CALIFORNIA PRIVACY PROTECTION AGENCY

TITLE 11. LAW
DIVISION 6. CALIFORNIA PRIVACY PROTECTION AGENCY
CHAPTER 1. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

INITIAL STATEMENT OF REASONS

PROBLEM STATEMENT

In November 2020, voters approved the Consumer Privacy Rights Act of 2020 (CPRA), amending and building on the California Consumer Privacy Act of 2018 (CCPA). The CPRA established a new agency, the California Privacy Protection Agency (Agency), to implement and enforce the CCPA. (Civ. Code, § 1798.199.10.)[1] The Agency is directed to adopt regulations to further the purposes of the Act, including promulgating regulations on 22 specific topics. (§ 1798.185.) The proposed regulations operationalize the CPRA amendments to the CCPA and provide clarity and specificity to implement the law.

The proposed regulations:

- Establish rules defining the notified purposes for which a business can collect, use, retain, and share consumer personal information consistent with consumers' expectations. (§ 1798.185, subd. (a)(10).)

- Establish rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide under the CCPA are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer. (§ 1798.185, subd. (a)(6).)

- Establish rules and procedures to facilitate and govern the submission of a consumer's request to opt-out of sale/sharing and request to limit and a business's compliance with the request, to ensure that consumers have the ability to exercise their choices without undue burden and to prevent businesses from engaging in deceptive or harassing conduct, including in retaliation against consumers for exercising their rights, while allowing businesses to inform consumers of the consequences of their decision. (§ 1798.185, subd. (a)(4).)

- Establish rules and procedures to facilitate a consumer's right to delete, correct, or obtain personal information. (§ 1798.185, subd. (a)(7).)

- Establish rules on how often and under what circumstances a consumer can request a correction; how a business responds to the request; how concerns regarding accuracy are

[1] All references are to the Civil Code unless otherwise indicated.

resolved; the steps taken to prevent fraud; and the right to submit an addendum when a request to correct health information has been rejected. (§ 1798.185, subd. (a)(8).)

- Establish procedures to extend the 12-month period of disclosure of information after a verifiable consumer request pursuant to section 1798.130, subdivision (a)(2)(B). (§ 1798.185, subd. (a)(9).)

- Define the requirements and specifications for an opt-out preference signal. (§ 1798.185, subd. (a)(19)(A) & (B).)

- Establish regulations governing how businesses respond to an opt-out preference signal where the business has elected to comply with section 1798.135, subdivision (b). (§ 1798.185, subd. (a)(20).)

- Establish regulations governing the use or disclosure of a consumer's sensitive personal information. (§ 1798.185, subd. (a)(19)(C).)

- Further define and add to the business purposes for which businesses, service providers, and contractors may use personal information consistent with consumer expectations, and further define the business purposes for which service providers and contractors may combine personal information. (§ 1798.185, subd. (a)(10).)

- Identify the business purposes for which service providers and contractors may use consumers' personal information pursuant to a written contract with a business, for the service provider or contractor's own business purpose. (§ 1798.185, subd. (a)(11).

- Establish procedures for filing complaints with the Agency (§ 1798.199.45) and procedures necessary for the Agency's administrative enforcement of the CPRA. (§ 1798.199.50).

- Define the scope and process for the exercise of the Agency's audit authority as well as the criteria for selecting those that would be subject to an audit. (§ 1798.185, subd. (a)(18).)

- Harmonize regulations governing opt-out mechanisms, notices, and other operational mechanisms to promote clarity and functionality. (§ 1798.185, subd. (a)(22).)

BENEFITS ANTICIPATED FROM REGULATORY ACTION

The proposed regulations provide a number of significant benefits to Californians. Building off of the existing CCPA regulations, the proposed regulations provide comprehensive guidance to consumers, businesses, service providers, and third parties, on how to implement and operationalize new consumer privacy rights and other changes to the law introduced by the CPRA amendments to the CCPA. (Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3(C)(2).) They set forth clear requirements for how businesses are to craft their methods for submitting consumer requests and obtaining consumer consent so that the consumer's choice is freely made and not manipulated, subverted, or impaired through the use of dark patterns. (*Ibid.*)

They also clearly explain that the CPRA amendments now restrict businesses from collecting, using, retaining, and sharing consumer personal information in a manner that is inconsistent with consumer expectations, unless they obtain the consumer's explicit consent. In doing so, the regulations place the consumer in a position where they can knowingly and freely negotiate with a business over the business's use of the consumer's personal information. (*Id.* at § 3(C)(3).)

In addition, the proposed regulations set forth the requirements for an opt-out preference signal that consumers may use to easily opt-out of the sale or sharing of their personal information with all businesses that they interact with online. With the goal of strengthening consumer privacy, the regulations support innovation in pro-consumer and privacy-aware products and services and help businesses efficiently implement privacy-aware goods and services. (*Id.* at § 3(C)(1) & (5).) They take into consideration how privacy rights are being implemented in the marketplace presently and build upon the development of privacy-forward products and services.

Finally, the proposed regulations take into consideration privacy laws in other jurisdictions and implement compliance with the CCPA in such a way that it would not contravene a business's compliance with other privacy laws, such as the General Data Protection Regulation (GDPR) in Europe and consumer privacy laws recently passed in Colorado, Virginia, Connecticut, and Utah. In doing so, it simplifies compliance for businesses operating across jurisdictions and avoids unnecessary confusion for consumers who may not understand which laws apply to them.

SPECIFIC PURPOSE AND NECESSITY OF EACH SECTION

§ 7000. Title and Scope.

Changes without regulatory effect. Authority and reference citations have been amended.

§ 7001. Definitions.

This section defines terms used throughout this Chapter. It is necessary to define these terms because many of them could have multiple meanings depending on the context of their usage. Furthermore, some of the terms are used in the CCPA without being defined. Defining the terms clarifies the meaning of the regulations and helps eliminate any misunderstandings or confusion. It assists businesses in implementing the law, as well as the regulations, and thereby increases the likelihood that consumers will enjoy the benefits of the rights provided them by the CCPA.

Deletion of existing subsection (a). The definition of "affirmative authorization" has been deleted because Civil Code section 1798.140, subdivision (h), now defines "consent." This change is necessary to make the regulations consistent with the amended language of the CCPA.

Subsection (a) establishes that "Agency" means the California Privacy Protection Agency created by Civil Code section 1798.199.10 *et seq*. The purpose of defining this term is to provide clarity to the regulations and to make them more readable, and thus, easier for consumers and businesses to understand. The definition is necessary to clearly identify the California Privacy Protection Agency and avoid any confusion given that there are many different state agencies in California.

Subsection (c) is revised to delete "registered with the Secretary of State to conduct business in California." This change is necessary because businesses have misinterpreted this language to mean that there is a special registry with the Attorney General's Office for authorized agents. This is not the case. Removing the language clears up the confusion.

Subsection (h) establishes what "disproportionate effort" means within the context of responding to a consumer request. This definition is necessary because Civil Code sections 1798.105, subdivision (c)(1), 1798.130, subdivision (a)(2)(B), and 1798.185, subdivision (a)(9), provide an exception to meeting certain obligations in response to a request to delete, request to correct, and request to know when doing so involves "disproportionate effort" and the public has asked the Agency for guidance on what this means during preliminary rulemaking activities. Defining this term clarifies when a business, service provider, or contractor can use this exception, and also prevents them from abusing this exception by claiming that everything requires "disproportionate effort" on their part.

Deletion of existing subsection (k). The definition of "household" has been deleted because Civil Code section 1798.140, subdivision (q), now defines "household." This change is necessary to make the regulations consistent with the CCPA as amended.

Subsection (k) revises the definition of "financial incentive" to align the regulation with the amended language of the statute. The subsection also includes that price or service differences are a type of financial incentive. This language is necessary to clarify that a price or service difference also requires a notice of financial incentive.

Subsection (l) establishes that "first party" means the consumer-facing business with which a consumer would reasonably expect to interact. The purpose of defining this term is to provide clarity to the regulations, as the CCPA and the regulations cover various parties with different types of relationship to the consumer and to each other. The use of the shortened phrase "first party" also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (m) establishes that "frictionless manner" means a business's response to an opt-out preference signal that complies with the requirements set forth in section 7025, subsection (f). The purpose of defining this term is to provide clarity to the regulations. The use of the shortened phrase "frictionless manner" also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (o) establishes that "notice of right to limit" means the notice given by a business informing consumers of their right to limit the use of the consumer's sensitive personal information as required by Civil Code sections 1798.121 and 1798.135 and specified in these regulations. The purpose of defining this term is to provide clarity and guidance on one of the disclosures required by the CCPA and specified in these regulations. The definition is intended to help businesses implement the regulations by giving a name to the notice required by Civil Code section 1798.121, subdivision (a), regarding the right to limit the use and disclosure of sensitive personal information. This definition clearly distinguishes the notice of right to limit from other notices required by the CCPA and assists businesses with making the notice easily understandable and accessible to consumers, as required by Civil Code section 1798.185,

subdivision (a)(6). It also makes these regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (p) revises "notice of right to opt-out" to add "of sale/sharing" to align the regulation with amendments to the statute that added "sharing." Adding "sale/sharing" is also necessary because Civil Code section 1798.185, subdivision (a)(16), introduces opt-out rights with respect to businesses' use of automated decisionmaking technology. Without specifying that the notice of right to opt-out refers to sale and sharing, consumers and businesses may be confused and think that it pertains to automated decisionmaking technology.

Subsection (r) establishes that "opt-out preference signal" means a signal that is sent by a platform, technology, or mechanism, on behalf of the consumer, that clearly communicates the consumer choice to opt-out of the sale and sharing of personal information and that complies with the requirements set forth in section 7025, subsection (b). The purpose of defining this term is to provide clarity to the regulations. The use of the shortened phrase "opt-out preference signal" also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (s) has been revised to add "or sharing" to align the regulation with the amended language of the statute. The phrase "including through the use of discounts, financial payments, or other benefits or penalties" has also been deleted to clarify that financial payments may not be a price or service difference. For example, a business could provide a financial incentive in the form of a gift card to a consumer in exchange for filling out a survey that includes the consumer's personal information. That financial payment would not be a price or service difference, though it may be a financial incentive. This revision is necessary to help businesses and consumers understand the relationship between financial incentives and price or service differences, especially in the way that they relate to CCPA's provisions on non-discrimination in Civil Code section 1798.125.

Subsection (u) establishes that "request to correct" means a consumer request that a business correct inaccurate personal information that it maintains about the consumer, pursuant to Civil Code section 1798.106. The purpose of defining this term is to provide clarity to the regulations. The use of the shortened phrase "request to correct" also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (w) has been revised to delete the reference to Civil Code, section 1798.100. This change is necessary to make the regulations consistent with the amended language of the CCPA.

Subsection (x) establishes that "request to limit" means a consumer request that the business limit the use and disclosure of a consumer's sensitive personal information, pursuant to Civil Code section 1798.121. The purpose of defining this term is to provide clarity to the regulations. The use of the shortened phrase "request to limit" also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (y) has been revised to add "to sale/sharing" and replace "affirmative authorization" with "an action demonstrating that the consumer has consented to the business's sale or sharing." The addition of "to sale/sharing" is necessary to align the regulation with the amended language

of the statute, and because Civil Code section 1798.185, subdivision (a)(16), introduces opt-out rights with respect to businesses' use of automated decisionmaking technology. Without specifying that the request to opt-in refers to sale and sharing, consumers and businesses may be confused and think that it pertains to automated decisionmaking technology. Replacing "affirmative authorization" is also necessary because Civil Code section 1798.140, subdivision (h), now defines "consent." This change is necessary to make the regulations consistent with the amended language of the CCPA.

Subsection (z) has been revised to add "of sale/sharing" and to include that the request refers to both sale and sharing to align the regulation with the amended language of the statute. The revision is also necessary because Civil Code section 1798.185, subdivision (a)(16), introduces opt-out rights with respect to businesses' use of automated decisionmaking technology. Without specifying that the request to opt-out refers to sale and sharing, consumers and businesses may be confused and think that it pertains to automated decisionmaking technology.

Subsection (aa) establishes that "right to correct" means the consumer's right to request a business to correct inaccurate personal information that it maintains about the consumer as set forth in Civil Code section 1798.106. The purpose of defining this term is to provide clarity to the regulations. The use of the shortened phrase "right to correct" also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (bb) establishes that "right to delete" means the consumer's right to request that a business delete personal information about the consumer that the business has collected from the consumer as set forth in Civil Code section 1798.105. The purpose of defining this term is to provide clarity to the regulations. The use of the shortened phrase "right to delete" also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (cc) establishes that "right to know" means the consumer's right to request that a business disclose personal information that it has collected, sold, or shared about the consumer as set forth in Civil Code sections 1798.110 and 1798.115. The purpose of defining this term is to provide clarity to the regulations. The use of the shortened phrase "right to know" also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (dd) establishes that "right to limit" means the consumer's right to request that the business limit the use and disclosure of a consumer's sensitive personal information as set forth in Civil Code section 1798.121. The purpose of defining this term is to provide clarity to the regulations. The use of the shortened phrase "right to limit" also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (ee) establishes that "right to opt-out of sale/sharing" means the consumer's right to direct a business that sells or shares personal information about the consumer to third parties to stop doing so as set forth in Civil Code section 1798.120. The purpose of defining this term is to provide clarity to the regulations. The use of the shortened phrase "right to opt-out of sale/sharing" also makes the regulations more readable, and thus, easier for consumers and businesses to understand.

Subsection (gg) has been revised to add requests to correct to align the regulation with the amended language of the statute. Civil Code section 1798.106, subdivision (c), states that a request to correct is to be a verifiable consumer request.

Subsection (ii) establishes that "unstructured" personal information means personal information that is not organized in a pre-defined manner, such as text, video files, and audio files. The purpose of defining this term is to provide clarity to the regulations as this term is used in connection with the right to correct.

Subsection (jj) has been revised to add "request to correct" to align the regulation with the amended language of the statute. Civil Code section 1798.106, subdivision (c), states that a request to correct is to be a verifiable consumer request.

Changes without regulatory effect. Non-substantive changes (e.g., reordering the type of CCPA requests) have been made throughout the section. Authority and reference citations have been amended. The subsections have been renumbered.

§ 7002. Restrictions on the Collection and Use of Personal Information.

Civil Code section 1798.100, subdivision (c), requires a business's collection, use, retention, and sharing of a consumer's personal information to be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and that the personal information not be further processed in a manner that is incompatible with those purposes. Civil Code section 1798.100, subdivision (a), also prohibits the business from collecting or using personal information for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, without providing the consumer with notice.

The purpose of section 7002 of these regulations is to interpret and clarify the different subdivisions of Civil Code section 1798.100 and is necessary to provide guidance for consumers and businesses regarding their implementation. This section is informed by and included because of public comments received by the Agency during preliminary rulemaking activities, observations in the current marketplace, and the purpose and intent set forth in the CPRA. Specifically, the interpretation provided in section 7002 reflects the explicit, stated purpose and intent of the CPRA that consumers "should know who is collecting their information and that of their children, how it is being used, and to whom it was disclosed so they have the information necessary to exercise meaningful control over businesses' use;" that consumers "should be able to control the use of their personal information;" and that businesses should only collect consumer's personal information for "specific, explicit, and legitimate disclosed purposes" and not for reasons incompatible with those purposes. (Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3(B)(2).) Section 7002 also reflects the mandate set forth in Civil Code section 1798.185, subdivision (a)(10), that the purposes for which businesses may use consumers' personal information should be consistent with consumers' expectations. Section 7002 helps fulfill the mandate to provide businesses and consumers "clear guidance about their responsibilities and rights," and to implement the law in such a way that the consumer is "in the position to knowingly and freely negotiate with a business over the business' use of the

consumer's personal information." (*Id*. at § 3(C)(2) & (3).) It restricts businesses from using consumers' personal information for disclosed purposes that are unrelated to a consumer's expectation simply because they are hidden within a lengthy and dense privacy policy.

Subsection (a) explains that a business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purpose(s) for which the personal information was collected or processed, and that to be reasonably necessary and appropriate, the business's activities must be within the reasonable expectations of an average consumer when the personal information was collected. The subsection further clarifies that the business can collect, use, retain, and/or share personal information for another disclosed purpose if that disclosed purpose is compatible with what an average consumer would reasonably expect.

This regulation is necessary to explain the limitations that Civil Code section 1798.100, subdivisions (a) and (c), place on the purposes for which a business may collect, use, retain, and share personal information, to provide guidance regarding what activities are "necessary and appropriate," and to interpret the phrase "context in which the personal information was collected" within Civil Code section 1798.100, subdivision (c). The subsection explains that a business's collection, use, retention, and/or sharing of consumer's personal information must not contravene reasonable consumer expectations by going beyond purposes that are related or compatible with the purposes an average consumer would reasonably expect. If businesses wish to use consumers' personal information for an unrelated or incompatible purpose, then the explicit consent of the consumer, in accordance with section 7004, is required. Requiring a business to obtain explicit consent places consumers in a position to exercise meaningful control over their personal information, while still allowing businesses to use the personal information for what an average consumer would expect without having to obtain explicit consent. (See Access Now, Data Minimization: Key to Protecting Privacy and Reducing Harm (May 2021); Consumer Reports and EPIC, How the FTC Can Mandate Data Minimization through a Section 5 Rulemaking (January 26, 2022).)

Subsection (b) provides four illustrative examples of how to comply with this requirement. This subsection benefits both businesses and consumers by providing clear examples of when the collection, use, retention, and sale or sharing of personal information is "reasonably necessary and proportionate" to the purpose for which it was collected, and when the disclosed purpose would be "compatible with the context in which the personal information was collected."

Subsection (c) implements and clarifies how Civil Code section 1798.100, subdivisions (a)(1) and (c), work together. Civil Code section 1798.100, subdivision (a)(1), existed prior to the CPRA amendments to CCPA, but was amended by the CPRA to clarify what "uses" of personal information by businesses the subdivision covers. Civil Code section 1798.100, subdivision (c), is entirely new, added via the CPRA amendments. This subsection explains the relationship between the pre-CPRA statutory language and the clarifications and requirements added by the CPRA amendments. It explains that businesses are restricted from collecting or using personal information beyond what was disclosed in the notice at collection. It incorporates existing section 7012, subsection (a)(4)'s requirement that a business that intends to collect new categories of personal information not disclosed in the notice at collection or intends to use it in a new way, provide a separate, updated notice at collection. But it also clarifies that the new use

or collection must still comply with subsection (a). Section 1798.100, subdivision (a)(1), makes clear that a business cannot change its practices after giving the notice at collection because the consumer could have reasonably relied on the information provided in the notice at collection when interacting with the business, while subdivision (c) places an additional requirement that a business's collection, use, and sharing of personal information has to be compatible with the context in which the personal information was collected, which subsection (a) interprets to mean that it must be a purpose reasonably expected by an average consumer.

