guidance on whether the parental consent form can be signed electronically.

Subsection (b) has been modified in three ways. First, the phrase “of this section” has been deleted because it is not necessary. Second, the phrase “at a later date” has been deleted to prevent any misinterpretation that a business could choose any future date to inform a parent or guardian of their right to opt-out on behalf of their child under 13. Though not intended as such, the initial proposed phrasing could be read as modifying when the business informs the parent or guardian rather than when the parent or guardian can opt out. This modification corrects this potential misinterpretation. Third, the phrase “subsections (a) through (f)” has been added because subsections (g) and (h) of section 999.315 are not applicable for children.

Subsection (c) has been added to require a business to establish, document, and comply with a reasonable method, in accordance with the methods set forth in subsection (a)(2), for determining that a person submitting a request to know or a request to delete on behalf of a child under the age of 13 is the parent or guardian of that child. This addition is necessary because the CCPA does not specify how a business should determine that the person submitting a request to know or request to delete is the parent or guardian of the child. This regulation clarifies that it is the business’s responsibility to establish and comply with a reasonable method for doing so and uses language consistent with other sections of the regulations. (See Section 999.323, subd. (a).) This subsection is also necessary to clarify that authorized agents may not submit a request to know or a request to delete the personal information of a child under the age of 13, as this would be inconsistent with COPPA. Requiring documentation of the method also provides transparency regarding the method established and a means to confirm that the business has established and is complying with a reasonable method.

R. 11 CCR § 999.331. Minors 13 to 16 Years of Age

Subsection (a) has been modified to replace the phrase “collects or maintains” with the word “sells.” This change is necessary to make the language in the regulation consistent with the CCPA. (See Civ. Code, § 1798.120, subd. (c).)

S. 11 CCR § 999.332. Notices to Minors Under 16 Years of Age

Subsection (a) has been modified to correct a grammatical error.

Changes made to Article 6. Non-Discrimination:

T. 11 CCR § 999.336. Discriminatory Practices

The first sentence of **subsection (b)** has been modified in several ways. The phrase “Notwithstanding subsection (a) of this section” has been deleted to make the subsection more readable and understandable to consumers and businesses. The phrase “as that term is defined in section 999.337” has been deleted as unnecessary and superfluous because the regulations have been modified to define the term “value of the consumer’s data” in the definitions section of the regulations. (See Section 999.301, subd. (w).) Finally, the phrase “a financial incentive” was

added to clarify that businesses may offer financial incentives that are reasonably related to the value of the consumer's data as permitted by the CCPA. (See Civ. Code, § 1798.125.)

Subsection (b) has been further modified to add a new second sentence: "If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference." This addition was made in response to comments that raised concerns regarding the difficulty of estimating the value of the consumer's data. Some businesses contended that it may be impossible to estimate the value of the consumer's data and suggested that this problem be resolved by removing the requirement that businesses offering financial incentives or price or service differences disclose the value of the consumer's data. The OAG disagrees with the assumption by commenters that a business may still offer a financial incentive or price or service difference, even if unable to estimate the value of the consumer's data. Civil Code section 1798.125 expressly provides that a business may only offer a price or service difference or a financial incentive related to the collection, retention, or sale of personal information if it is "reasonably related to the value provided to the business by the consumer's data." Thus, the modification makes clear that, if a business offers a financial incentive or price or service difference, it must do so on the basis that such financial incentive or price or service difference is reasonably related to the value of the consumer's data. If no such basis exists, the business cannot offer the financial incentive or price or service difference.

Former subsections (c) and (d) have been reordered. Former subsection (c) has been renumbered and is now **subsection (d)**, and former subsection (d) has been renumbered and is now **subsection (c)**. The switch in order is necessary to improve the readability of these regulations. The substance of **subsection (c)**, formerly subsection (d), has not been modified.

Renumbered **subsection (d)** contains several new examples to further clarify the application of these anti-discrimination regulations. **Subsection (d)(1)** has been modified to correct certain typographical errors. Hyphens have been added to the phrase "\$5-per-month" and removed from the phrase "opt out." In the first line, the subsection has been modified to replace the word "and" with the phrase "as well as." These changes are necessary to make the example more readable for the benefit of both businesses and consumers. **Subsection (d)(2)** has been deleted in its entirety and replaced with a new example. This change was made in response to comments that raised concerns that the initial proposed example was confusing and unhelpful. **Subsections (d)(3)** and **(d)(4)** set forth new examples and have been included in response to comments requesting additional guidance regarding the anti-discrimination regulations. These examples benefit businesses by demonstrating how a business may offer a financial incentive or price or service difference while remaining in compliance with the CCPA and these regulations.