§ 7003. Requirements for Disclosures and Communications to Consumers.

Civil Code section 1798.185, subdivision (a)(6), gives the Agency authority to establish rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide under the CCPA are provided in a manner that may be "easily understood by the average consumer, are accessible to consumers with disability, and are available in the language primarily user to interact with the consumer…." This regulation consolidates guidance regarding how businesses are to provide information to consumers into one place instead of repeatedly stating the same thing in multiple places. The regulation also extends some of the requirements to other disclosures and communications the business has with consumers, not just the notices required under the CCPA. The regulation is necessary to ensure that disclosures are provided to consumers in a manner that is easily accessible and understandable to consumers, including those with disabilities, as required by Civil Code section 1798.185, subdivision (a)(6). This regulation also benefits businesses and consumers by making the regulation easier to read and understand and less repetitive.

Subsection (a) consolidates the requirements set forth in existing sections 7011(a)(2)(a), 7012(a)(2)(a), 7013(a)(2)(a), and 7016(a)(2)(a) and clarifies that all disclosures and communications to consumers shall be easy to read and understandable to the consumer. This subsection continues to be necessary to clarify that the guidance applies to more than just the notice at collection, notice of right to opt-out, privacy policy, and notice of financial incentive, in accordance with Civil Code section 1798.185, subsection (a)(6). It also benefits businesses and consumers by making the regulation less repetitive, and thus, easier to read and understand. The subsection is still necessary because studies have found that presentation and the use of plain language techniques positively influence the effectiveness and comprehension of privacy policies. (See Schaub et al., A Design Space for Effective Privacy Notices, which was presented at the Symposium on Usable Privacy and Security (SOUPS 2015), July 22-24, 2015; Center for Plain Language, Privacy-policy analysis (2015); Chen et al., Fighting the Fog: Evaluating the Clarity of Privacy Disclosures in the Age of CCPA, which was presented at the 20th Workshop on Privacy in the Electronic Society (WPES '21), November 15, 2021.) The subsection continues to take a performance-based approach, calling for the disclosures and communications to be designed and presented in a way that makes it easy to read and understandable by consumers.

Subsection (b) consolidates the requirements set forth in existing sections 7011(a)(2)(b)-(d), 7012(a)(2)(b)-(d), 7013(a)(2)(b)-(d), and 7016(a)(2)(b)-(d). This benefits businesses and consumers by making the regulation less repetitive, and thus, easier to read and understand. This subsection continues to provide general principles for making required notices accessible and comprehensible. It specifies that the disclosures have to be in the same language in which the

business provides other information to consumers in California, such as languages in which it provides contracts and other information. It uses the language of "reasonably accessible to consumers with disabilities" to acknowledge that the definition of disabilities may be broad, and thus, the business's obligations are tied to a generally recognized industry standard 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 25, 2022].) 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. It is also the standard that the California government is required to comply with per Government Code section 11546.7.

Subsection (c) clarifies that, for websites, a conspicuous link must appear in a similar manner as other links used by the business on its webpage, and at least the same approximate size or color as other links. This subsection is necessary to ensure that businesses make the link as clear and conspicuous or otherwise accessible as other types of links on a webpage, but it also provides the business flexibility to make it more conspicuous by using the phrase "at least." If a required disclosure is not conspicuous, then a consumer may not see or take the opportunity to read the material information required to be disclosed. The "conspicuous" definition also addresses the placement and format of disclosures so that they can be seen and read even when viewed on different sized screens and monitors. From a technical and design perspective, businesses can feasibly implement the requirements because they are consistent with current technology and web design usability principles. It also provides businesses with clear guidance about what is required of them.

Subsection (d) clarifies that, for mobile applications, a conspicuous link shall be accessible within the application, such as through the application's settings menu, and included in the business's privacy policy, which must be accessible through the mobile application's platform page or download page. This subsection is necessary to ensure that businesses make the link easily accessible both within the application and before the consumer downloads the application. It also provides businesses with clear guidance about what is required of them.

§ 7004. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent.

Civil Code section 1798.185, subdivisions (a)(4)(A) and (a)(7), give the Agency authority to establish rules and procedures to facilitate and govern the submission of consumer requests under the CCPA. This mandate requires that the Agency ensure that consumers have the ability to exercise their choices without undue burden and to prevent businesses from engaging in deceptive or harassing conduct. (*Id.)* Relatedly, CPRA amendments to the CCPA add a definition for "consent" that explicitly states that acceptance of general terms of use or an agreement obtained through use of dark patterns does not constitute consent. (Civ. Code, § 1798.140, subd. (h).) A "dark pattern" is defined to mean a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy,

decisionmaking, or choice, and may be further defined by regulation. (Civ. Code, § 1798.140, subd. (l).) Accordingly, the purpose of section 7004 of these regulations is to provide guidance to businesses regarding how to craft methods for submitting CCPA requests and obtaining consumer consent that ensure that the consumer's choice is freely made and not manipulated, subverted, or impaired through the use of dark patterns. This section also furthers the purpose and intent of the CCPA by ensuring that businesses provide consumers with easily accessible means to exercise their rights. (Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3(B)(4).)

This section is informed by significant academic scholarship on the topic of dark patterns and consumer consent, as well as public comments submitted to the Agency during preliminary rulemaking activities. (See Lupianez-Villanueva et al., European Commission, Directorate-General for Justice and Consumers, Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation: Final Report (2022); Competition and Markets Authority, Evidence Review of Online Choice Architecture and Consumer and Competition Harm (April 5, 2022) (hereafter Competition and Markets Authority); King & Stephan, *Regulating Privacy Dark Patterns in Practice – Drawing Inspiration from California Privacy Rights Act* (2021) 5 Geo. L. Tech. Rev. 251; World Economic Forum, Redesigning Data Privacy: Reimagining Notice & Consent for Human-Technology Interaction, White Paper (July 2020); Nouwens et al., Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence, which was presented at the CHI '20, April 25-30, 2020 (hereafter Nouwens); Mathur et al., Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites, which was presented at the 22nd ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW), November 2019.) It addresses not only narrow situations where consent must affirmatively be given (*e.g.*, when participating in a financial incentive program or opting into the sale of personal information), but general methods for submitting CCPA requests to address abuse by businesses who craft methods in ways that discourage consumers from exercising their rights. It benefits businesses by providing clear and extensive guidance on best practices for obtaining consent and includes many illustrative examples that identify common dark patterns. This is especially helpful because, by definition, a dark pattern does not require intent on behalf of the business to subvert consumer choice. (Civ. Code, § 1798.140, subd. (l).) The section also benefits consumers by identifying and outlawing widespread practices that subvert and manipulate consumer choice.

Subsection (a) sets forth the principles that businesses must follow in designing and implementing their methods for submitting CCPA request and obtaining consumer consent. It includes the language "[e]xcept as expressly allowed" to explain that following other requirements set forth in the regulations or in the CCPA would not be in violation of this regulation. For example, section 7020, subsection (d), allows a business to use a two-step process for online requests to delete. Doing so would not be considered a violation of subsection (a)(5), which prohibits unnecessary burden or friction to the process of submitting a CCPA request, because it is allowed under these regulations. However, the business shall otherwise comply with section 7004.

Subsection (a)(1) requires that the methods for submitting CCPA requests and obtaining consent use language that is easy to read and understand, and when applicable, comply with the requirements for disclosures set forth in section 7003. The subsection is necessary to ensure that

consumers can understand the processes by which they submit CCPA requests and provide consent.

Subsection (a)(2) explains that the businesses' methods must provide symmetry in choice and shall not make the path for a consumer to exercise a more privacy-protective option to be longer than the path to exercise a less privacy-protective option. This is necessary to ensure that the consumer's choice for submitting CCPA requests and providing consent is freely made and not manipulated, subverted, or impaired through the use of dark patterns. It provides several real-world examples to illustrate how businesses are to apply this principle. **Subsection (a)(2)(A)** is existing section 7027, subsection (h)(1), and specifically prohibits businesses from requiring a consumer to go through more steps in opting out of the sale of personal information than the number of steps required for the consumer to opt-in to the sale of personal information after previously opting out. Instead of imposing a prescriptive standard based on the number of steps used, the regulation holds the business to a standard that the business would create for itself, *i.e.*, the flow process for opting into the sale of data. Businesses are motivated to use a simple and easy flow process for opting into the sale of data because it is advantageous for them. Requiring the business to use the same number of steps for opting out of the sale of the data sets a performance-based standard that is both flexible for a wide variety of industries and factual scenarios, but also measurable and clearly enforceable. It addresses a common dark pattern that researchers characterize as a "roach motel" (easy to get in but hard to get out) and provides a concrete way for businesses to measure whether they are using a minimal number of steps. (See Luguri & Strahilevitz, *Shining a Light on Dark Patterns*, (2021) 13 J. Legal Analysis, 43, 49; Complaint at ¶ 8, Fed. Trade Comm'n v. Age of Learning, Inc. (C.D. Cal 2020) (No. 2:20-cv-07996); Thomas Germain, *How to Spot Manipulative 'Dark Patterns' Online* (January 30, 2019) Consumer Reports.) The subsection also identifies for businesses how to measure the start of the flow process for both the opt-out and opt-in process so that they can accurately compare the number of steps for both processes. Because the CCPA does not require that businesses obtain opt-in consent for the sale of personal information, except for consumers under the age of 16, the phrase "opt-in to the sale of personal information after having previously opted out" is used to advise businesses that the comparison of the opt-out process should be with the opt-in process for consumers 16 years and older. **Subsection (a)(2)(B)** prohibits a very common practice observed in the marketplace. **Subsections (a)(2)(C) through (E)** demonstrate how asymmetrical choices are not just in the length of the path, but in how the choices are presented. (See Competition and Markets Authority, *supra*, pp. 30-97; Nouwens, *supra*, p. 9)

Subsection (a)(3) instructs businesses to avoid language or interactive elements that are confusing to the consumer, explicitly prohibits the use of double negatives, and requires toggles and buttons to clearly indicate the state of the consumer's choice. This is necessary to ensure that the consumer's choice for submitting CCPA requests and providing consent is freely made and not manipulated, subverted, or impaired through the use of dark patterns. It also provides real-world examples to illustrate how businesses are to apply this principle. The prohibition on double negatives is not new, but is found in existing section 7027, subsection (h)(2). **Subsection (a)(3)(A)** is a clear example of a double negative used by businesses that confuses the consumer. **Subsections (a)(3)(B) and (C)** demonstrate how elements, like toggles and buttons, can confuse the consumer. (See Habib, Evaluating the Usability of Privacy Choice Mechanisms, Institute for Software Research, School of Computer Science, Carnegie Mellon University (2021) p. 72; Habib et al., Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy

Choices with Icons and Link Texts, which was presented at the CHI Conference on Human Factors in Computing Systems (CHI '21), May 8-13, 2021, pp. 11-12.)

Subsection (a)(4) instructs businesses to avoid manipulative language or choice architecture and explicitly prohibits the use of language or wording that guilts or shames the consumer. This is necessary to addresses a common dark pattern that researchers characterize as "confirm-shaming." (Competition and Markets Authority, *supra*, p. 114). The subsection also prohibits bundling consent in such a way that subverts the consumer's choice. The subsection provides a number of real-world examples to illustrate how businesses are to apply this principle. **Subsection (a)(4)(A)** is an example of confirm-shaming that is extremely prevalent in the marketplace. **Subsection (a)(4)(B)** is existing section 7027, subsection (h)(3), and addresses another common practice where the business questions and guilts the consumer for making their choice. **Subsection (a)(4)(C)** is an example of how a business may bundle consent in a way that manipulates the consumer. (See Nouwens, *supra*, pp. 5-10; O'Connor et al., (Un)clear and (In)conspicuous: The Right to Opt-Out of Sale under CCPA (July 14, 2021) pp. 6-7 (hereafter O'Connor).)

Subsection (a)(5) prohibits businesses from adding unnecessary burden or friction to the process by which a consumer submits a CCPA request. It explains that businesses should be testing their methods to ensure that they are functional. This guidance is particularly important because it speaks to the fact that a dark pattern does not require intent to subvert consumer choice, but rather that it has the effect of subversion. The subsection provides examples to illustrate how businesses are to apply this principle. **Subsection (a)(5)(A)** is existing section 7027, subsection (h)(5), and is an example of unnecessary burden and friction. **Subsection (a)(5)(B)** is an example of how untested and broken methods may cause unnecessary burden on consumers, and **subsection (a)(5)(C)** is an example of unnecessary friction in business process. All of these examples are taken from practices seen in the marketplace. (See Competition and Markets Authority, *supra*, pp. 76-82; O'Connor, *supra*, pp. 7-8.)

Subsection (b) clarifies that a method that does not comply with subsection (a) may be considered a dark pattern and explains that any agreement obtained through the use of dark patterns shall not constitute consent in accordance with Civil Code section 1798.140, subdivision (h). This subsection is necessary to clarify the consequence for businesses that use dark patterns and to clarify what is a dark pattern.

Subsection (c) incorporates Civil Code section 1798.140, subdivision (l)'s, definition of a "dark pattern," which does not require a user interface to be created by the business with the intention to subvert or impair consumer choice. Whether a dark pattern exists depends on the substantial effect of the user interface. This subsection is necessary to clarify the definition of a dark pattern. This subsection also addresses public comments the Agency received during preliminary rulemaking activities calling upon the Agency to limit the definition of dark patterns to only instances of deception. This would not be in line with the explicit language of Civil Code section 1798.140, subdivision (l), which explicitly defines a dark pattern to exist when the substantial effect of the user interface subverts or impairs consumer choice, regardless of the intent of the business when creating the interface.

Article 2. Required Disclosures to Consumers

Change without regulatory effect. The title of the article has been changed to "Required Disclosures to Consumers" to more accurately reflect the content within this article.

§ 7010. Overview of Required Disclosures.

This section provides clarity and guidance regarding the disclosures that businesses must provide to consumers. It was originally drafted in response to public comments received by the Attorney General's Office expressing confusion about the number and type of notices that businesses are required to provide. The term "disclosure" is broader than the word "notices" and more adequately reflects the type of disclosures required by the CCPA. This section provides a roadmap of the different disclosures businesses must provide to consumers and clarifies when a business must provide the disclosure. This section is necessary to ensure that businesses understand and abide by the obligations of the CCPA. Revisions and additions to this section reflect changes to align the regulation with the amended language of the statute. The specific changes are explained below.

Subsection (b) has been revised to state that a business that controls the collection of the consumer's personal information is to provide a notice at collection. This change is necessary to align the regulation with the express language of the statute.

Subsection (c) has been revised to include that a business that sells or shares personal information is to provide a notice of right to opt-out or the alternative opt-out link in accordance with the CCPA and the regulations. This change is necessary to align the regulation with the amended language of the statute, which expanded the right to opt-out to include the sharing of personal information and introduced the new structure for opt-out links set forth in Civil Code section 1798.135. This subsection includes the language "[e]xcept as set forth in section 7025" to acknowledge that if the business processes an opt-out preference signal in a frictionless manner, it is not required to provide the specified notice of right to opt-out or alternative opt-out link. This language is necessary to align the regulation with the express language of the statute.

Subsection (d) requires that a business that uses or discloses sensitive personal information for purposes other than those specified in section 7027, subsection (l), must provide a notice to limit or the alternative opt-out link in accordance with the CCPA and these regulations. This section is necessary because Civil Code section 1798.121, subdivision (a), requires business to provide notice to consumer of this new right to limit.

Changes without regulatory effect. Reference citations have been amended. The title has been amended to better reflect the content of the regulation. The subsections have been renumbered.

§ 7011. Privacy Policy.

Civil Code section 1798.130, subdivision (a)(5), requires a business to disclose certain information in its privacy policy and to update that information at least once every 12 months. The purpose of this section is to set forth the rules and procedures businesses must follow regarding the form, content, and posting of the privacy policy. The regulation is necessary to ensure that the privacy policy contains the necessary information and is provided in a manner

that makes it easily accessible and understandable to consumers. Revisions and additions to this section reflect changes to align the regulation with the revised language of the statute. The section has also been reorganized to better assist businesses and consumers in understanding what information must be included in the privacy policy. The specific changes are explained below.

Subsection (a) has been revised to further clarify the purpose of the privacy policy. It states that the purpose is to provide consumers with a comprehensive description of a business's online and offline practices regarding the collection, use, sale, sharing, and retention of consumer personal information and to inform consumers of the rights they have regarding their personal information and any information necessary for them to exercise those rights. The privacy policy provides in one place all the disclosures required by the CCPA, as well as all the information consumers need to know to exercise their rights under the CCPA. The revision is necessary to clarify that the reason why information about the CCPA rights are included in the privacy policy is not just to inform the consumer about them, but to provide the consumer with information on how to exercise those rights with the business. This benefits consumers because it ensures that consumers can access all the information about their CCPA rights in one place.

Existing subsections (a)(2)(A)-(D) have been deleted because the content has been moved to section 7003.

Subsection (b) has been added to clarify that the privacy policy shall comply with section 7003, subsections (a) and (b), which is where the content was moved. Repeating this requirement in subsection (b) is necessary for clarity so that all rules pertaining to privacy policies are in one place.

Subsection (c) contains the information found in existing subsection (a)(2)(E).

Subsection (d) has been revised to include "that complies with section 7003, subsection (c) and (d)" to reference the new regulation that explains what a "conspicuous link" means. Repeating this requirement in subsection (d) is necessary for clarity so that all rules pertaining to privacy policies are in one place. The last sentence of the subsection has also been revised to state "shall" instead of "may." This is necessary to provide consumers an easy way to access information about the business's collection and use of personal information within the mobile application. Requiring inclusion of a link to the privacy policy in the application's settings menu is necessary so that a consumer does not have to search for the application's download page to access the privacy policy. This revision benefits businesses by providing clear direction regarding what is expected of them and it benefits consumers in ensuring that this information is easily accessible to the consumer.

Subsection (e) is a reorganization of existing subsection (c). Rather than listing what must be included by right, the revised subsection lists the required information in an order that focuses on the business's data practices and the general flow of data through a business, from its collection and use through the business's sharing, selling, and retention of the personal information. It then goes on to include an explanation of CCPA rights, as required by Civil Code section 1798.130, subdivision (a)(5), how the consumer can exercise those rights, and what the consumer can expect from the process. The substance of what must be included in the privacy policy is

primarily the same except that it now includes the new rights added by the CPRA's amendments to the CCPA (*i.e.*, right to correct, right to limit, right to opt-out of the sale and sharing of personal information) and information about the business's response to opt-out preference signals.

The subsection is necessary because it provides a comprehensive picture of a business's privacy practices and of how consumers can exercise their rights under the CCPA. The subsection consolidates all statutory requirements for the privacy policy, which are distributed throughout the CCPA, and other helpful information, making the privacy policy a useful resource for consumers and others interested in evaluating the effectiveness of the CCPA. The reorganization is not meant to prescribe the organization of any business's privacy policy, but it does conform to how many businesses already organize their privacy policy. Thus, it is beneficial to businesses because it makes it easier for them to use the regulation as a checklist to ensure that all the information necessary is included in their privacy policy.

Changes without regulatory effect. Reference citations have been amended. The subsections have been renumbered.

§ 7012. Notice at Collection of Personal Information.

Civil Code section 1798.100, subdivision (a), requires a business that controls the collection of a consumer's personal information to inform consumers, at or before the point of collection, of the categories of personal information it collects, the purposes for which the categories are used, whether it is sold or shared, and how long the business intends to retain it. The purpose of this section is to set forth the rules and procedures businesses must follow regarding the form, content, and posting of the notice at collection, including as it relates to third parties that control the collection of personal information. This regulation is necessary to ensure that the notice is easily accessible and understandable to consumers and businesses have clear guidance on how to provide the information required in Civil Code section 1798.100, subdivision (a). Revisions and additions to this section are also necessary to align the regulation with the revised language of the statute. The specific changes are explained below.

Subsection (a) has been revised to clarify the purpose of the notice at collection. It pulls from the stated purpose and intent of the CPRA, which states that "[c]onsumers should know who is collecting their personal information and that of their children, how it is being used, and to whom it is disclosed, so that they have the information necessary to exercise meaningful control over business' use of their personal information that of their children." (Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3(A)(1).) Subsection (a) now incorporates how the notice is meant to provide meaningful control to the consumer, and that meaningful control means that the notice should provide consumers with the opportunity to choose how to engage with the business in light of their information practices. For example, upon receiving the notice at collection, the consumer should have all the information necessary to choose whether or not to engage with the business, or to direct the business not to sell or share their personal information and to limit the use and disclosure of the sensitive personal information so that they can exercise those rights at the earliest point in time that the information is collected. This prevents any delay that may lead to the dissemination or use of the consumer's information against the consumer's wishes. This clarification is necessary to guide businesses as they make decisions on how to provide notice.

To the extent that there are multiple ways a business can provide notice, the business should pick the manner that would best accomplish the purpose of the notice.

Existing subsection (a)(2) has been deleted because the content has been moved to section 7003. **Subsection (b)** has been added to clarify that the notice at collection shall comply with section 7003, subsections (a) and (b), which is where the content was moved. Repeating this requirement in subsection (b) is necessary for clarity so that all rules pertaining to notices at collection are in one place. **Subsection (c)** contains the information found in existing subsection (a)(3). **Subsection (c)(2)** now provides an example of how the notice can be given in connection with information that is collected by a webform. This additional example provides further guidance to businesses with regard to a common manner for collecting personal information.

Existing subsection (a)(4) has been deleted because Civil Code section 1798.100, subdivision (c), now prohibits a business from collecting, using, retaining, and sharing a consumer's personal information if that processing is incompatible with the context in which the personal information was collected. Section 7002 interprets Civil Code section 1798.100, subdivision (c), to mean that the business's collection, use, retention, and sharing of the personal information must be consistent with what an average consumer would expect when the personal information was collected. Accordingly, a business can no longer collect personal information that a consumer would not reasonably expect a business to collect regardless of how the business gives notice. The business must now obtain the consumer's consent for such uses in accordance with section 7004.

Existing subsection (a)(5) has been moved and incorporated into section 7002, subsection (c).

Subsection (d) contains the information found in existing subsection (a)(6).

Subsection (e) contains the information found in existing subsection (b). It has additional language to align the regulation with the revised language of the Civil Code section 1798.100. **Subsection (e)(5)** has been simplified to cite to the link to the notice of right to opt-out of sale/sharing instead of the "Do Not Sell My Personal Information" link because not all businesses that sell or share personal information are required to have a link. The CPRA revisions to the CCPA allow businesses to use an alternative opt-out link or to not post the link if they provide a frictionless response to an opt-out preference signal. However, pursuant to the regulations, all businesses must still provide a notice of right to opt-out of sale/sharing.

Subsection (e)(6) requires a business that allows third parties to control the collection of personal information on its website or on its premises to include the names of the third parties in its notice; or, in the alternative, information about the third parties' business practices. This is necessary to provide the consumer with all the information necessary to choose whether or not to engage with the business. Although Civil Code section 1798.100, subdivision (b), requires third parties controlling the collection to post the notice at collection on their website, consumers would not be able to learn what these third parties are doing with their information because they do not know where to look. This runs counter to the purpose of the notice at collection and the intent of the CPRA amendments to the CCPA. Furthermore, given the requirement in Civil Code section 1798.100, subdivision (d), that a business enter into contracts with all third parties that it sells, shares, or discloses personal information to, businesses should be able to identify all

third parties without significant burden. To the extent that the business does not want to identify the third parties, the business has the option of including information about those third parties' practices within its own privacy policy. This alternative meets the objective of the notice at collection and provides the business with some flexibility.

Subsection (f) has been revised to explain that the notice may be given by providing a link that takes the consumer directly to the specific section of the business's privacy policy that contains the information required in subsection (c). It further clarifies that directing the consumer to the top of the privacy policy where the consumer is required to scroll through lengthy descriptions in order to obtain the required information is not sufficient to meet this standard. This revision is necessary to ensure that the consumer is taken directly to the information required by the notice and to prevent consumers being led on a wild goose chase for the material information. (See Mahoney, California Consumer Privacy Act: Are Consumers' Digital Rights Protected?, Consumer Reports (October 1, 2020) pp. 14-23, 32 (hereafter Mahoney); O'Connor, *supra*, pp. 6-8.)

Subsection (g) has been added to explain what is meant by the new language "controls the collection" added to Civil Code section 1798.100, subdivisions (a) and (b). This regulation is necessary to clarify in what circumstances a business and/or a business "acting as a third party" is controlling the collection of personal information and what obligations those businesses have. The regulation benefits both businesses and consumers by providing clear guidance and setting expectations regarding who needs to provide a notice of collection, how they should provide the notice, and what that notice should include.

Subsection (g)(1) explains that more than one business may control the collection of personal information, and thus, have the obligation to provide a notice at collection. It also provides an example of how more than one business may control the collection of personal information. **Subsection (g)(1)(A)** further explains that the fact that more than one business may control the collection of personal information does not impact a first party's obligation to comply with a consumer's request to opt-out of the sale/sharing. A first party that authorizes a third party to jointly control the collection of personal information is still "making available" that personal information to the third party, which may be considered a "sale" or "sharing." Accordingly, a first party who receives a request to opt-out of sale/sharing must comply with the consumer's request in accordance with the CCPA and these regulations. This regulation is necessary to dispel any misunderstanding that these sections affect a party's obligation to honor a consumer's request to opt-out of sale/sharing.

Subsection (g)(2) requires first parties that allow businesses, acting as third parties, to control the collection of personal information to include the names of those third parties in their notice at collection, or, in the alternative, include information about the third parties' practices in the first party's notice. This is necessary to provide the consumer with all the information necessary to choose whether or not to engage with the business. Although Civil Code section 1798.100, subdivision (b), requires third parties controlling the collection to post the notice at collection on their website, consumers would never be able to learn what these third parties are doing with their information because they do not know where to look. This runs counter to the purpose of the notice at collection and the intent of the CPRA amendments to the CCPA. In the alternative,

the first party and third party can work together to include the required information in the first party's notice at collection. This would address the need to identify the third party.

Subsection (g)(3) explains the requirement in Civil Code section 1798.100, subdivision (b), which requires business acting as a third party that control the collection of personal information on the first party's premises to post their own notice at collection in a clear and conspicuous manner at the location. This is necessary to clarify how the requirements are different when the third party is collecting personal information on the first party's physical premises.

Subsection (g)(4) provides three illustrative examples of how to comply with this requirement. This subsection benefits both businesses and consumers by providing clear examples of third party businesses that control the collection of personal information in both an online and offline context and how they can provide a notice at collection.

Subsections (h), (j), and (k) have been revised to align the regulation with the revised language of the statute.

Subsection (i) has been revised to clarify that data brokers do not need to provide a notice at collection if they do not collect personal information directly from the consumer. This clarification is necessary because there are instances when data brokers may be collecting personal information directly from the consumer, and thus, they would be obligated to provide a notice at collection. (Civ. Code, § 1798.100.) "Of sale/sharing" has also been added to "request to opt-out" to include that the request refers to both sale and sharing to align the regulation with the amended language of the statute

Changes without regulatory effect. Reference citations have been amended. The subsections have been renumbered.

§ 7013. Notice of Right to Opt-Out of Sale/Sharing and the "Do Not Sell Or Share My Personal Information" Link.

The CPRA's amendment to Civil Code section 1798.120 extended the right of a consumer to opt out of a business's sale of personal information to the business's sharing of personal information, as that term is defined in Civil Code section 1798.140, subdivision (ah). Relatedly, all businesses covered by the CCPA that sell or share personal information must also provide notice to the consumer of their right to opt-out of the sale and sharing of their personal information pursuant to Civil Code section 1798.135, which requires that the business post a "Do Not Sell or Share My Personal Information" link. Accordingly, changes have been made to this section to align the regulation with the amended language of the statute.

The purpose of section 7013 of these regulations is to set forth the rules and procedures businesses must follow regarding the form, content, and posting of the notice of right to opt-out and how it relates to the "Do Not Sell or Share My Personal Information" link. The regulation is necessary to ensure that the notice of right to opt-out and the "Do Not Sell or Share My Personal Information" link contain the information required by Civil Code section 1798.135, subdivision (a), and are provided in a manner that makes them easily accessible and understandable to consumers, including those with disabilities, as required by Civil Code section 1798.185, subdivision (a)(6). The specific changes are explained below.

Subsection (a) has been revised to explain that the purpose of the "Do Not Sell or Share My Personal Information" link is to either immediately effectuate the consumer's right to opt-out of the sale/sharing or direct the consumer to the notice of right opt-out where they can both learn about their right to opt-out and exercise that right. This revision allows businesses to execute the consumer's right to opt-out of sale/sharing with one click, which some businesses are already doing, and gives deference to businesses to craft their methods to opt-out so that they are easily accessible to consumers, in line with the purpose and intent of the CCPA. (Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3(B)(4).)

Existing subsection (a)(2) has been deleted because the content has been moved to section 7003. **Subsection (b)** has been added to clarify that the notice of right to opt-out of sale/sharing shall comply with section 7003, subsections (a) and (b), which is where the content was moved. Repeating this requirement in subsection (b) is necessary for clarity so that all rules pertaining to the notice of right to opt-out of sale/sharing are in one place.

Subsection (c) requires the "Do Not Sell or Share My Personal Information" link be a conspicuous link that is located in either the header or footer of the business's internet homepages. The term "conspicuous link" is explained in section 7003 and the term "homepage" is explicitly defined Civil Code section 1798.140, subdivision (p). The regulation benefits businesses by providing them explicit guidance regarding the placement of the link and benefits consumers so that they know where to look for the link. This subsection is also in response to comments received by the Agency during its preliminary rulemaking activities that consumers experience difficulty finding the link. (See O'Connor, *supra*, p. 5; Mahoney, *supra*, pp. 14-23.)

Subsection (d) operationalizes Civil Code section 1798.135, subdivision (a)(3), which gives the business discretion to use an alternative opt-out link that easily allows consumers to exercise their right to opt-out of sale/sharing and their right to limit. It also operationalizes Civil Code section 1798.135, subdivision (b)(1), which gives the business the choice of posting the "Do Not Sell or Share My Personal Information" link or processing an opt-out preference signal in a frictionless manner in accordance with the regulations. It clarifies that if a business uses an alternative opt-out link or processes an opt-out preference signal in a frictionless manner, it must comply with sections 7015 and 7025(f) and (g), and must still post a notice of right to opt-out of sale/sharing by including it in its privacy policy. This section is necessary to explain how these different parts of the CCPA work together with these regulations.

Subsection (e) has been revised to include both sale and sharing of personal information to align the regulation with the amended language of the statute. **Subsection (e)(1)** has been revised to remove the instructions regarding the placement of the link in light of the more specific instructions set forth in subsection (b). It also clarifies that if clicking on the "Do Not Sell or Share My Personal Information" link immediately effectuates the consumer's right to opt-out of sale/sharing or if the business processes an opt-out preference signal in a frictionless manner and is not required to post the link, the notice shall be included in the business's privacy policy. This section is necessary to clarify the business's obligations under different circumstances. **Subsection (e)(2)** has been revised to align the regulation with the amended language of the statute and to cross-reference the correct section of the regulations. **Subsection (e)(3)** has been revised to clarify that the notice shall be provided in the same manner in which the business collects the personal information that it sells or shares. The subsection includes additional

illustrative examples that addresses situations such as connected devices and augment or virtual reality. These revisions are necessary to address new ways in which businesses are collecting personal information that they sell or share so that the notice is effective in informing consumers of their right to opt-out of the sale/sharing.

Subsection (f) has been revised to align the regulation with the amended language of the statute. Changes have been made to make it easier to read and understand.

Existing subsection (f) has been deleted because the opt-out icon has been incorporated into section 7015 regarding the alternative opt-out link.

Subsections (g) and (h) have been revised to align the regulation with the amended language of the statute.

Changes without regulatory effect. The title has been amended to better reflect the content of the regulation. The subsections have been renumbered.

§ 7014. Notice of Right to Limit and the "Limit the Use of My Sensitive Personal Information" Link.

Civil Code section 1798.121, subdivision (a), requires all businesses that use or disclose a consumer's sensitive personal information for certain purposes to provide notice to consumers of their right to limit the use or disclosure of their sensitive personal information. The purpose of section 7014 is to set forth the rules and procedures businesses must follow regarding the form, content, and posting of the notice of right to limit. The regulation also addresses situations where a business does not maintain a website or interacts with consumers in ways other than online. This regulation is necessary to ensure that the notice is easily accessible and understandable to consumers and businesses have clear guidance on how to provide the information required in Civil Code sections 1798.121 and 1798.135.

Subsection (a) explains the different purposes of the notice of right to limit and the "Limit the Use of My Sensitive Personal Information" link. It explains that the "Limit the Use of My Sensitive Personal Information" link is meant to either immediately effectuate the consumer's right to limit or direct the consumer to the notice of limit where they can both learn about their right to opt-out and exercise that right. This regulation allows businesses to execute the consumer's right to limit with one click and gives deference to businesses in how to craft their methods so that they are easily accessible to consumers, which is in line with the purpose and intent of the CCPA. (Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3(B)(4).) This regulation is necessary to clarify the distinction between the notice of right to limit and the "Limit the Use of My Sensitive Personal Information" link.

Subsection (b) has been added to clarify that the notice of right to limit shall comply with section 7003, subsections (a) and (b). Repeating this requirement in subsection (b) is necessary for clarity so that all rules pertaining to the notice of right to limit are in one place.

Subsection (c) implements Civil Code section 1798.135, subdivision (a)(2), regarding how to make the notice of right to limit reasonably accessible to consumers. It requires the "Limit the Use of My Sensitive Personal Information" link be a conspicuous link that is located in either the

header or footer of the business's internet homepages. The term "conspicuous link" is explained in section 7003 and the term "homepage" is explicitly defined Civil Code section 1798.140, subdivision (p). The regulation benefits businesses by providing them explicit guidance regarding the placement of the link and benefits consumers so that they know where to look for the link. This subsection is also informed by comments received by the Agency during its preliminary rulemaking activities that consumers experience difficulty finding the link. (See Mahoney, *supra*, pp. 14-23; O'Connor, *supra*, p. 5.)

Subsection (d) operationalizes Civil Code section 1798.135, subdivision (a)(3), which gives the business discretion to use an alternative opt-out link that easily allows consumers to exercise their right to opt-out of sale/sharing and their right to limit. It clarifies that if a business uses an alternative opt-out link, it must comply with sections 7015 and still post a notice of right to limit by including it in its privacy policy. This section is necessary to explain how these different parts of the CCPA work together with these regulations.

Subsection (e) also implements Civil Code section 1798.135, subdivision (a)(2), regarding how to make the notice of right to limit reasonably accessible to consumers. It recognizes that there are businesses, primarily smaller ones, that may not have websites and whose interactions occur generally offline, and guides them on how they can provide the notice of right to opt-out. The subsection takes a performance-based approach for businesses that do not have a website, requiring them to establish another method for informing consumers of the right to limit that complies with section 7003. The subsection also clarifies that the notice shall be provided in the same manner in which the business collects the sensitive personal information that it uses or discloses for purposes other than those specified in section 7027, subsection (l). It takes a performance-based approach to adapt notices to the context in which the sensitive personal information is collected and provides illustrative examples. This is necessary to facilitate consumer awareness and the effectiveness of the notice.

Subsection (f) specifies the contents of the notice of right to limit, implementing Civil Code sections 1798.121, subdivision (a), and 1798.135, subdivision (a)(2). This subsection is necessary to clarify what information needs to be included in the notice. It benefits businesses by providing clear direction regarding what is expected of them and it benefits consumers in ensuring that this information is easily accessible to the consumer.

Subsection (g) implements Civil Code section 1798.185, subdivision (a)(6), clarifying when businesses do not need to provide a notice of right to limit. It explains that businesses that do not use or disclose sensitive personal information for purposes other than those specified in section 7027, subsection (l), do not need to provide a notice of right to limit as long as they explicitly state so in their privacy policy. This requirement is necessary to provide transparency for consumers, both by providing information in the privacy policy and by avoiding the potentially confusing posting of a notice of right to limit that would have no effect on the business's practices. It also promotes data governance and accountability by requiring a business to ensure that it complies with its posted policy.

Subsection (h) addresses a situation where a business that is exempt from posting a notice of right to limit later decides to use or disclose sensitive personal information for purposes other than those specified in section 7027, subsection (l), including information it had collected during

the period it did not post a notice of right to limit. Because using and disclosing a consumer's sensitive personal information without giving them notice and the opportunity to limit the business's use goes against the intent and purposes of the CCPA, the subsection requires the business to treat personal information collected from the consumer during the time it did not post a notice of right to limit as if the consumer had submitted a request to limit.

§ 7015. Alternative Opt-Out Link.