Subsection (f) has been modified to correct the format of the Civil Code citation and to correct the cite to Civil Code section 1798.145, subdivision (i)(3), because it was renumbered after the CCPA's amendment by AB 1355 (Assem. Bill No. 1355, approved by Governor, Oct. 11, 2019 (2019-2020 Reg. Sess.)).

Subsection (g) has been added to state that “[a] price or service difference that is the direct result of compliance with a state or federal law shall not be considered discriminatory.” This addition was made in response to concerns raised in comments that compliance with certain state or federal laws, including COPPA, could directly cause businesses to engage in practices that would otherwise violate the provisions of this section. The change is necessary to address this concern.

U. 11 CCR § 999.337. Calculating the Value of Consumer Data

Subsection (a) has been deleted because it is no longer necessary in light of the CCPA’s amendment by AB 1355 (Assem. Bill No. 1355, approved by Governor, Oct. 11, 2019 (2019-2020 Reg. Sess.)) that the value of the consumer’s data is the value of that data “to the business” (Civ. Code, § 1798.125).

Former subsection (b) has been renumbered and is now **subsection (a)**. **Subsection (a)** has been modified to replace the word “use” with “consider.” This change is necessary because the word “consider” more correctly describes how businesses should rely on the factors that follow. Several of the numbered factors would not alone constitute a method for calculating the value of the consumer’s data; thus, they should be “considered” when developing such a calculation rather than “used” for the calculation.

Subsections (a)(1) and **(a)(2)** have been modified to delete the phrase “or a typical consumer’s data” in response to public comments that the phrase was confusing. As used in the initial proposed regulations, the term “typical consumer’s data” referred to the data of any natural person residing in the United States and was included to permit businesses to use the value of such data if it was difficult or impossible to separate out the value of data from California residents. To address this concern, the OAG has instead added subsection (b), addressed below. Businesses will benefit from the increased clarity provided by this change.

Former subsection (a)(3) has been deleted in response to concerns that vulnerable consumers may be harmed if businesses calculate the value of the consumer’s data on the basis of “separate tiers, categories, or classes of consumers.” Deletion of this subsection will benefit consumers and businesses by removing the option to treat various groups of consumers differently while maintaining the flexibility for businesses to use “[a]ny other practical and reasonably reliable method of calculation used in good-faith,” as provided in subsection (b)(8).

New subsection (a)(3) has been added to include “[t]he aggregate value to the business of the sale, collection, or deletion of consumers’ data divided by the total number of consumers” as a method for businesses to consider in calculating the value of the consumer’s data. This was added in response to businesses’ concerns that they would be unable to estimate the value of the consumer’s data because certain businesses only know the value of consumers’ data in the aggregate. Subsection (a)(3) now explicitly provides a method for businesses that value data in the aggregate to calculate the value for a single consumer.

Subsection (a)(8) has been modified to add the word “reasonably” before the phrase “reliable method of calculation.” This change was made in response to comments concerned that the

phrase “reliable method of calculation,” without further modification, implied a level of certainty regarding how to calculate the value of a consumer’s data that they contended does not currently exist in many industries. The addition of “reasonably” is necessary to avoid this implication.

Subsection (b) has been added and states that “[f]or the purpose of calculating the value of consumer data, a business may consider the value to the business of the data of all natural persons in the United States and not just consumers.” The initial proposed regulation likewise permitted businesses to consider the value to the business of data from all natural persons in the United States, rather than only California consumers; however, the initial proposed regulation achieved this by defining “typical consumer” as “a natural person residing in the United States” and then permitted consideration of the value of the “typical consumer’s data” in the factors now provided in subsection (a). Comments in response to the initial draft of the regulations indicated that the initial formulation was confusing, and thus, the OAG added subsection (b) to state this concept more explicitly. Businesses will benefit from this more straightforward description.

SUMMARY OF COMMENTS AND DEPARTMENT RESPONSES

The OAG received 209 comment letters during the 45-day comment period, 99 comment letters during the first 15-day comment period, and 68 comment letters during the second 15-day comment period. The summary of the comments and the OAG’s responses are attached as the following appendices.