Civil Code section 1798.135, subdivision (a)(3), provides the business the option of posting a single, clearly labeled link on their website in lieu of posting the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links. The purpose of section 7015 is to articulate the purpose of this alternative opt-out link and to set forth rules and procedures businesses must follow regarding the form, content, and posting of the link. The regulation is necessary to ensure uniformity of the alternative opt-out link so that the link is easily accessible and understandable to consumers, including those with disabilities, and to ensure that the link easily allows the consumer to opt out of the sale and sharing of the consumer's personal information to limit the use or disclosure of the consumer's sensitive personal information as required by Civil Code section 1798.135, subdivision (a)(3).

Subsection (a) clarifies that the purpose of the alternative opt-out link is to permit businesses to post a single opt-out link rather than two separate links for ease of use by consumers and businesses. This subsection further clarifies how the alternative opt-out link is not only to inform the consumer about their rights, but to give the consumer the opportunity to exercise both their right to opt-out and right to limit. This regulation benefits both consumers and businesses by simplifying and streamlining information about opt-outs.

Subsection (b) sets forth requirements for the title and appearance of the alternative opt-out link. This subsection is necessary to create uniformity, to guide businesses who utilize this option, and to inform consumers on how to find the link. The use of the icon and the uniform title ("Your Privacy Choices" or "Your California Privacy Choices") are informed by academic studies that tested a number of different icon designs and taglines and found that the icon and title are among the best choices to effectively convey privacy choices. (See Cranor et al., Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA (February 4, 2020); Cranor et al., CCPA Opt-Out Icon Testing – Phase 2 (May 28, 2020).) The prescriptive placement of the link in the header or footer of the website is also informed by academic studies and benefits consumers and businesses by setting clear expectations and facilitating consumers' ability to find the link quickly. (*Ibid*.) The requirement that the link be conspicuous and the icon be the same size as other icons ensures that businesses will not bury or hide the link.

Subsection (c) clarifies the information that must be made available to the consumer via the alternative opt-out link. **Subsection (c)(2)** further clarifies that the alternative opt-out link shall direct users to a form or mechanism by which the consumer can submit their request to opt-out and request to limit. It requires that the method be easy for consumers to execute, require minimal steps, and comply with section 7004 preventing dark patterns. This is necessary to ensure that businesses provide the consumer the opportunity to submit their requests immediately

and that they do not incorporate any dark patterns that may subvert the consumer's intent of exercising their privacy rights.

§ 7016. Notice of Financial Incentive.

Existing subsection (a)(2)(A)-(D) has been deleted because the content has been moved to section 7003. **Subsection (b)** has been added to clarify that the notice of financial incentive shall comply with section 7003, subsections (a) and (b), which is where the content was moved. Repeating this requirement in subsection (b) is necessary for clarity so that all rules pertaining to notices of financial incentives are in one place.

Subsection (c) contains the information found in existing subsection (a)(2)(E). It has been revised to clarify that the notice may be given by providing a link that takes the consumer directly to the specific section of the business's privacy policy that contains the information required in subsection (d). This revision is necessary to take the consumer directly to the information required by the notice and prevent businesses from burying the material information. (See Mahoney, *supra*, pp. 14-23.)

Subsection (d)(5) has been revised to delete "financial incentive" to clarify that only price and service differences require a valuation of data. Other kinds of financial incentives where a monetary or specific benefit (*e.g.*, free t-shirt, gift card, etc.) is given for the exchange of data do not require a valuation because the consumer is aware of the value of the good and able to factor it into their decision of whether to provide the personal information. **Subsection (d)(5)(B)** has been revised to include more than one method for calculating the value of the data. This is necessary because there may be more than one way in which the business calculates the value of the consumer's data.

Changes without regulatory effect. The subsections have been renumbered.

Article 3. Business Practices for Handling Consumer Requests

§ 7020. Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know.

Civil Code section 1798.106 gives consumers the right to request a business to correct inaccurate personal information that it maintains about the consumer. Accordingly, this section has been revised to apply the existing methods for submitting requests to delete and requests to know to the new right to correct. This change is necessary to operationalize the right to correct.

Subsections (a) and (b) have been revised to align the regulation with the revised language of Civil Code section 1798.130, subdivision (a)(1). Previously, there were different requirements for the number of methods and the manner by which businesses were to receive requests to delete and request to know. The CPRA consolidated the requirements so that they are the same for requests to delete, requests to correct, and request to know. Accordingly, these subsections have been revised and consolidated to make the regulation easier to read and understandable for businesses and consumers.

Subsection (d) has been revised to add that the two-step process to make online requests to delete shall otherwise comply with section 7004. This is necessary to ensure that the two-step process is not implemented in a manner that would subvert the consumer's intention.

Changes without regulatory effect. Non-substantive changes (*e.g.*, reordering the type of CCPA requests) have been made throughout the section. The title has been amended to better reflect the content of the regulation. Reference citations have been amended.

§ 7021. Timelines for Responding to Requests to Delete, Requests to Correct, and Requests to Know.

Civil Code section 1798.106 gives consumers the right to request a business to correct inaccurate personal information that it maintains about the consumer. Accordingly, this section has been revised to apply the existing timelines for responding to requests to delete and requests to know to the new right to correct. This change is necessary to operationalize the right to correct.

Changes without regulatory effect. Non-substantive changes (*e.g.*, reordering the type of CCPA requests and grammatical changes) have been made throughout the section. The title has been amended to better reflect the content of the regulation. Reference citations have been amended.

§ 7022. Requests to Delete.

CPRA revisions to Civil Code section 1798.105 place additional obligations on businesses, service providers, contractors, and third parties with regard to a consumer's right to delete. Accordingly, this section has been revised to address and operationalize these additional obligations. The specific changes to the regulations are explained below.

Subsections (b)(2) and (3) require a business that receives a verifiable request to delete to notify any service providers or contractors to delete the consumer's personal information from their records, and to notify all third parties to whom the business has sold or shared the personal information to also delete the information unless this proves impossible or involves disproportionate effort. These revisions incorporate the requirements of Civil Code section 1798.105, subdivision (c). Incorporating these statutory requirements in the regulation are necessary for clarity so that all rules regarding how to respond to a consumer's request to delete are in one place. This benefits both businesses and consumers by making clear what a business must do and what a consumer can expect to be done in response to their request.

Subsection (b)(3) also requires a business that claims that notifying third parties is impossible or involves disproportionate effort to provide a detailed explanation. Requiring an explanation is necessary to prevent businesses from abusing this exception by simply stating it is impossible or involves disproportionate effort. An explanation would allow the consumer and those enforcing the statute to hold businesses accountable with relatively little cost to the business.

Subsection (c) has been added to make clear what is required of service providers and contractors who have been instructed by the business to comply with a consumer's request to delete. Civil Code section 1798.105, subdivision (c)(3), requires that the any service providers, contractors, or third parties who may have accessed personal information through the business's

service provider or contractor be notified. This regulation makes clear that a service provider or contractor instructed to comply with a consumer's request to delete is required to pass along that request to delete to its own service providers, contractors, and any third parties to whom it disclosed the consumer's personal information. This is necessary to effectuate a consumer's request to delete. **Subsection (c)(4)** also requires a service provider or contractor that claims compliance is impossible or involves disproportionate effort to provide a written explanation why the business cannot notify all third parties. This is necessary to prevent the abuse of the exception to comply with the request.

Subsection (d) has been revised to extend the guidance about how businesses handle personal information on archived or backup systems to service providers and contractors. Allowing service providers and contractors to delete the consumer's personal information on archived or backup systems at the time that they are accessed or used balances the interests of consumers with the potentially burdensome costs of deleting information from backup systems that may never be utilized.

Subsection (e) has been revised to extend the guidance about maintaining records of requests to delete to service providers, contractors, and third parties. This is necessary to ensure that the consumer's personal information remains deleted from the entity's records.

Subsection (f) has been revised to clarify that a business that denies a consumer's request to delete, in whole or in part, is required to explain to the consumer the basis of the denial, including the factual basis for contending that compliance proves impossible or involves disproportionate effect. **Subsection (f)(4)** has been added to make clear that the business is to inform service providers and contractors to delete the consumer's personal information that is not subject to the exception and to not use any retained personal information for any other purpose than provided for by the exception. These changes are necessary to operationalize the CPRA amendments to the CCPA and to make clear the obligations of a business in denying a consumer's request to delete. The subsection is also necessary to provide consumers transparency into the business's practices. It also prevents businesses from using statutory or regulatory exceptions to retain data for their own purposes in derogation of the consumer's request.

Subsection (g) has been revised to include "sharing" to align the regulation with the amended language of the statute.

Subsection (h) has been revised to require a business that provides consumers the ability to delete select categories of personal information, such as purchase history or browsing history, or voice recordings, to inform the consumer of their ability to do so and to direct them to how they can do so. This requirement is necessary to address situations in the marketplace where businesses that have the capability of allowing consumers to delete portions of their information only offer the consumer an all-or-nothing choice to engage with the business. Consumers are deterred from exercising their right and never directed to any other option to exercise granular control over their data. For example, an online retail platform that collects multiple categories of personal information across many different devices will only provide the consumer with the option of deleting their entire account even though they have the ability to give the consumer granular control over their personal information. This section requires the business to inform

consumers of their options to delete select categories of their personal information if that option is available.

This regulation balances the burden on the business with the benefit to the consumer. The burden is minimal on the business because it only requires that the business inform the consumer of the already existing controls but it addresses the coercive nature of giving consumers an all-or-nothing choice when another option is available.

Changes without regulatory effect. Non-substantive changes (*e.g.*, replacing request to opt-out with request to opt-out of sale, adjustments to capitalization of terms) have been made throughout the section. Subsections have been renumbered. Reference citations have been amended.

§ 7023. Requests to Correct.

Civil Code section 1798.106 gives consumers the right to request a business to correct inaccurate personal information that it maintains about the consumer. The purpose of section 7023 of these regulations is to operationalize the right to correct by setting forth the rules and procedures businesses must follow for submission and handling of requests to correct. The regulation is necessary because Civil Code section 1798.185, subdivision (a)(7), requires the Agency to establish rules and procedures to further the purposes of section 1798.106. Civil Code section 1798.140, subdivision (n), also requires the Agency to approve "designated methods for submitting requests" under the CCPA. This regulation will benefit both businesses and consumers by setting forth consistent processes for handling requests to correct, while also affording businesses flexibility to evaluate the nature of the contested information, its use and source, and its impact on the consumer when determining how to appropriately respond to a request to correct.

Subsection (a) makes operational Civil Code section 1798.106, subdivision (c), which requires that when a business receives a verifiable consumer request to correct inaccurate personal information, the business shall use commercially reasonable efforts to correct. If the request to correct is not verifiable, the business is not obligated to correct, but it must inform the consumer of the reason for denial of the request. This regulation benefits both businesses and consumers by minimizing use of the correction requests for fraudulent or improper purposes, and will further benefit consumers by informing them of the reason their request was denied. This provision further clarifies that requests to correct are subject to the same verification process as requests to delete and requests to know, which benefits businesses by promoting consistency and efficiency in handling requests.

Subsection (b) explains that businesses are to consider the totality of the circumstances in determining whether the personal information at issue is inaccurate and warrants correction. A business may deny the consumer's request to correct if it determines that the contested personal information is more likely than not accurate based on the totality of the circumstances.
Subsection (b)(1) explains that the totality of circumstances includes looking at the nature of the information at issue (*e.g.*, whether it is objective, subjective, unstructured, sensitive, etc.), how the business obtained it, and any documentation relating to its accuracy of the information whether provided by the consumer, the business, or another source. This standard is informed by

public comments that the Agency received during preliminary rulemaking activities. The Agency received a wide variety of comments on the scope of the right to correct. For example, some commentators suggested exempting all subjective information and information obtained from a third party from the obligation to correct, while others specifically urged against such exemptions. The totality of the circumstances test avoids bright-line rules exempting whole categories of information and instead allows businesses to weigh the various attributes of the information collectively. Where contested information is objective or sensitive in nature, it is of utmost importance that businesses determine whether the information is accurate, and if not, comply with the request to correct. In contrast, where contested information is subjective in nature or recorded in an unstructured form, it may be more difficult for the business to reach a determination of accuracy. The source of the information may also be indicative of its accuracy and should be a factor that businesses consider.

Subsection (b)(2) clarifies that where a business is not the source of the contested information and cannot verify its accuracy, the consumer's assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate. This approach minimizes the administrative burden on consumers, consistent with Civil Code section 1798.185, subdivision (a)(7), and also benefits businesses by instructing them how to proceed in the absence of any documentation of either accuracy or inaccuracy, apart from the fact of the consumer's request. In contrast, where a business does have documentation confirming the accuracy of contested information, the burden of proving its inaccuracy may rest with the consumer. This issue is further addressed in subsection (d).

Subsection (c) sets forth the steps a business must take to comply with a verified request to correct. In addition to correcting the information on its existing systems, the business must instruct any service providers to correct the information in their systems as well, and both the business and any service providers must take steps to ensure that the information remains corrected going forward. Failure to take these steps could result in continued use and/or dissemination of inaccurate information, which would harm consumers and undermine the right to correct. **Subsections (c)(1) and (2)** are illustrative examples of how to comply with subsection (c), with subsection (c)(2) further clarifying that a business is obligated to correct information stored in a backup or archived system only if that system comes into active use. This provision is responsive to public comments submitted to the Attorney General's Office when it operationalized the request to delete. It is intended to minimize the burden on the business of complying with requests to correct, and is consistent with regulations pertaining to requests to delete. (See Cal. Code Regs., tit. 11, § 7022, subd. (e).)

Subsection (d) provides guidance regarding how businesses and consumers are to use documentation to determine the accuracy or inaccuracy of contested information. **Subsection (d)(1)** requires businesses to accept, review, and consider any documentation provided by the consumer even if the business does not explicitly require documentation. This provision benefits consumers by ensuring that they have a fair opportunity to present evidence that contested information is inaccurate. It was drafted in response to public comments noting that in other contexts, including in the consumer credit-reporting industry, consumer requests to correct do not consistently receive meaningful consideration. However, to avoid disproportionate burden on business, this provision should be read in combination with subsection (h) such that a

business is not obligated to continue to accept or review documentation once it has determined a request is fraudulent or abusive.

Subsection (d)(2) permits, but does not mandate, a business to require documentation from the consumer to rebut its own documentation that the personal information is accurate. It also sets forth factors that the business shall consider in determining the necessity of the documentation requested and which way those factors sway. The subsection explains that the business should consider the nature of the personal information, the nature of the documentation upon which the business considers the personal information to be accurate, the purpose for which the business uses the personal information, and the impact on the consumer. By not requiring businesses to request documentation from consumers in all instances, this provision aims to reduce the burden on businesses and consumers and to provide greater flexibility to businesses. For example, if the purpose for which the business uses the personal information is not that significant, the impact to the consumer is high, and the documentation that the business has is not that reliable, the business may decide to comply with the request without asking the consumer to provide any documentation. This subsection is informed by public comments submitted to the Agency during preliminary rulemaking activities regarding the nature and degree of evidence that should be required.

Subsection (d)(3) and (4) addresses businesses' obligations with respect to documentation submitted by consumers. These provisions clarify that documentation submitted in connection with a request to correct shall be used and maintained only for that purpose and to comply with record-keeping obligations under section 7101, and shall be protected by reasonable security measures in accordance with Civil Code section 1798.81.5. These provisions are necessary to protect consumers' privacy and mitigate the risk associated with making requests to correct, insofar as such requests may require consumers to share even more information with the business than it already maintains.

Subsection (e) gives businesses the option to delete rather than correct contested personal information if doing so would not result in additional or continued harm to the consumer, or if the consumer consents to deletion instead of correction. This subsection is informed by public comments submitted to the Agency during preliminary rulemaking activities, some of which urged giving businesses the option to delete rather than correct contested information, and others noting that deletion is not an appropriate substitution for correction in certain instances (for example, where deleting rather than correcting an entry could negatively affect a consumer's creditworthiness). This subsection aims to balance competing interests while minimizing burdens associated with the right to correct on both consumers and businesses, and recognizes that where deleting contested information is not likely to impact the consumer, a "commercially reasonable" method for handling the request under Civil Code section 1798.106, subdivision (c), may include deleting the contested information. This subsection further aims to prevent deletion from improperly being used as a substitute for correction. If a business does not have a consumer's consent to delete the information rather than correct it, the business should communicate with the consumer to determine whether and how the contested information is negatively affecting the consumer. The list of potential negative impacts on the consumer set forth in this subsection is not intended to be exhaustive.

Subsection (f) addresses how businesses must respond to requests to correct and makes clear that businesses must in all cases inform a consumer of the outcome of their request. Subsections (f)(1) through (5) set forth the particular information a business must provide if it denies a consumer's request. **Subsection (f)(1)** requires businesses to inform consumers of the reasons for denial, giving consumers transparency into the business's process for handling their request and providing them with a potential basis for future communication with the business or other businesses regarding the denial. Consumers and businesses alike benefit from transparency and consistency in the process of granting or denying requests. **Subsection (f)(1)** further acknowledges that a request may be denied if compliance is impossible or would require disproportionate effort, thus putting into operation Civil Code section 1798.106, subdivision (a), which provides that the scope of the right to correct takes into account the nature of the personal information at issue and the business's purpose for processing it. Where a request is denied because compliance is impossible or would require disproportionate effort, **subsection (f)(2)** requires businesses to provide a detailed explanation to promote transparency and consumer understanding. Requiring an explanation is also necessary to prevent businesses from abusing this exception by simply stating it is impossible or involves disproportionate effort. An explanation would allow the consumer and those enforcing the statute to hold businesses accountable with relatively little cost to the business.

When a consumer's request has been denied, **subsection (f)(3)** requires a business to give the consumer the option of requesting that the company maintain a notation in its system regarding the denied request, and that the business share this notation with any third party with whom it discloses, shares, or sells the contested information. The Agency received conflicting public comments regarding whether consumers should be permitted to provide an addendum to businesses about their request, and whether businesses should be required to accept such an addendum even if the request is denied. This subsection aims to balance those conflicting comments by requiring businesses to maintain only a notation, and only at the consumer's request. This requirement is further intended to prevent the proliferation of potentially inaccurate personal information, and acknowledges that in some instances, a consumer may continue to believe contested information is inaccurate even though the business is unable to correct or delete the information or has determined that it is most likely accurate. Consistent with subsection (h), a business is not obligated to make or disclose this notation if it determines that the consumer's request was fraudulent or abusive. This exception aims to minimize the burden on the business of compliance, and to protect consumers from potential abuses of the right to correct such as attempted identity theft.