- Appendix A. Summary and Response to Comments Submitted during 45-Day Period
- Appendix B. List of Commenters from 45-Day Period
- Appendix C. Summary and Response to Comments Submitted during 1st 15-Day Period
- Appendix D. List of Commenters from 1st 15-Day Period
- Appendix E. Summary and Response to Comments Submitted during 2nd 15-Day Period
- Appendix F. List of Commenters from 2nd 15-Day Period

For ease of reference, the OAG assigned a number to each written and oral comment submission received. Because most comment letters contained multiple substantive comments that needed to be addressed, for each substantive comment, the OAG assigned subnumbers to the comment submission number. The OAG also added a prefix to denote whether the submission was a written or oral comment—“W” for written and “O” for oral. For oral comments, the “O” is followed by an abbreviation for the location of the hearing. Specifically, “OSac” refers to the Sacramento hearing, “OLA” refers to the Los Angeles hearing, “OSF” refers to the San Francisco hearing, and “OFres” refers to the Fresno hearing. Accordingly, in the OAG’s summary and response to comments, the comment number “W15-3” refers to the third substantive comment included in the 15th written comment received, and “OLA14-1” refers to the first substantive point of the 14th commenter at the Los Angeles public hearing.

The “Summary and Response to Comments” is organized according to the chronological order of the proposed regulations that they address. Comments relating to multiple sections of the regulations are grouped together at the beginning of each Article number. Comments generally about the regulations, but not regarding a particular section or subsection of the regulations, are grouped together at the end under the heading of “Other.” Subheadings have been included where comments are related to similar topics. Page numbers and transcript references have also been included for ease of reference.

The “List of Commenters” identifies the person and/or entity that submitted the comment during a particular comment period and provides the response number(s) that correspond(s) to the commenter’s substantive point(s). It is essentially an index that assists the commenter in locating the OAG’s response to their comment, given the extensive number of substantive comments received. In some instances, the commenter’s substantive point may have been responded to by multiple response numbers.

LOCAL MANDATE DETERMINATION

The proposed regulations do not impose any mandate on local agencies or school districts.

ALTERNATIVES DETERMINATIONS

In accordance with Government Code section 11346.9, subdivision (a)(4), the OAG has determined that no reasonable alternative it considered or that has otherwise been identified and brought to its attention would be more effective in carrying out the purpose for which the action is proposed, or would be as effective and less burdensome to affected private persons than the proposed action, or would be more cost-effective to affected private persons than the proposed action, or would be more cost-effective to affected private persons and equally effective in implementing the statutory policy or other provision of law.

The OAG considered two alternative approaches to the regulations, described in the SRIA and presented below, and determined that they would as effective but more burdensome on businesses, or less burdensome on businesses but less effective in carrying out the purposes for which the regulations are proposed. (SRIA, p. 42.)

More stringent regulatory requirement. A more stringent regulatory alternative considers mandating more prescriptive compliance requirements, including detailed training programs and record-keeping practices for all businesses subject to the CCPA. This requirement would be an additional requirement (beyond the proposed regulations) for potentially hundreds of thousands of California businesses and would impose substantial costs. Even though this approach may be as effective in implementing the CCPA, the OAG rejects this regulatory alternative in order to ease the compliance burden for smaller businesses subject to the CCPA that do not necessarily have the resources to devote additional staff to handle CCPA related tasks.

Less stringent regulatory requirement. A less stringent regulatory alternative would, among other things, allow a limited exemption for GDPR-compliant firms. Limitations would be specific to areas where GDPR and CCPA conform in both standards and enforcement, subject to auditing as needed. This approach could achieve significant economies of scale in both private compliance and public regulatory costs. The OAG rejects this regulatory alternative because of key differences between the GDPR and CCPA, especially in terms of how personal information is defined and the consumer's right to opt-out of the sale of personal information (which is not required in the GDPR). Even though this approach may be less burdensome to businesses, it would be less effective in carrying out the purposes of the CCPA.

The final regulations represent a balanced approach that seeks to lessen the incremental costs to comply with the regulations while still protecting consumers by providing them with tools to control how businesses use and sell their personal information.

ALTERNATIVES THAT WOULD LESSEN ADVERSE ECONOMIC IMPACT ON SMALL BUSINESSES

The OAG considered several alternatives in drafting the proposed regulations. In considering the following alternatives, the OAG sought to balance the benefits to consumers, the burden to businesses, and the purposes of the CCPA. The alternatives considered and rejected are below.

Section 999.301, subds. (d) and (e):

The OAG considered and rejected alternative approaches to the definitions for “categories of sources” and “categories of third parties.” One included a hands-off approach that left the terms undefined. But leaving the terms undefined would likely result in vague and confusing language in privacy policies and less protection for the consumer. Moreover, the OAG does not agree that undefined terms would be less burdensome on small businesses given that some businesses requested definitions for these terms to better understand their compliance obligations.

Sections 999.305, subd. (a)(2)(d), 999.306, subd. (a)(2)(d), 999.307, subd. (a)(2)(d), 999.308, subd. (a)(2)(d):

The OAG considered and rejected the alternative of deleting the requirement to comply with the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium. This alternative is not as effective in providing meaningful notice to consumers about their privacy rights. The CCPA requires that the notice be accessible to consumers with disabilities. (Civ. Code, § 1798.185, subd. (a)(6).) The regulations limit the burdens on business by only requiring them to follow an already recognized industry standard, which reduces the burden on business in complying with a mandated standard that may be novel or not widely adopted. Further, as described in the SRIA, the costs to businesses to comply with notice requirements are attributable to the CCPA rather than the regulation. (SRIA, p. 17.)

Section 999.305, subd. (a)(4):

The OAG considered and rejected the alternative of deleting the requirements to provide a just-in-time notice for mobile devices that collect personal information that the consumer would not reasonably expect to be collected. This alternative is not as effective in providing meaningful notice at collection of the categories of personal information collected about them. The regulation is necessary to make notices more conspicuous when a consumer's personal information is being collected for purposes not reasonably expected.

Section 999.305, subd. (a)(5):

The OAG considered and rejected the alternative of allowing businesses to post an updated online notice at collection, instead of requiring them to obtain explicit consent from a consumer, when a business uses a consumer's information for purposes materially different than what was disclosed in the notice at collection. This alternative is not as effective in providing meaningful notice to consumers about their privacy rights and may incentivize businesses to minimize or delay updating notices of new or more controversial uses. Further, as described in the SRIA, the costs to businesses to comply with notice requirements are attributable to the CCPA rather than the regulation. (SRIA, p. 17.)

Section 999.306, subd. (e):

The OAG considered the alternative of allowing a subsequently posted notice of right to opt-out to apply retroactively instead of requiring businesses to obtain affirmative authorization from consumers to sell personal information collected during the time when a notice of right to opt-out was not posted. This alternative is not as effective in informing consumers of their right to opt-out at the point of collection, when consumers are likely to be most aware of what personal information the business is collecting from them.

Section 999.307, subd. (b):

The OAG considered and rejected the alternative of eliminating businesses' obligation to provide a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference in the Notice of Financial Incentive. Businesses offering financial incentives must provide the consumer with "the material terms of the financial incentive program" before the consumer opts in to the financial incentive program. The OAG considers the value of the consumer's data to be a material term of any financial incentive program because any financial incentive or price or service difference must be "reasonably related" to the value of the consumer's data. (Civ. Code, § 1798.125, subds. (a) & (b).) To lessen the burden on businesses, the regulation only requires that the estimate be made in good faith and it gives business the discretion to determine which method of calculation is best suited to its circumstances. (ISOR, p. 28.)

Section 999.308, subd. (c)(6):

The OAG considered and rejected the alternative of eliminating the requirement to list in the business's privacy policy a contact for questions or concerns about the business's privacy

policies and practices. This alternative is not as effective in providing meaningful notice to consumers about their rights under the CCPA and how to exercise those rights. (Civ. Code, § 1798.130, subd. (a)(6).)

Section 999.313, subd. (c)(3):

The OAG considered and rejected alternative conditions that would allow more businesses to avoid searching for personal information not maintained in a searchable or reasonably accessible format in response to a request to know. Though the alternatives would lessen the burden on businesses, they would too easily allow a business to evade its obligations under the CCPA and could incentivize behavior that would undermine a consumer's ability to exercise their CCPA right to know what personal information the business has collected about them. (Civ. Code, § 1798.110.)

Section 999.313, subd. (c)(9):

The OAG considered and rejected the alternative of allowing businesses to send consumers information about their general business practices rather than an individualized response in response to a request to know categories of personal information, categories of sources, and/or categories of third parties. This alternative is not as effective in complying with the intent of the CCPA to inform consumers about the personal information businesses have collected about them. (Civ. Code, § 1798.110.)

Section 999.313, subd. (d)(4):

The OAG considered and rejected the alternative of not requiring businesses to inform the consumer whether or not it has complied with the consumer's request. This alternative is not as effective in allowing consumers to exercise their right to delete. (Civ. Code, § 1798.105.) Consumers need the ability to confirm that the business received and acted upon the request or, in the event that the business denied the request, allowing the consumer to follow up or remedy any deficiencies resulting in the denial.