Subsection (f)(4) pertains specifically to denials of a consumer's request to correct personal information concerning their health. This provision is necessary to operationalize Civil Code section 1798.185, subdivision (a)(8)(D). It requires businesses, when they deny such a request, to inform consumers of their right to submit a written addendum as described in section 1798.185, subdivision (a)(8)(D). It further sets forth businesses' obligations to maintain and disclose such information. Like the provision in subsection (f)(3), this provision is intended to prevent the proliferation of potentially inaccurate health information.

Subsection (f)(5) requires a business to inform the consumer of their right to delete the contested personal information, if that option is available to them. This regulation is necessary to ensure that consumers are aware of their right to delete personal information as an alternative to

correction. This provision is consistent with section 7022, subsection (g), which requires a business to inform a consumer of their right to opt-out of sale/sharing of their personal information if the consumer has made a request to delete which the business has denied. This benefits consumers by informing them of other rights that are applicable to them that may address their concern.

Subsection (g) pertains to repeat requests to correct and aims to minimize the burden on businesses by allowing them to reject any subsequent request to correct, if within the preceding six months the consumer already made a request to correct the same piece of information and if that prior request was denied. It further provides that, if the subsequent request is accompanied by new or additional documentation showing that the contested information is inaccurate, the business may not summarily deny the subsequent request. By directing businesses to consider new or additional documentation, this provision avoids imposing overly stringent limitations on consumers, who may need more than one exchange with a business to understand what type of documentation will best support a request to correct.

Subsection (h) allows businesses to deny requests to correct that it has reason to believe are fraudulent or abusive, as is consistent with regulations pertaining to requests to opt-out of sale/sharing (section 7026, subsection (e)) and requests to limit (section 7027, subsection (f)). In such cases, requests may be denied if the business has a good-faith, reasonable, and documented basis for determining that the request is fraudulent or abusive. This subsection responds to public comments about potential misuse of the correction process submitted to the Agency during preliminary rulemaking activities, and is necessary to prevent harm to both businesses and consumers. This subsection imposes a minimal burden on businesses while ensuring that legitimate requests are not denied as potentially fraudulent or abusive without the consumer having the opportunity to learn of the reason for denial.

Subsection (i) clarifies a business's obligations when it is not the source of the contested information, *i.e.*, when it acquired the contested information from another business or provider. In this situation, the business must handle the request to correct, consistent with these regulations, and must also inform the consumer of the source of the contested information in order to allow the consumer to make an informed decision about whether to make a separate request to that source. This provision reflects a number of public comments submitted to the Agency during preliminary rulemaking activities, some of which suggested that a business should not be required to correct information if it was obtained from another source, and that the business should instead be permitted to direct the consumer to the source. However, this approach would frustrate the right to correct and unduly burden consumers by putting the onus on consumers to make multiple requests until they reach the initial source of the data. This process could take several months and would not address the immediate harm to the consumer by the business using inaccurate information. This approach would likely also cause consumer confusion, as personal information may have been handled by any number of businesses with whom the consumer may be unfamiliar.

Under **subsection (j)**, consumers who have made a request to correct may ask the business, following disposition of the request, to share with them a list of all of the pieces of information the business maintains about the consumer; if such a request is made, the business must comply. This subsection allows consumers to verify independently that the contested information was in

fact corrected, or if applicable, deleted as an alternative to correction. This subsection further makes clear that this request following disposition of a request to correct does not count as one of the two requests to know with which businesses are obligated to respond within a 12-month period under Civil Code section 1798.130, subdivision (b). This subsection is in response to public comments submitted to the Agency during preliminary rulemaking activities observing that the twice-yearly limit on businesses' obligations to respond to requests to know could have unintended consequences on consumers' ability to exercise the right to correct.

§ 7024. Requests to Know.

Subsection (h) has been revised to align the regulation with the revised language of the statute. Civil Code section 1798.130, subdivision (a)(2)(B), requires a business to respond to a request to know with specific pieces of personal information that the business has collected about the consumer for the 12-month period preceding the business's receipt of the request and beyond pursuant to a regulation. In accordance with Civil Code section, subdivision (a)(3)(A), the specific pieces of personal information shall include personal information that the business's service providers and contractors obtained as a result of providing services to the business. This subsection is necessary to operationalize this provision. It requires that a business provide all personal information it collected and maintains about the consumer on or after January 1, 2022 unless doing so proves impossible or involves disproportionate effort. If a business claims that providing information beyond the 12-month period preceding receipt of the request is impossible or involves disproportionate effort, the business must provide a detailed explanation. Requiring an explanation is necessary to prevent businesses from abusing this exception by simply stating it is impossible or involves disproportionate effort. An explanation would allow the consumer and those enforcing the statute to hold businesses accountable with relatively little cost to the business.

Subsection (i) has been added because the CPRA amended Civil Code section 1798.130 to add subdivision (a)(3)(A), which requires service providers and contractors to provide assistance to businesses in responding to requires to know. This subsection is necessary to clarify the requirements of a service provider and contractor when a consumer makes a request to know of the business it is servicing. It provides them with clear guidance about what is required of them. Incorporating this statutory requirement in the regulation is necessary for clarity so that all rules regarding how to respond to a consumer's request to know are in one place.

Subsection (k) has been revised to align the regulation with the revised language of the statute.

Changes without regulatory effect. Subsections have been renumbered. Reference citations have been amended.

§ 7025. Opt-Out Preference Signal.

The CCPA required that the Attorney General promulgate regulations to facilitate the submission of a request to opt-out of the sale of personal information. To promote innovation and ease of use for consumers making requests, the CCPA regulations require a business to treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, as a valid request to opt-out, so long as that control clearly communicates or

signals that the consumer intends to opt-out of the sale of personal information. The CPRA's amendments to Civil Code section 1798.120 expanded the consumer's right to opt-out of the sale of personal information to include sharing personal information for cross-context behavioral advertising, whether or not for monetary or other valuable consideration. Corresponding amendments to Civil Code section 1798.135 expanded and refined how a consumer exercises these rights; for example, section 1798.185, subdivision (a)(19), requires the promulgation of regulations on "an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer's intent to opt-out of the sale or sharing of the consumer's personal information...." Civil Code section 1798.185, subdivisions (a)(19) and (20), set forth factors the Agency should consider in drafting requirements for the opt-out preference signal and how a business processes consumer requests received via the opt-out preference signal for stopping the sale and sharing of personal information. In drafting this regulation, the Agency considered each subdivision of Civil Code section 1798.185, subdivision (a)(19) and (20). The proposed language of these regulations, as well as the intentional omission of language, reflects these considerations.

In an effort to prioritize drafting regulations that operationalize and assist in the immediate implementation of the law, these regulations only address the opt-out preference signal as an expression of a consumer's right to stop the sale and sharing of personal information. These regulations do not include limiting the use of sensitive personal information, or how a consumer may express opt-in to the sale or sharing of personal information if the consumer is between the ages of 13 and 16 years or how a consumer's parent or guardian may express opt-in if the consumer is less than 13 years of age. (See Civ. Code, § 1798.185, subds. (a)(19)(B)-(C).) The Agency did not address these areas in an effort to reduce the burden on businesses to respond to differing signals, and because no mechanism currently exists to communicate the expression of these rights. It was also to prioritize the Agency's limited resources in promulgating regulations and to allow innovation to occur in new areas required by the CPRA amendments.

Subsection (a) affirms the purpose of the opt-out preference signal. This regulation is necessary to provide clarity on the intent and goal of the opt-out preference signal, which is to facilitate a specific, comprehensive expression of a consumer exercising their right to stop the sale and sharing of their personal information.

Subsection (b) sets forth the requirements for the opt-out preference signal sent by a platform, technology, or mechanism, per Civil Code section 1798.185, subdivision (a)(19). This regulation is necessary to further operationalize the opt-out preference signal and to provide the requirements and technical specifications for an opt-out preference signal that must be recognized as a valid request to opt-out of sale/sharing. **Subsection (b)(1)** clarifies that the opt-out preference signal must be in a format commonly used by businesses and provides an example of a format. The regulation is a performative standard but provides additional guidance for a specification modeled after an existing technical standard recognized by the World Wide Web consortium, which relies on a common mechanism supported by web browsers and internet websites: a header field in an HTTP request. Accordingly, this subsection builds on an existing specification and designed mechanism that some businesses have already implemented to process a consumer's request to opt-out via a technical mechanism that has emerged since the finalization of the CCPA regulations, the Global Privacy Control, which communicates a person's "do not sell" request on behalf of the person or device. **Subsection (b)(1)** is necessary

to clarify that businesses are not required to process requests that are in an unusable or unfamiliar format.

Subsection (b)(2) sets forth that a platform, technology, or mechanism must make clear to the consumer what the signal's effect will be and explains that this can be done through the signal's configuration or public disclosures about the signal. This subsection builds on existing section 7026, subsection (c)(1), which requires user-enabled global privacy controls to clearly communicate or signal that a consumer intends to opt-out of the sale of their personal information. By specifying that the effect of the signal can be explained either in the signal's configuration or public disclosures, the regulation allows for situations where consumers affirmatively choose products or services that include built-in privacy-protective features because these products or services are designed with privacy in mind. The selection of privacy-by-design products or services is an affirmative step and sufficient to express the consumer's intent to opt out of the sale and sharing of personal information. Additional steps are not necessary, even if this means that a consumer relies on a privacy-by-default opt-out mechanism that is built into a platform, technology, or mechanism. In doing so, the regulation implements Civil Code section 1798.185, subdivisions (a)(19)(A)(ii) and (iii), which state that an opt-out preference signal should clearly represent a consumer's intent, be free of defaults constraining or presupposing intent, be consumer-friendly, be clearly described, and be easy for the consumer to use. This regulation is necessary to clarify how a consumer demonstrates their intent to opt-out of the sale or sharing of their personal information through the use of an opt-out preference signal, including through the use of privacy-by-design products.

The subsection also states that the platform, technology, or mechanism need not explicitly reference California, to allow for flexible innovation and for opt-out preference signals to comply with multiple jurisdictions' requirements, especially as other states have passed privacy legislation that provides for a consumer right to opt-out via universal opt-out mechanisms. Requiring that the signal explicitly reference California would be burdensome to businesses because it would reduce the interoperability of a universal signal and require state-specific implementation, which is unnecessary given that the sale or sharing of personal information is not unique to any individual State or jurisdiction. Furthermore, binding the signal to a specific State is not necessary because it is merely legal in nature and not required for functionality. If a business treats consumers differently depending on the state that they reside in, they can seek this information in response to the signal. (See subsection (c) below.) The signal itself is not required to include this information. This regulation is necessary to ensure that opt-out preference signals recognized in California are compatible with signals recognized in other jurisdictions, which is in line with the purpose and intent of the CCPA. (Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3(C)(8).)

Subsection (c) provides the requirements for how a business responds to an opt-out preference signal. This regulation is necessary to operationalize the opt-out preference signal as required by Civil Code section 1798.135, subdivision (e), and to provide clarity regarding a business's obligations in responding to an opt-out preference signal. This regulation is also necessary because without it, businesses may reject or ignore tools that empower consumers to effectuate their opt-out right. (See OAL File No. Z-2019-1001-05, OAL Matter No. 2020-0603-03, Final Statement of Reasons for section 999.315, subsection (d)(2), p. 37, available at https://oag.ca.gov/privacy/ccpa/regs.)

Subsection (c)(1) restates existing section 7026, subsection (c)'s, language that an opt-out preference signal (formerly referred to as a user-enabled global privacy control) shall be treated as a valid request to opt-out submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer. This regulation is necessary to align the regulation with the revised language of the statute that uses the term "opt-out preference signal" and extends requests to opt-out to both the sale and sharing of personal information. This regulation is also necessary to address a common misinterpretation of Civil Code section 1798.135, subdivisions (b)(3) and (e), that complying with an opt-out preference signal is optional for the business. Not so. Civil Code section 1798.135 gives the business a choice between (1) posting the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" link, or the other alternative Opt-Out link and (2) processing the opt-out preference signal in a frictionless manner in accordance with the regulations. (See Civ. Code, § 1798.135, subd. (b)(1) (referencing technical specifications described in Civil Code section 1798.185, subdivision (a)(20), about a frictionless processing of the signal, and not subdivision (a)(19), regarding the opt-out preference signal generally.) Whether or not the business posts the opt-out links, the CPRA amendments to the CCPA require a business to always comply with an opt-out preference signal.

Subsection (c)(2) implements Civil Code section 1798.185, subdivision (a)(19)(A)(ii), which states that an opt-out preference should not require the consumer to provide additional information beyond what is necessary to send the signal. The regulation acknowledges, however, that a business may need additional information from the consumer to apply the request to opt-out of sale/sharing to offline sales, and thus, permits the business to provide consumers with the option to provide additional information if it will help facilitate the request. This regulation is necessary to address the realities of the way in which businesses sell and share personal information and the technical limitations of the opt-out preference signal. It balances the consumer's privacy interest with a business's ability to operationalize and process the opt-out. It also limits the further downstream use of consumer personal information with a purpose limitation that prevents a business from using, disclosing, or retaining any information used in processing the opt-out request. This regulation is necessary to strengthen consumer privacy and is consistent with the purpose and intent of the CCPA to minimize the collection, use, and disclosure of personal information to only that which is necessary to accomplish the purpose for which it was collected, used, and shared. (Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3(B)(2)-(3).)

Subsection (c)(3) provides businesses with clarity and guidance for what it may do if the opt-out preference signal conflicts with the consumer's business-specific privacy setting that permits selling or sharing of personal information. It requires the business to default to processing the opt-out request but permits the business to notify the consumer of the conflict and provide the consumer with an opportunity to consent to the sale or sharing of their personal information in accordance with section 7004. Repeating this requirement to comply with section 7004 is necessary for clarity so that all the requirements of responding to an opt-out preference signal are in one place. Subsection (c)(3) further clarifies that the opt-out preference signal should be processed as the expression of a consumer's choice in the first instance, but that if a consumer subsequently consents to the sale or sharing of their personal information, the business may ignore the opt-out preference signal for as long as the consumer is known to the business. The sequencing on which choice by the consumer controls takes into consideration the fact that the

general default status for consumers is that they are opted into the sale/sharing of personal information, as well as Civil Code section 1798.120, which provides that a consumer has the right to opt-out of sale/sharing "at any time." As illustrated in the example in subsection (c)(7)(B), the first instance that an opt-out preference signal is detected should override the consumer's existing privacy setting because the consumer can opt-out at any time. If the consumer subsequently consents to the sale of personal information, the business is provided specific tailored instruction from the consumer that the signal is not meant to apply to that business, operationalizing a selective consent mechanism for the consumer. This regulation is necessary to implement Civil Code section 1798.185, subdivision (a)(19)(A)(v), which states that consumers should have a mechanism where they can selectively consent to a business's sale or sharing of their personal information without affecting the consumer's preferences with respect to other businesses or disabling the opt-out preference signal globally.

Subsection (c)(4) provides businesses with guidance for what they may do if the opt-out preference signal conflicts with the consumer's participation in the business's financial incentive program that requires consent to selling or sharing of personal information. It requires the business to notify the consumer of the impact of the opt-out preference signal on the consumer's participation, and ask the consumer if they intend to withdraw from the financial incentive program. This regulation provides both the business and consumer with the ability to clarify the expression of the opt-out preference signal. The sequencing on which choice by the consumer controls takes into consideration the fact that Civil Code section 1798.125, subdivision (b), requires the consumer's voluntary opt-in consent to participate in a financial incentive program, whereby the consumer receives some value in exchange for the sale or sharing of their personal information. Accordingly, greater deference is placed on the consumer's preexisting choice as it relates to a financial incentive. The business may ignore the signal unless the consumer confirms otherwise. This regulation is necessary to implement Civil Code section 1798.185, subdivision (a)(19)(A)(v), which states that consumers should have a mechanism where they can selectively consent to a business's sale or sharing of their personal information without affecting the consumer's preferences with respect to other businesses or disabling the opt-out preference signal globally, and to clarify a business's obligations in responding to an opt-out preference signal when it relates to a financial incentive program.

Subsection (c)(5) clarifies that a business shall not interpret the absence of an opt-out preference signal after previously receiving an opt-out preference signal as consent to opt-in to the sale or sharing of personal information. This regulation is necessary to dispel any potential misinterpretation by businesses that the absence of an opt-out preference signal means the consumer no longer is exercising their right to opt-out of sale/sharing. For example, a consumer may log in from a different device that does support an opt-out preference signal. Moreover, the method by which consumers consent to the sale or sharing of their personal information must comply with section 7004. The mere absence of an opt-out preference signal is not sufficient to demonstrate consent to opt-in to the sale or sharing of personal information. This regulation is in line with the purpose and intent of the law to strengthen consumer privacy and place consumers on more equal footing with businesses to direct businesses to stop selling or sharing their data. (Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 2(H).) The regulation also benefits both consumers and businesses by setting a clear boundary line for what constitutes consent in interpreting the opt-out preference signal, building on other regulations, including the proposed language in section 7004.

Subsection (c)(6) requires a business to display whether a consumer's opt-out preference signal has been accepted, and provides exemplar language for how a business can communicate this information to the consumer. This regulation is necessary to avoid confusion for consumers on their opt-out state while using a business's website or online services; it will inform the consumer if they are opted out and that the business has processed the opt-out preference signal. It also gives consumers the ability to know that the signal is being consistently applied across the different websites they visit and engenders confidence in the opt-out preference signal preventing the sale or sharing of their personal information. This regulation implements Civil Code section 1798.185, subdivision (a)(19)(A)(ii), which states that the opt-out preference signal should be consumer-friendly, clearly described, and easy for the consumer to use.

Subsection (c)(7) provides illustrative examples for how business should respond to the opt-out preference signal. This subsection benefits both businesses and consumers by providing clear examples of what consumers should expect when they signal their right to opt-out via the opt-out preference signal and how businesses may comply with the regulation.

Subsection (d) makes explicit that neither the business nor a platform, technology, or mechanism shall use, disclose, or retain personal information collected from the consumer in connection with the sending or processing the request to opt-out. Subsection (d) incorporates the requirements of Civil Code section 1798.135, subdivision (c)(6), which explicitly prohibits the use of any personal information collected from the consumer in connection with the submission of the consumer's opt-out request for any purpose other than complying with the opt-out request. Incorporating this statutory requirement in the regulation is necessary to clarify that this requirement also applies to opt-out preference signals. This regulation also implements Civil Code section 1798.185, subdivision (a)(19)(i), which states that the opt-out preference signal should ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business. By applying the prohibition of using personal information collected in connection with an opt-out request for any other purpose to both the business and to the platform, technology, or mechanism that sends the opt-out preference signal, this regulation prevents creators of opt-out preference signals from having any unfair advantage over other businesses.