Section 999.313, subd. (d)(6):

The OAG considered and rejected the alternative of not requiring businesses to inform the consumer of the reason for why the consumer's request to delete was denied (although the modified regulation provides for situations in which a business would be prohibited from disclosing the reason by law). This alternative is not as effective in allowing consumers to exercise their right to delete. (Civ. Code, § 1798.105.) A meaningful right to delete should give consumers the opportunity to understand why a request has been denied, and to follow up or remedy any deficiencies resulting in the denial.

Section 999.313, subd. (d)(7):

The OAG considered and rejected the alternative of not requiring businesses to ask consumers who have had their right to delete denied whether they would like to opt-out of the sale of their personal information, if those businesses sell personal information. This alternative is not as effective in allowing consumers to exercise their rights under the CCPA. Requiring the business

to ask the consumer whether they would like to opt-out of the sale of their personal information when the business denies their request to delete provides the consumer with the ability to prevent the proliferation of their personal information in the marketplace. Moreover, this regulation lessens the burden on the business by simply requiring that the business direct the consumer to how they can opt-out of the sale of their personal information and not requiring them to treat the denial as a request to opt-out.

Section 999.314, subd. (c):

The OAG considered and rejected additional uses of personal information allowed for service providers under this regulation. Though the additional uses may lessen the burden on service providers, they may functionally operate to make personal information available to multiple businesses and effectively usurp the consumer's right to prevent the sale of their personal information. (Civ. Code, § 1798.120.)

Section 999.315, subd. (d):

The OAG considered and rejected the alternative of leveraging a business's designated methods for submitting requests to know and requests to delete for submitting requests to opt-out. However, this alternative is insufficient because it would not be an effective method to counterbalance the ease and frequency by which personal information is collected and sold in online contexts, such as when a consumer visits a website. Also, because requests to opt-out do not need to be verified, unlike requests to know and to delete, using a procedure that requires verifiable requests would place a barrier on the consumer's exercise of the right to opt-out, which would be contrary to the CCPA.

The OAG considered and rejected the alternative of eliminating a consumer's use of user-enabled global privacy controls as a mechanism to signal the consumer's choice to opt-out. The regulation is necessary to provide a global mechanism for consumers to use, as opposed to going website by website to opt out of sale. It will also drive innovation for privacy services that facilitate the exercise of consumer rights in furtherance of the purposes of the CCPA. If made discretionary, businesses are likely to reject or ignore tools that empower consumers to effectuate their opt-out right, such as by refusing to recognize the privacy control. To lessen the burden on businesses, the regulation requires that user-enabled privacy controls must clearly communicate a consumer's intent to opt-out of sale.

Section 999.315, subd. (e):

The OAG considered and rejected the alternative of eliminating the business's requirement to direct third parties to which it sold the consumer's personal information after receiving the consumer's request to opt-out but before complying with it that the third party should not sell the consumer's information. This alternative is not as effective in allowing consumers to exercise their right to opt-out because it would allow the further proliferation of the consumer's information during the 15 business days that the business has to comply with the request.

Section 999.323, subd. (d):

The OAG considered and rejected the alternative of eliminating the prohibition of fees for the verification of requests to know and requests to delete. This alternative is not as effective in allowing consumers to exercise their right to know and right to delete because it would allow businesses to create fee barriers for consumers exercising their rights under the CCPA.

Section 999.326:

The OAG considered and rejected the proposal that the regulations limit the ability of authorized agents to act on behalf of a consumer. The OAG believes this proposal would impermissibly narrow the scope of the statute, which authorizes consumers to use authorized agents under the CCPA.

DOCUMENT INCORPORATED BY REFERENCE

The following document is incorporated in the regulations by reference: World Wide Web Consortium, *Web Content Accessibility Guidelines (WCAG) 2.1* (June 5, 2018) <<https://www.w3.org/TR/WCAG21/>> [as of May 21, 2020].

The document is incorporated by reference because it would be cumbersome, unduly expensive, or otherwise impractical to publish the document in the California Code of Regulations. During the rulemaking proceeding, the document was made available upon request and was available for viewing on the OAG's website.

NON-DUPLICATION

Some of the regulations may repeat or rephrase in whole or in part a state or federal statute or regulation. This was necessary to satisfy the clarity standard set forth in Government Code section 11349.1, subdivision (a)(3).