This regulation is also necessary to strengthen consumer privacy and is consistent with the CPRA's amendments that limit how complying entities use consumer personal information. (Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3(B)(2)-(3).) This subsection benefits both businesses and consumers because it sets forth clear guidance to prevent the conversion of personal information into a use that the consumer would not reasonably expect.

Subsection (e) clarifies the language in Civil Code section 1798.135, subdivision (b), to definitively state that a business that sells or shares personal information is always required to process a consumer's request via an opt-out preference signal. This regulation is necessary to respond to incorrect interpretations in the marketplace that complying with an opt-out preference is optional for the business. The CPRA amendments to Civil Code section 1798.135 never rendered the opt-out preference signal as optional; rather, the "option" presented in the statute's text is between providing a frictionless response to the opt-out preference signal or a non-frictionless response to the opt-out preference signal. Specifically, Civil Code section 1798.135 sets forth the requirement that a business post new links to their homepage: (1) two links, titled

"Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal information," or (2) a single, clearly labeled link on their homepage that easily allows consumers to exercise these rights. If a business does not want to post the identified links, it can instead respond to the opt-out preference signal in a frictionless manner in accordance with these regulations. (See Civ. Code, § 1798.135, subd. (b)(1), citing to Civ. Code, § 1798.185, subd. (a)(20).) The explicit reference to Civil Code section 1798.185, subdivision (a)(20), within Civil Code section 1798.135, subdivision (b)(1), indicates that the choice between posting and not posting certain links depends on the way in which the business processes an opt-out preference signal, specifically whether the business processes the signal in a frictionless manner. To the extent that businesses are confused by the language in Civil Code section 1798.135, subdivision (e), which references subdivision (b)(1), these regulations make clear that businesses must comply with an opt-out preference signal regardless of whether or not they post the identified opt-out links.

Subsection (f) sets forth the minimum requirements for businesses who process the opt-out preference signal in a frictionless manner. This regulation is necessary to operationalize Civil Code section 1798.135, subdivision (b), in accordance with Civil Code section 1798.185, subdivision (a)(20). It provides clarity to businesses seeking to operationalize their response to an opt-out preference signal in a frictionless manner. It reiterates Civil Code section 1798.185, subdivision (a)(20), which prohibits a business from responding in a manner that charges the consumer a fee, makes products or services offered by the business not function properly or fully for the consumer, or displays a notification or pop-up in response to the signal. Including these statutory requirements in the regulation is necessary for clarity because it consolidates all the requirements regarding the frictionless response in one place. **Subsection (f)(1)**'s prohibition on charging a fee or requiring any valuable consideration in response to the opt-out preference signal clarifies that a business that offers a financial incentive in response to an opt-out preference signal would not be responding in a frictionless manner. **Subsection (f)(2)** explains what it means for a business to change the consumer's experience with a product or service offered by the business. **Subsection (f)(3)** clarifies that a notification or pop-up in response to the signal would include any text, graphic, animation, sound, video, or interstitial content. The subsection also clarifies that a display of the consumer's opt-out status would not be in violation of this requirement. While Civil Code section 1798.185, subdivision (a)(20), also states that the business cannot respond in a manner that intentionally degrades the functionality of the consumer's experience or attempts to coerce the consumer to opt-in to the sale or sharing of their personal information, the Agency determined that it is not necessary to include these requirements in the regulation because responding in that manner would not be allowed under any circumstance.

Subsection (g) sets forth the requirements for a business that is not required to post the "Do Not Sell My or Share My Personal Information" link or the alternative opt-out link. This subsection is necessary to operationalize Civil Code section 1798.135, subdivision (b)(1). It explains that a business that does not provide the required links must process opt-out preference signals in a frictionless manner, provide specific disclosures in its privacy policy so that consumers understand how they can exercise their rights, and allow the opt-out preference signal to fully effectuate the consumer's request to opt-out. The regulation further clarifies through examples that businesses that sell or share personal information offline cannot fall within the exception provided in Civil Code section 1798.135, subdivision (b)(1), because the opt-out preference

signal would not fully effectuate the consumer's request to opt-out of sale/sharing. **Subsection (g)** is necessary to ensure that consumers still have a means of understanding and easily exercising their right to opt-out of sale/share when a business sells or shares personal information in an offline manner. Giving businesses the option of not posting the "Do Not Sell My Personal Information" link or alternative opt-out when the opt-out preference signal does not fully address all instances in which a business sells or shares consumer personal information would give consumers a false understanding that their opt-out request is fully processed. Moreover, it would allow businesses to bury their method for opting out of the offline sale and sharing of personal information in their privacy policies. Notably, subsection (g) only gives businesses the option of not posting the "Do Not Sell My Personal Information" link because the opt-out preference signal only addresses the right to opt-out of sale/sharing at this time. In an effort to prioritize drafting regulations that operationalize and assist in the immediate implementation of the law, reduce the cost on businesses to respond to differing signals, and because no mechanism currently exists to communicate the expression of the right to limit, the Agency did not apply the opt-out preference signal to the right to limit. Accordingly, businesses that use or disclose sensitive personal information for purposes other than those set forth in section 7027, subsection (l), must still post the "Limit the Use of My Sensitive Personal Information" even if it processes an opt-out preference signal in a frictionless manner.

§ 7026. Requests to Opt-Out of Sale/Sharing

The CPRA's amendment to Civil Code section 1798.120 extended the right of a consumer to opt out of a business's sale of personal information to the business's sharing of personal information, as that term is defined in Civil Code section 1798.140, subdivision (ah). The regulation is necessary because Civil Code section 1798.185, subdivision (a)(4), requires the Agency to establish rules and procedures to facilitate and govern the submission of a request by a consumer to opt-out of the sale or sharing of personal information and to govern business compliance with a consumer's request to opt-out of the sale/sharing. Civil Code section 1798.140, subdivision (i), also requires the Agency to approve "designated methods for submitting requests" under the CCPA. Accordingly, section 7026 has been revised to operationalize the extension of the right to opt-out to include opting out of the sharing of personal information. Subsections have also been reorganized to make the regulation easier to read and understandable for businesses and consumers. The specific changes are explained below.

Subsection (a) has been revised to align the regulation with the revised language of the statute and to address new provisions regarding the different opt-opt links and the opt-out preference signal. It consolidates existing subsections (b) and (c) and sets forth the performative standard at the beginning of the subsection and provides the illustrative examples in subsections (a)(1) through (4). It still requires that the business provide two or more designated methods for submitting requests to opt-out of sale/sharing and that the business consider various factors in determining which methods to offer to consumers. At least one method must still reflect the manner in which the business primarily interacts with the consumer. This subsection is necessary because Civil Code section 1798.135 only identifies how businesses with an online presence are to comply with section 1798.120. It does not address other types of business situations. This subsection ensures that businesses do not pick obscure methods for submitting requests as a way of discouraging consumers from exercising their right.

Subsection (a)(1) explains that a business that collects personal information online must allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and through an interactive form accessible via the "Do Not Sell My Personal Information" link, alternative opt-out link, or the business's privacy policy. This subsection is necessary to clarify that a business selling or sharing personal information online must honor an opt-out preference signal because public comments during preliminary rulemaking activities informed the Agency that there was confusion regarding the meaning of existing language in the regulation.

Subsection (a)(2) and (3) provides examples for different contexts, such as when a business collects personal information both in person and online. **Subsection (a)(4)** addresses how a notification regarding cookies, such as a cookie banner or cookie controls, is not, by itself, an acceptable manner in which to opt-out of the sale and sharing of personal information because cookies concern the collection of personal information and not the sale or sharing of personal information. This subsection is necessary to address observations in the marketplace of how businesses are inappropriately using such a method and to clear up any confusion regarding this issue.

Subsection (b) is existing subsection (h). Much of the existing subsection has been deleted because it was incorporated into section 7004 of these regulations. **Subsection (b)** now incorporates a reference to section 7004. Repeating this requirement in subsection (b) is necessary for clarity so that all rules pertaining to requests to opt-out of sale/sharing are in one place.

Subsection (c) prohibits a business from requiring a consumer to create an account or provide additional information beyond what is necessary to direct the business to stop the sale or sharing of the consumer's personal information in accordance with Civil Code section 1798.135, subdivision (c)(1). Including this statutory requirement in the regulation is necessary for clarity because it consolidates all the requirements regarding requests to opt-out of the sale/sharing into one place. Moreover, seeking additional personal information may deter or encumber consumers seeking to exercise their right to opt-out in violation of section 7004. This regulation applies the internationally recognized fair information practice principle ("FIPP") of data minimization, *i.e.*, to only collect data directly relevant and necessary to accomplish the specified purpose. It does not impose a prescriptive restriction on required data points, but rather, places a performance-based standard on businesses to only require personal information that is necessary to implement the request. If a business cannot explain why the personal information is necessary, it should not require it from consumers. This regulation is necessary to facilitate the law, but it was also included in existing section 7027, subsection (h)(4), because the Attorney General had seen and consumer studies had documented significant abuse by businesses in this area. (See Mahoney, *supra*, pp. 26-30, 33-34.)

Subsection (d) prohibits a business from requiring a verifiable consumer request for a request to opt-out of sale/sharing. **Subsection (d)** is consistent with section 7027, subsection (e), which likewise clarifies that businesses are prohibited from requiring requests to limit to be verifiable consumer requests. The CCPA does not require requests to opt-out of sale/sharing and requests to limit to be verifiable consumer requests because the potential harm to consumers from non-verified requests is minimal. This subsection is in response to observations in the marketplace and comments received by the Agency during preliminary rulemaking activities that some

businesses have misused the verifiable request process to impede consumers' exercise of their right to opt-out of sale. This subsection recognizes that, in some cases, a business may need additional information from a consumer to process a request to opt-out of the sale/sharing, and permits businesses to request additional information but only insofar as it is needed. This subsection is necessary because requiring verification for requests to opt-out of sale/sharing unnecessarily impedes consumers exercising their rights.

Subsection (e) is existing subsection (g) and has been revised to include the sharing of personal information to align the regulation with the revised language of the statute. The phrase "to the requestor" has also been included to clarify to whom the explanation should be given.

Subsection (f) is existing subsection (e) and sets forth the different things that a business must do to comply with a request to opt-out sale/sharing into one regulation. This subsection is necessary to set forth the timeframe for complying with requests to opt-out of sale/sharing and to clarify businesses' obligations vis-à-vis contractors, service providers, and third parties. Additionally, it is necessary to protect consumers' right to opt-out of sale/sharing, by ensuring that consumers' requests are communicated to, and complied with by, the entities that receive the personal information at issue, which may not be the business to which the consumer submitted their request.

Specifically, **subsection (f)(1)** explains that businesses must stop selling and sharing the consumer's personal information to third parties as quickly as feasibly possible and within a maximum of 15 business days. This regulation is informed by the same reasons that the Attorney General's Office considered in setting this same deadline for requests to opt-out of sale previously. The Attorney General weighed various comments received and determined that 15 business days appropriately balanced the right of consumers to opt out of sale 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, this subsection works together with **subsection (f)(2)**, which addresses concerns about the further proliferation of personal information by requiring businesses to direct any third parties to whom the business has sold or shared the information at issue after the consumer submitted their request and before complying comply with the consumer's request. This allows the consumer's request to opt-out of the sale/sharing to functionally operate as if it were complied with upon the business's receipt and also incentivizes businesses to comply with consumers' requests as soon as possible. **Subsection (f)(1)** also clarifies that providing personal information to service providers or contractors does not constitute a sale or sharing of personal information. This provides guidance to businesses who may be confused by how this right to opt-out of sale/sharing relates to the businesses' relationship to different persons.

Subsection (f)(3) addresses situations in which a business authorizes third parties to collect personal information on its behalf, or where the business and the third party jointly control the collection of personal information. This provision requires the business to notify the third party of the request to opt-out of sale/sharing and of the third party's obligation to comply with section 7052, subsection (a), within the same timeframe. This subsection implements Civil Code section 1798.135, subdivision (f), which requires a business to communicate a request to opt-out of

sale/sharing to any person authorized by the business to collect personal information. **Subsection (f)(4)** requires businesses to provide a means by which the consumer can verify that their request to opt-out of sale/sharing has been processed by the businesses. This is necessary to promote transparency and consumer understanding regarding the outcome of their request. The Agency considered the alternative of requiring the business to confirm receipt of the request to opt-out of sale/sharing, but determined that such a requirement was too prescriptive and may create friction in the consumer's user experience. Instead, the Agency determined that requiring a performance-based standard that gives flexibility to the business regarding how to display the status of the consumer's request addresses the need for transparency with a lesser burden to the business to craft the means in accordance with how it manages other CCPA requests.

Subsection (g) is existing subsection (d). It has been revised to clarify that, in responding to a request to opt-out of sale/sharing, a business may give the consumer the option to opt-out of the sale or sharing of personal information for certain uses as long as a single option to opt-out of the sale or sharing of all personal information is more prominently presented than other choices. It also explains that doing so will prevent the business from using the exception provided for in Civil Code section 1798.135, subdivision (b)(1), that applies to businesses that process an opt-out preference signal in a frictionless manner. This subsection is necessary because it provides clear guidance regarding how businesses can give consumers choices for opting out of the sale or sharing of their information and how this regulation interacts with other parts of the law. It is informed by public input the Attorney General's Office received during previous rulemaking activities that providing choices to consumers regarding what personal information can be sold may be beneficial to both consumers and businesses, but it also requires a single option to prevent consumer confusion and to prevent businesses from presenting options to consumers in a strategic manner intended to curtail exercise of the right to opt-out of sale/sharing. In addition, this subsection is consistent with the regulations set forth at section 7022, subsection (h), regarding requests to delete, and section 7027, subsection (h), regarding requests to limit, which benefits businesses by facilitating compliance.

Subsection (h) incorporates the requirements found in Civil Code section 1798.135, subdivision (a)(4). Including this statutory requirement in the regulation is necessary for clarity so that all the requirements regarding the right to opt-out of sale/sharing are in one place.

Subsection (i) is existing subsection (f). It has been revised to apply to requests to opt-out of the sale and sharing of personal information and also explain that requests made by an opt-out preference signal do not require written permission from the consumer. These revisions are necessary to operationalize the right to opt-out of sale/sharing and to explain how opt-out preference signals interact with other parts of the CCPA and these regulations. Because section 7025, subsection (b)(2), already addresses the consumer's choice in using the opt-out preference signal, there is no need for a business to require written permission from the signal before complying with the consumer's request.

Subsection (j) incorporates the requirements found in Civil Code section 1798.135, subdivision (c)(4), which requires that a business wait at least 12 months from the date of a consumer's request before asking the consumer to consent to the sale or sharing of their personal information. Including this statutory requirement in the regulation is necessary for clarity so that all the requirements regarding the right to opt-out of sale/sharing are in one place.

Changes without regulatory effect. Non-substantive changes (*e.g.*, replacing request to opt-out with request to opt-out of sale/sharing, grammatical changes) have been made throughout the section. The title has been amended to better reflect the content of the regulation. Subsections have been renumbered.

§ 7027. Requests to Limit Use and Disclosure of Sensitive Personal Information.

Civil Code section 1798.121 gives consumers the right to request a business to limit its use and/or disclosure of their sensitive personal information. The purpose of section 7027 is to operationalize the right to limit by setting forth the rules and procedures businesses must follow regarding submission and handling of requests to limit. The regulation is necessary because Civil Code section 1798.185, subdivision (a)(4)(A), requires the Agency to establishes rules and procedures relating to requests to limit. Civil Code section 1798.140, subdivision (n), also requires the Agency to approve "designated methods for submitting requests" under the CCPA. This regulation will benefit both businesses and consumers by clarifying businesses' obligations and facilitating consistency in how requests to limit are handled. This regulation further benefits businesses, and facilitates compliance with Civil Code section 1798.121, by providing a list in subsection (l) of the ways in which businesses may use sensitive personal information that do not require the business to post a notice of right to limit. Overall, this regulation aims to balance the burden of compliance by businesses with the consumer's interest in protecting their sensitive personal information. It also aims to facilitate transactions between consumers and businesses and recognizes that use or disclosure of sensitive personal information is sometimes necessary to complete a transaction or carry out a business's operations.

Subsection (a) sets forth the purpose of requests to limit and ties the process for making and handling such requests to the heightened privacy interest consumers have in protecting their sensitive personal information. (Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3(A)(2).) The purpose of the right to limit is to give consumers meaningful control over how their sensitive personal information is collected, used, and disclosed in accordance with the purpose and intent of the CCPA. (*Ibid.)* This regulation is necessary to guide businesses as they make decisions on how to implement this right and apply these regulations. To the extent that there are different ways in which the business can apply the regulations, the business should pick the manner that would best accomplish the purpose of the right.

Subsection (b) sets forth businesses' obligations under Civil Code section 1798.121, subdivision (a), and is necessary to set forth the rules and procedures businesses must follow. This subsection requires a business that uses or discloses sensitive personal information to provide two or more designated methods for submitting requests to limit, subject to certain exemptions listed in subsection (l). In requiring two methods for submitting requests to limit, this provision is consistent with the CCPA's treatment of requests to know, requests to delete, and requests to correct, as set forth in Civil Code section 1798.130, subdivision (a)(1)(A). This subsection further allows the business to determine the methods for submission of requests to limit, provided that one of the two methods must reflect the manner in which the business interacts with the consumer. This is necessary to ensure that consumers receive meaningful access to this right. It benefits businesses by allowing them flexibility in determining how to receive requests to limit, while minimizing the burden on consumers because at least one of the methods for

submitting requests is likely to reflect the manner in which the consumer has interacted with the business in the past (*e.g.*, online, in a brick-and-mortar store, etc.).

Subsections (b)(1) through **(4)** illustrate appropriate methods that a business may provide for submission of requests, taking into account how the business interacts with consumers, the manner in which it collects the sensitive personal information, available technology, and ease of use by the consumer. This subsection is necessary to provide businesses with guidance regarding methods for submission. A business that collects sensitive personal information from consumers online must provide at least one of the submission methods described in subsection (b)(1), including via the "Limit the Use of My Sensitive Personal Information" link in accordance with section 7014 of these regulations. The examples provided in **subsections (b)(2) and (3)** are illustrative and do not set forth mandatory submission methods. **Subsection (b)(4)** makes clear that a cookie banner or similar notification about cookies does not necessarily comply with the requirements of **subsections (b)(1)** for website methods of submission. In order to comply, the cookie banner or similar notification must notify the consumer about the right to limit in specific terms. This provision is necessary to ensure that consumers are aware of the right to limit and to avoid consumer confusion in response to concerns regarding how the right to opt-out of sale has been implemented in the marketplace.

Subsection (c) provides additional requirements that apply to all submission methods and is necessary to ensure consumers are aware of and able to exercise the right to limit. This provision incorporates the requirements set forth in section 7004 and thereby promotes consistency among the various types of consumer requests the CCPA authorizes.

Subsection (d) prohibits a business from requiring a consumer to create an account or provide additional information beyond what is necessary to direct the business to limit the use or disclosure of the consumer's sensitive personal information in accordance with Civil Code section 1798.135, subdivision (c)(1). Including this statutory requirement in the regulation is necessary for clarity because it consolidates all the requirements regarding the right to limit into one place.

Subsection (e) prohibits the business from requiring requests to limit to be verifiable consumer requests. **Subsection (e)** is consistent with section 7026, subsection (d), which likewise prohibits businesses from requiring requests to opt-out of sale/sharing to be verifiable consumer requests. The CCPA does not require requests to opt-out of sale/sharing and requests to limit to be verifiable consumer requests because the potential harm to consumers from non-verified requests is minimal. This subsection is in response to observations in the marketplace and comments received by the Agency during preliminary rulemaking activities that some businesses have misused the verifiable request process to impede consumers' exercise of their right to opt-out of sale. This subsection recognizes that, in some cases, a business may need additional information from a consumer to process a request to limit, and permits businesses to request additional information but only insofar as it is needed. This subsection is necessary to clarify for businesses that they are not to require verification for requests to limit and doing so will be considered an unnecessary impediment to consumers exercising their right in violation of the CCPA and these regulations.

Subsection (f) allows a business to deny requests to limit that it has reason to believe are fraudulent or abusive, as is consistent with regulations pertaining to requests to correct (section 7023, subsection (h)) and requests to opt out of sale/sharing (section 7026, subsection (e)). In all such cases, requests may be denied if the business has a good-faith, reasonable, and documented basis for determining that the request is fraudulent or abusive. The business must inform the requestor of its reason for denying the request and explain its reasons for believing the request to be fraudulent or abusive. This subsection is necessary to prevent harm to both businesses and consumers. It imposes a minimal burden on businesses while ensuring that legitimate requests are not denied as potentially fraudulent or abusive without the consumer having the opportunity to learn of the reason for denial.

Subsection (g) sets forth the different things that a business must do to comply with a request to limit. This subsection is necessary to set forth the timeframe for complying with requests to limit and to clarify businesses' obligations vis-à-vis contractors, service providers, and third parties. Additionally, it is necessary to protect consumers' right to limit, by ensuring that consumers' requests are communicated to, and complied with by, the entities that actually directly use or disclose the sensitive personal information at issue, which may not be the business to which the consumer submitted their request.

Specifically, **subsection (g)(1)** explains that businesses must stop using and disclosing the consumer's sensitive personal information for any purposes other than those set forth in subsection (l) as quickly as feasibly possible and within a maximum of 15 business days. This is the same timeframe provided for requests to opt-out under section 7026, subsection (f), and informed by the same reasons that warranted that time frame. The Agency weighed various comments received and determined that 15 business days appropriately balanced 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, this subsection works together with **subsection (g)(3)**, which addresses concerns about the further proliferation of sensitive personal information by requiring businesses to direct any third parties to whom the business has disclosed or made available the information at issue after the consumer submitted their request to comply with the consumer's request. This allows the consumer's request to limit to functionally operate as if it were complied with upon the business's receipt and also incentivizes businesses to comply with consumers' requests as soon as possible.

Subsection (g)(2) facilitates compliances with Civil Code section 1798.121, subdivision (c), which requires service providers and contractors to comply with a consumer's request to limit once instructed to do so by the business. This subsection further clarifies that businesses must instruct their service providers or contractors to comply within the same timeframe. The subsection benefits businesses and consumers by consolidating all the requirements regarding the right to limit into one place. **Subsection (g)(4)** addresses situations in which a business authorizes third parties to collect sensitive personal information on its behalf, or where the business and the third party jointly control the collection of sensitive personal information. This provision requires the business to notify the third party of the request to limit and of the third party's obligation to comply with section 7052, subsection (b), within the same timeframe. This subsection implements Civil Code section 1798.135, subdivision (f), which requires a business to

communicate a request to limit to any person authorized by the business to collect personal information. **Subsection (g)(5)** requires businesses to provide a means by which the consumer can verify that their request to limit has been processed by the businesses. This is necessary to promote transparency and consumer understanding regarding the outcome of their request. The Agency considered the alternative of requiring the business to confirm receipt of the request to limit, but determined that such a requirement was too prescriptive and may create friction in the consumer's user experience. Instead, the Agency determined that requiring a performance-based standard that gives flexibility to the business regarding how to display the status of the consumer's request addresses the need for transparency with a lesser burden to the business to craft the means in accordance with how it manages other CCPA requests.

Subsection (h) clarifies that, in responding to a request to limit, a business may give the consumer the option to permit specified uses or disclosures of the consumer's sensitive personal information, other than those set forth in subsection (l) of this regulation that are already excepted from the right to limit. However, the business must make the single option to limit all non-excepted uses more prominent to the consumer than any options to permit specified uses. This subsection benefits both businesses and consumers by allowing requests to limit, where appropriate, to be targeted to limit only certain uses or disclosures. The subsection regarding prominence of the single option is necessary to prevent consumer confusion and to prevent businesses from presenting options to consumers in a strategic manner intended to curtail exercise of the right to limit. In addition, this subsection is consistent with the regulations set forth at section 7022, subsection (h), regarding requests to delete, and section 7026, subsection (g), regarding requests to opt-out of sale/sharing, which benefits businesses by facilitating compliance.

Subsection (i) clarifies that a request to limit may be made by a consumer's authorized agent so long as the agent has the written permission of the consumer. This provision allows a business to ask the authorized agent for the consumer's written permission, and to deny the request if the agent does not produce it. This subsection is necessary to limit abuse or fraud and ensure that when requests to limit are made by someone other than the consumer, the person making the request is a legitimate authorized agent of the consumer. It provides businesses flexibility to require proof, but does not mandate additional record-keeping obligations.

Subsection (j) facilitates compliance with Civil Code section 1798.135, subdivision (a)(4). This subsection does not impose any additional obligations. Including this statutory requirement in the regulation is necessary for clarity because it consolidates all the requirements regarding the right to limit into one place.

Subsection (k) facilitates compliance with Civil Code section 1798.135, subdivision (c)(4), which requires that a business wait at least 12 months from the date of a consumer's request to limit before asking the consumer to consent to the use or disclosure of their sensitive personal information for purposes other than those disclosed in subsection (l). Including this statutory requirement in the regulation is necessary for clarity because it consolidates all the requirements regarding the right to limit into one place.

Subsection (l) sets forth all the permissible uses of sensitive personal information that are outside of the consumer's right to limit. These exemptions are found in Civil Code section

1789.121. Because section 1789.121, subdivision (a), cross-references the permissible uses described in section 1789.140, subdivision (e), paragraphs (2), (4), (5), and (8), this subsection describes all permissible uses in a single, easily referenced list with the goal of facilitating compliance and easing the burden of compliance on businesses. The following identifies the statutory references for each provision.

Subsection (l)(1): Civil Code § 1789.121, subd. (a).

Subsection (l)(2): Civil Code §§ 1789.121, subd. (a), 1798.140, subds. (e)(2), (ac)(1).

Subsection (l)(3): Civil Code § 1798.121, subd. (a), 1798.140, subds. (e)(2), (ac)(1).

Subsection (l)(4): Civil Code §§ 1789.121, subd. (a), 1798.140, subds. (e)(2), (ac)(3).

Subsection (l)(5): Civil Code §§ 1789.121, subd. (a), 1798.140, subd. (e)(4).

Subsection (l)(6): Civil Code §§ 1789.121, subd. (a), 1798.140, subd. (e)(5).

Subsection (l)(7): Civil Code §§ 1789.121, subd. (a), 1798.140, subd. (e)(8).

Illustrative examples are provided to aid understanding. This regulation benefits businesses and consumers by making the regulation easier to read and understand and less repetitive.

§ 7028. Requests to Opt-In After Opting-Out of the Sale or Sharing of Personal Information or Limiting the Use and Disclosure of Sensitive Personal Information.

The CPRA's amendments to the CCPA extended the right of a consumer to opt out of a business's sale of personal information to the business's sharing of personal information (Civ. Code, § 1798.120) and added a new right to limit the use and disclosure of sensitive personal information (Civ. Code, § 1798.121). Accordingly, changes have been made to this section and are necessary to align the regulation with the amended language of the statute.

Subsection (a) has been revised to extend the procedures for requests to opt-in to include requests to opt-in to the sharing of personal information and requests to opt-in to the use and disclosure of sensitive personal information. This is necessary to align the regulation with the amended language of the statute.

Subsection (b) has been revised to extend the right to opt-out to include opting out of the sharing of personal information. It has also been revised to clarify that consent is required when opting a consumer back into the sale or sharing of their personal information after they have opted out. Methods for obtaining the consumer's consent shall comply with section 7004 of these regulations. This revision is necessary to harmonize this subsection with new regulations governing how a business is to obtain consent.

Subsection (c) has been added to address situations where consumers initiate transactions with businesses after making a request to limit when those transactions may require that the business disclose or use the consumer's sensitive personal information in a manner inconsistent with the request to limit. In order to balance the consumer's privacy interest with both the consumer's and the business's interest in completing their transaction, this subsection allows a business to obtain the consumer's consent to use or disclose the information for that purpose even if it is

within 12 months of the consumer's request during which the business is not allowed to ask the consent to reverse their decision. (See Civ. Code, § 1798.135, subd. (c)(4).) The subsection further instructs that section 7004 applies to obtaining the consumer's consent. This subsection is necessary to provide guidance to businesses on how to implement the new right to limit and to also ensure that consumers are aware of their rights and can exercise them in an informed manner.

Changes without regulatory effect. The title has been amended to better reflect the content of the regulation.

§ 7031. Requests to Know or Delete Household Information.

This section has been deleted because Civil Code section 1798.145, subdivision (p), states that requests to know and requests to delete do not apply to household data. The existing regulation is obsolete in light of this statutory amendment.

Article 4. Service Providers, Contractors, and Third Parties

A new article has been added to create better organization within Chapter 1.

§ 7050. Service Providers and Contractors.

The CPRA amendments to the CCPA added a new category of persons (*i.e.*, contractors) with whom a business may share personal information for a business purpose without being considered a "sale" or "sharing" subject to the restrictions in Civil Code section 1798.120. Though contractors and service providers differ slightly in that contractors do not necessarily have to process personal information "on behalf of a business" (see Civ. Code, § 1798.140, subds. (j) and (ag)), there are no other differences with regard to how service providers and contractors are to handle personal information under the CCPA. The CPRA amendments also revised provisions relating to the business purposes for which service providers and contractors can process personal information. Accordingly, this section has been revised to apply service provider regulations to contractors and to also address the revised definition of business purposes.

The purpose of section 7050 is to clarify who is a service provider or contractor, how service providers and contractors are to handle consumer requests made pursuant to the CCPA, and to harmonize different parts of the CCPA that have led to confusion regarding how the CCPA applies to service providers and contractors. The regulation is necessary because Civil Code section 1798.185, subdivisions (a)(10) and (11), require the Agency to issues regulations identifying the business purposes and circumstance under which a service provider or contractor may use and/or combine consumers' personal information. This section is informed by comments received by the Agency during preliminary rulemaking activities. The specific changes to the regulation are explained below.

Subsection (a) has been revised to apply to both service providers and contractors and an example has been added to clarify what the regulation is meant to address. This subsection is necessary because the statutory definition of "service provider" and "contractor" excludes persons or entities that service non-profit and government entities through its use of the word

"business," which is defined to include only entities "organized or operated for the profit or financial benefit of its shareholders or other owners." (Civ. Code, § 1798.140, subds. (d), (j)(1), and (ag)(1).) Without this subsection, entities that process personal information on behalf of non-profit and government entities in accordance with a written contract may be required to comply with consumer requests even when those non-profits and government entities in ultimate control of the information are not required to do so. This unintended and undesired consequence will lead to significant disruption in the functioning of those non-profits and governmental entities and is not in furtherance of the purposes of the CCPA, which explicitly excluded non-profits and government entities from being subject to the CCPA.

Existing subsection (b) has been deleted because it is no longer necessary in light of the CPRA's amendment of Civil Code section 1798.100, which now applies to situations where a business "controls the collection" of a consumer's personal information.

Subsection (b) is existing subsection (c). It has been revised throughout to apply to both service providers and contractors. This subsection is necessary because it provides clear guidance regarding the interrelationship of the terms "service provider," "contractor," "business purpose," and "commercial purpose" defined in the CCPA. (Civ. Code, § 1798.140, subds. (ag), (j), (e), and (g).) Both a service provider and a contractor are prohibited from using personal information for any purpose other than the business purpose specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract. (*Id.*) This subsection clarifies what is and is not an appropriate use of personal information that would advance the commercial purposes of the service provider rather than the business purpose of the business.

In **subsection (b)(1)**, "directed" has been replaced with "authorized" to align the regulation with the language used in Civil Code section 1798.135, subdivision (f). **Subsection (b)(2)** has been revised to make the regulation easier to read and understandable for businesses and consumers. **Subsection (b)(4)** explains that a service provider or contractor can use personal information to build or improve the quality of their services as long as they do not use personal information to perform services on behalf of another person. The subsection also provides two illustrative examples. This regulation is necessary to operationalize when a service provider or contractor may combine the personal information received in connection with their role as a service provider or contractor. (See Civ. Code, § 1798.140, subds. (j)(1)(A)(iv) and (ag)(1)(D).) **Subsection (b)(5)** has added "malicious, deceptive" to align the regulation with Civil Code section 1798.140, subdivision (ac)(2), which defines "security and integrity." The citations in **subsection (b)(6)** have been updated.

Subsection (c) has been added to clarify that cross-contextual behavioral advertising is not a business purpose for which a service provider or contractor can contract with a business. The subsection also provides an illustrative example. This subsection is necessary to explain Civil Code section 1798.140, subdivision (e)(6). It addresses concerns raised by the public during the Attorney General's previous rulemaking activities.

Existing subsection (d) has been deleted because it is no longer necessary in light of Civil Code section 1798.140, subdivision (ag)(1)(A).

Subsection (d) is existing subsection (e). It has been revised to apply to both service providers and contractors and to apply to all requests made pursuant to CCPA, which now include requests to correct and requests to limit. The subsection clarifies that, if a service provider or contractor receives a CCPA request directly from the consumer, it is to either act in accordance with the business's instruction as required by Civil Code sections 1798.105, subdivision (c)(3), 1798.121, subdivision (c), 1798.130, subdivision (a)(3)(A), and these regulations, or to inform the consumer that the service provider or contractor cannot comply because the request has been sent to a service provider or contractor. These revisions are necessary to align the regulation with the amended statute.

Subsection (e) is existing subsection (f). It has been revised to apply to both service providers and contractors. It clarifies that a service provider or a contractor that is also a "business," as that term is defined in Civil Code section 1798.140, subdivision (d), shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider or contractor. This subsection is necessary because it provides clear guidance on how entities that are both a service provider or a contractor and a business are to handle consumer requests and other obligations under the CCPA. It addresses concerns raised by the public during the Attorney General's previous rulemaking activities.

Changes without regulatory effect. Non-substantive changes (*e.g.*, grammatical changes) have been made throughout the section. The title has been amended to better reflect the content of the regulation. The section and the subsections have been renumbered. Authority and reference citations have been amended.

§ 7051. Contract Requirements for Service Providers and Contractors.

The CPRA amendments to the CCPA set forth a number of contractual requirements for persons who are to be considered service providers or contractors under the CCPA. The purpose of section 7051 is to consolidate all the provisions that must be included in a service provider or contractor's contract with the business, to explain the consequence if the provisions are not included in the contract, and to clarify the duties of a service provider, contractor, and business as it relates to the contract. It is beneficial to businesses, service providers, and contractors because it allows them to use the regulation as a checklist to ensure that all the statutorily required information is included in their contracts.

Subsection (a) sets forth all the provisions that must be included in a service provider or contractor contract. This is necessary because the requirements are listed in several different places throughout the CCPA. The following identifies the statutory references for each provision.

Subsection (a)(1): Civil Code § 1798.140, subds. (j)(1)(A)(i) and (ag)(1)(A).

Subsection (a)(2): Civil Code §§ 1798.100, subd. (d)(1).

Subsection (a)(3): Civil Code § 1798.140, subds. (j)(1)(A)(ii) and (ag)(1)(B).

Subsection (a)(4): Civil Code § 1798.140, subds. (j)(1)(A)(ii) and (ag)(1)(B).

Subsection (a)(5): Civil Code § 1798.140, subds. (j)(1)(A)(iii) and (ag)(1)(C).

Subsection (a)(6):	Civil Code §§ 1798.100, subd. (d)(2), 1798.105, subd. (c)(3), 1798.121, subd. (c), 1798.130, subd. (a)(3), 1798.81.5.
Subsection (a)(7):	Civil Code §§ 1798.100, subd. (d)(3), 1798.140, subd. (ag)(1)(D).
Subsection (a)(8):	Civil Code § 1798.100, subd. (d)(4).
Subsection (a)(9):	Civil Code § 1798.100, subd. (d)(5).
Subsection (a)(10):	Civil Code §§ 1798.105, subd. (c)(3), 1798.121, subd. (c), 1798.130, subd. (a)(3)(A).

Consolidating all the requirements into one place helps businesses, service providers, and contractors understand what is required of them.

Subsections (a)(2) and (3) require the contract to identify the specific business purpose or service and make clear that the contract shall not generally refer to the entire contract. This requirement is necessary to address observations in the marketplace and comments received by the Agency during preliminary rulemaking activities that businesses' contracts do not clearly identify the business purpose for which the service provider is processing personal information. **Subsections (a)(3) and (4)** are derived from the same Civil Code section, but they have been broken up into two separate requirements to make it easier for businesses to read and understand. **Subsection (a)(8)** sets a deadline of no later than five business days as the deadline for notifying a business if it determines that it can no longer meet its obligations. This is necessary so that the business can take prompt action to ensure compliance and to protect consumer personal information from unauthorized use or disclosure. Five business days is a reasonable and feasible maximum timeframe for service providers and contractors to provide notice to the affected business.

Subsection (b) requires service providers and contractors to have a contract that complies with subsection (a) when subcontracting their work. This is necessary to facilitate compliance with Civil Code section 1798.140, subdivision (ag)(2), which requires service providers and contractors who subcontract with another person in providing services to comply with the CCPA and these regulations. **Subsection (c)** explains that the effect of not having a contract that complies with subsection (a) in place is that the person to whom the business is disclosing personal information is not a "service provider" or a "contractor. Thus, the disclosure of personal information may be a sale for which the business must provide the consumer a right to opt-out of sale/sharing. This is necessary to ensure compliance with the CCPA and inform businesses of the consequences of failing to have a required contract in place.

Subsection (d) makes clear that a service provider and contractor must comply with the terms of the contract required under subsection (a). This subsection is necessary to make clear that a failure to comply with the required contract is a violation of the CCPA enforceable by the Agency and the Attorney General's Office.

Subsection (e) clarifies that whether a business conducts due diligence of its service providers or contractors factors into whether the business can rely on the defense set forth in Civil Code section 1798.145, subdivision (i). The subsection explains that a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's

systems may not be able to claim that it did not know or have reason to believe that the service provider or contractor intended to use the personal information in violation of the CCPA. This subsection is necessary to ensure that the provisions required to be in the contract have real meaning and businesses do not shirk their duties to ensure that personal information disclosed to service providers and contractors is used in a lawful manner. Businesses, service providers, and contractors are to comply with not just the letter of the law, but the spirit of the law.

§ 7052. Third Parties.

The CPRA amendments to the CCPA add requirements on third parties who are forwarded consumer requests from a business who sold or shared personal information with them. The purpose of section 7052 is to clarify what is required of third parties with regard to consumer's CCPA requests. This regulation provides businesses and third parties with clear guidance about what is required of them and is informed by comments received by the Agency during preliminary rulemaking activities.

Subsection (a) facilitates compliance with Civil Code sections 1798.100, subdivision (d), 1798.105, subdivision (c)(1), and 1798.135, subdivision (f). When a business receives a request to delete or a request to opt-out of sale/sharing from a consumer, it is required to notify all third parties to whom the business has sold, shared, made available, or authorized to collect the consumer's personal information. (Civ. Code, §§ 1798.105, subd. (c)(1), 1798.135, subd. (f).) Moreover, the third party is contractually obligated to comply with the CCPA and provide the same level of privacy protection as is required by the CCPA. (Civ. Code, § 1798.100, subd. (d).) This regulation explains that in response to the notification, the third party is to comply with the consumer's request in the same way a business is required to comply under sections 7022, subsection (b), and 7026, subsection (f). The third party shall no longer retain, use, or disclose the personal information unless the person becomes a service provider or contractor that complies with the CCPA and these regulations. This is necessary to ensure that a consumer's privacy elections are honored by all entities that have received their personal information.

Subsection (b) facilitates compliance with Civil Code sections 1798.100, subdivision (d), and 1798.135, subdivision (f). When a business receives a request to limit, it is required to notify all third parties to whom the business has provided, made available, or authorized the collection of the consumer's sensitive personal information for purposes other than those set forth in section 7027, subsection (l). (Section 7027, subsection (g)(4); *see also* Civil Code, § 1798.135, subd. (f).) Moreover, the third party is contractually obligated to comply with the CCPA and provide the same level of privacy protection as is required by the CCPA. (Civ. Code, § 1798.100, subd. (d).) This regulation explains that in response to the notification, the third party is to comply with the consumer's request in the same way a business is required to comply under section 7027, subsection (g). The third party shall no longer retain, use, or disclose the sensitive personal information for purposes other than those set forth in section 7027, subsection (l). This is necessary to ensure that a consumer's privacy elections are honored by all entities that have received their sensitive personal information.

Subsection (c) requires a third party that collects personal information from a consumer online (*e.g.*, through a first party's website) and receives an opt-out preference signal to recognize and treat the signal as a request to opt-out of sale/sharing and not retain, use, or disclose that personal

information unless informed by the business otherwise. In the alternative, the third party can become a service provider or contractor that complies with the CCPA and these regulations. This subsection is necessary to efficiently effectuate a consumer's request to opt-out of sale/sharing with the multiple third parties that may be collecting a consumer's personal information online, such as through a first party's website. Requiring a third party who has been authorized to collect personal information from the consumer to check for and comply with an opt-out preference signal unless told otherwise prevents a third party from avoiding its obligations to comply with requests to opt-out of sale/sharing. It benefits businesses by sharing the burden of communicating online requests to opt-out of sale/sharing and benefits consumers by ensuring that third parties tracking them online comply with their requests. Including the exception for when the business informs third parties that the consumer has consented to the sale/sharing of personal information addresses how the consumer can selectively consent to the business's sale or sharing of a consumer's personal information in accordance with section 7025, subsection (c)(4) and (5).

§ 7053. Contract Requirements for Third Parties.

Civil Code section 1798.100, subdivision (d), requires a business that collects a consumer's personal information and that sells that personal information to, or shares it with, a third party for a business purpose to enter an agreement with the third party that includes certain provisions. The purpose of section 7053 is to clearly set forth all the provisions that must be included in third party contract with the business, to explain the consequence if the provisions are not included in the contract, and to clarify the duties of the third party and the business as it relates to the contract. This regulation benefits businesses and third parties by providing clear guidance regarding what is expected of them.

Subsection (a) sets forth all the provisions that must be included in the contract with a third party to whom the business sells or shares personal information. This is necessary because the requirements are listed in several different places throughout the CCPA. The following identifies the statutory references for each provision.

Subsection (a)(1): Civil Code § 1798.100, subd. (d)(1).

Subsection (a)(2): Civil Code § 1798.100, subd. (d)(1).

Subsection (a)(3): Civil Code §§ 1798.100, subds. (d)(2), (a), (b), and (c), 1798.105, subd. (c), 1798.106, subds. (a), (b), and (c), 1798.110, subds. (b), (c), 1798.115, subds. (b), (c), and (d), 1798.120, subd. (b), (c), and (d), 1798.121, subd. (b), 1798.125, subd. (a), 1798.130, 1798.135, and 1798.81.5.

Subsection (a)(4): Civil Code § 1798.100, subd. (d)(3).

Subsection (a)(5): Civil Code § 1798.100, subd. (d)(5).

Subsection (a)(6): Civil Code § 1798.100, subd. (d)(4).

Consolidating all the requirements into one place helps businesses and third parties understand what is required of them.

Subsection (a)(1) requires the contract to identify the specific business purpose or service and make clear that the contract shall not generally refer to the entire contract. This requirement is necessary to address observations in the marketplace and comments received by the Agency during preliminary rulemaking activities that businesses' contracts do not clearly identify the business purpose in service provider contracts. The Agency anticipates that general statements will likely be used in third party agreements unless businesses and third parties are expressly required to do otherwise. **Subsection (a)(2)** provides that the third party can only use personal information for the limited and specified purposes identified in the contract. This is necessary to ensure that businesses and third parties comply with Civil Code section 1798.100, subdivision (d)(1). **Subsection (a)(3)** clarifies that the third party must comply with applicable sections of the CCPA and these regulations and provides examples of what that would include. **Subsection (a)(4)** borrows from Civil Code section 1798.140, subdivision (ag)(1)(D), in providing an example of a reasonable way in which a business may ensure that a third party uses the personal information received from the business in a manner consistent with the CCPA and these regulations. **Subsection (a)(5)** requires the contract to include that the business has the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information. This is necessary to ensure compliance with Civil Code section 1798.100, subdivision (d)(5). **Subsection (a)(6)** sets a deadline of no later than five business days as the deadline for notifying a business if it determines that it can no longer meet its obligations. This is necessary so that the business can take prompt action to ensure compliance and to protect consumer personal information from unauthorized use or disclosure. Five business days is a reasonable and feasible maximum timeframe for third parties to provide notice to the affected business.

Subsection (b) requires businesses that authorize a third party to collect personal information on its website to contractually require the third party to check for and comply with a consumer's opt-out preference signal unless informed by the business that the consumer has consent to the sale or sharing of their personal information. This is necessary so that a consumer's election to opt-out is implemented by all persons who receive the consumer's personal information online. This benefits consumers in ensuring that their request to opt-out is meaningful and easily executed without their having to make individualized requests with each business who receives their personal information. Indeed, many of these third parties may be unknown to the consumer because they are not the business with whom the consumer intended to interact.

Subsection (c) explains that the consequence of a third party not having a contract that complies with subsection (a) is that the third party shall not collect, use, process, retain, sell, or share the personal information received from the business. This is necessary to ensure compliance with the CCPA and inform third parties of the consequences of failing to have a required contract in place.

Subsection (d) makes clear that the third party must comply with the terms of the contract required under subsection (a). This subsection is necessary to make clear that a failure to comply with the contract is a violation of the CCPA enforceable by the Agency and the Attorney General's Office.

Subsection (e) clarifies that whether a business conducts due diligence of its third parties factors into whether the business can rely on the defense set forth in Civil Code section 1798.145,

subdivision (i). The subsection explains that a business that never enforces the terms of the control nor exercises its rights to audit or test the third parties' systems may not be able to claim that it did not know or have reason to believe that the third party intended to use the personal information in violation of the CCPA. This subsection is necessary to ensure that the provisions required to be in the contract have real meaning and businesses do not shirk their duties to ensure that personal information disclosed to third parties is used in a lawful manner. Businesses and third parties are to comply with not just the letter of the law, but the spirit of the law.

Article 5. Verification of Requests

Changes without regulatory effect. The article has been renumbered.

§ 7060. General Rules Regarding Verification.

Civil Code sections 1798.106, subdivision (c), and 1798.130, subdivision (a)(2), require that requests to correct be verifiable consumer requests. Accordingly, this section on verification has been revised to apply to requests to correct. This change is necessary to operationalize the right to correct and right to know.

Subsection (a) has been revised to include requests to correct. This change is necessary to align the regulation with the amended statute.

Subsection (b) has been added to clarify that a business shall not require a consumer to verify their identity when making a request to opt-out or a request to limit. The CCPA does not require requests to opt-out of sale/sharing and requests to limit to be verifiable consumer requests because the potential harm to consumers from non-verified requests is minimal. This subsection is in response to observations in the marketplace and comments received by the Agency during preliminary rulemaking activities that some businesses have misused the verifiable request process to impede consumers' exercise of their right to opt-out of sale. This subsection recognizes that, in some cases, a business may need additional information from a consumer to process a request to opt-out of the sale/sharing, and permits businesses to request additional information but only insofar as it is needed. This subsection is necessary because requiring verification for requests to opt-out of sale/sharing unnecessarily impedes consumers exercising their rights.

Subsection (c)(3) has been revised because sensitive personal information is now defined by Civil Code section 1798.140, subdivision (ae).

Subsection (h) has been added to specifically address requests to correct. It requires businesses to verify consumers making requests to correct based on personal information that is not the subject of the request to correct. This is necessary to operationalize the right to correct and to provide guidance to businesses responding to requests to correct.

Changes without regulatory effect. Non-substantive changes (*e.g.*, reordering the type of CCPA requests) have been made throughout the section. Subsections have been renumbered. Reference citations have been amended.

§ 7061. Verification for Password-Protected Accounts.

Civil Code sections 1798.106, subdivision (c), and 1798.130, subdivision (a)(2), require that requests to correct be verifiable consumer requests. Accordingly, this section on verification has been revised to apply to requests to correct. This change is necessary to operationalize the right to correct.

Changes without regulatory effect. Non-substantive changes (*e.g.*, reordering the type of CCPA requests) and grammatical corrections have been made throughout the section. Reference citations have been amended.

§ 7062. Verification for Non-Accountholders.

Civil Code sections 1798.106, subdivision (c), and 1798.130, subdivision (a)(2), require that requests to correct be verifiable consumer requests. Accordingly, this section on verification has been revised to apply to requests to correct. This change is necessary to operationalize the right to correct.

Subsection (d) has been revised to include some examples that are relevant to requests to correct. This is necessary to operationalize the right to correct.

Changes without regulatory effect. Non-substantive changes (e.g., reordering the type of CCPA requests) have been made within the section. Reference citations have been amended.

§ 7063. Authorized Agents.

Subsection (a) has been revised to apply to the new right to correct. Civil Code section 1798.106 gives consumers the right to request a business to correct inaccurate personal information that it maintains about the consumer and Civil Code section 1798.185, subdivision (a)(7), requires the Agency to establish rules and procedures to facilitate a consumer's authorized agent's ability to exercise that right. This change is necessary to operationalize the consumer's right to use an authorized agent to make a request to correct.

Subsection (b) has been revised to state that a business shall not require that a power of attorney be the only way by which a consumer may use an authorized agent to act on their behalf. This change is necessary to address abuses in the marketplace and clear up any confusion regarding this issue.

Changes without regulatory effect. Non-substantive changes (*e.g.*, reordering the type of CCPA requests) have been made within the section. The title has been amended to better reflect the content of the regulation. Reference citations have been amended.

Article 6. Special Rules Regarding Consumers Under 16 Years of Age

§ 7070. Consumers Under 13 Years of Age.

The CPRA's amendment to Civil Code section 1798.120 extended the right of a consumer to opt out of a business's sale of personal information to the business's sharing of personal information.

Accordingly, changes have been made to this section and are necessary to align the regulation with the amended language of the statute.

Changes without regulatory effect. Non-substantive changes (*e.g.*, reordering the type of CCPA requests) have been made within the section.

§ 7071. Consumers 13 to 15 Years of Age.

The CPRA's amendment to Civil Code section 1798.120 extended the right of a consumer to opt out of a business's sale of personal information to the business's sharing of personal information. Accordingly, changes have been made to this section and are necessary to align the regulation with the amended language of the statute.

§ 7072. Notices to Consumers Under 16 Years of Age.

The CPRA's amendment to Civil Code section 1798.120 extended the right of a consumer to opt out of a business's sale of personal information to the business's sharing of personal information. Accordingly, changes have been made to this section and are necessary to align the regulation with the amended language of the statute.

Article 7. Non-Discrimination

§ 7080. Discriminatory Practices.

Subsections (a) and (b) have been revised to delete financial incentive to clarify how Civil Code section 1798.125 applies to discriminatory practices. Previously, these subsections grouped financial incentives with price and service differences when addressing discriminatory practices; however, Civil Code section 1798.125, subdivision (a), does not include financial incentives when addressing discrimination. Financial incentives where some type of benefit is given directly for the collection, sale/sharing, or retention of personal information do not invoke a discrimination analysis because there is a separate negotiation taking place for the specific incentive. This change is necessary to align to regulation to the language of the statute, as well as to clear up confusion in the marketplace caused by the existing regulation.

Subsection (c) has been revised to include requests to correct to align the regulation with the amended language of the statute, which gives consumers a new right to request a business to correct inaccurate personal information that it maintains about the consumer. (Civ. Code, § 1798.106.)

Changes without regulatory effect. Non-substantive changes (e.g., reordering the type of CCPA requests) have been made within the section.

§ 7081. Calculating the Value of Consumer Data.

Subsection (a) has been revised to delete "financial incentive" to clarify that only price and service differences require a valuation of data. Other kinds of financial incentives where a monetary or specific benefit (e.g., free t-shirt, gift card, etc.) is given for the exchange of data do

not require a valuation because the consumer is aware of the value of the good and able to factor it into their decision of whether to provide the personal information.

Article 8. Training and Record-Keeping

Change without regulatory effect. A non-substantive grammatical change has been made to the title.

§ 7100. Training.

Changes without regulatory effect. Reference citations have been amended.

§ 7101. Record-Keeping.

Changes without regulatory effect. Reference citations have been amended.

§ 7102. Requirements for Businesses Collecting Large Amounts of Personal Information.

Subsection (a)(1) has been put into a new order and metrics for the two new rights—right to correct and right to limit—have been added. This is necessary to inform the Agency, Attorney General, policymakers, academics, and members of the public about businesses' compliance with the CCPA. It considers the burden on businesses to compile and post this information by limiting the requirement to those businesses that handle a large amount of personal information, specifically, the personal information of approximately 10% of California's total population or more.

Changes without regulatory effect. Non-substantive changes (e.g., reordering the type of CCPA requests) have been made within section 7063. The subsections have been renumbered. Reference citations have been amended. Reference citations have been amended.

Article 9. Investigations and Enforcement

§ 7300. Sworn Complaints Filed with the Agency.

Subsection (a) provides the requirements for filing a sworn complaint. The information that must be included in a sworn complaint is necessary so that the Agency has sufficient information to evaluate the complaint and determine an appropriate response. It is also necessary for the complainant to authorize the alleged violator and Agency to communicate regarding the complaint so that the Agency can investigate the allegations.

Subsection (b) implements Civil Code section 1798.199.45, subdivision (b), which states that the Agency is required to notify the complainant in writing of the action, if any, the Agency has taken or plans to take on the sworn complaint, together with the reasons for that action or nonaction. Including this statutory requirement in the regulation is necessary for clarity so that all procedures are in one place. This subsection also provides that duplicate complaints submitted by the same complainant may be rejected without notice. This is necessary to preserve Agency resources.

§ 7301. Agency Initiated Investigations.

This section provides that all matters that do not result from a sworn complaint may be opened on the Agency's initiative. Providing the Agency with discretion to open a matter is necessary due to Agency expertise, resources, and priorities.

§ 7302. Probable Cause Proceedings.

Civil Code section 1798.199.55 allows the Agency to initiate the administrative hearing process after it determines there is probable cause for believing a violation has occurred. **Subsection (a)** provides a definition for probable cause because it is not defined in the CCPA. The definition is necessary so that the public and regulated parties understand the standard that must be met prior to initiating an administrative hearing. This subsection provides that probable cause exists when the evidence supports a reasonable belief that the CCPA has been violated. This definition is also necessary because the Agency should be allowed to initiate an administrative hearing if the evidence supports a reasonable belief that a violation has occurred. A finding of probable cause does not mean a violation has necessarily occurred. Rather, a violation must be proved in the subsequent administrative hearing.

Subsection (b) implements Civil Code section 1798.199.50, which requires the Agency to provide the alleged violator with notice of the probable cause proceeding. Including this statutory requirement in the regulation is necessary for clarity so that all procedures are in one place.

Civil Code section 1798.199.50 provides that a probable cause proceeding shall be private unless the alleged violator files with the Agency a written request that the proceeding be public. **Subsection (c)(1)** provides that a request for a public proceeding must be filed at least 10 business days before the proceeding. This is necessary so that the Agency has sufficient time to reserve a room for the public hearing and handle related logistics. This subsection further provides that a private proceeding may be conducted in whole or in part by telephone or videoconference. This is necessary to increase convenience for the parties and to minimize the costs associated with a public hearing, such as travel and hotel.

Subsection (c)(2) provides that Agency staff shall conduct the proceeding informally and shall determine whether there is probable cause based on the probable cause notice and any information or arguments presented at the probable cause proceeding by the parties. This subsection further provides that only the alleged violator(s), their legal counsel, and Enforcement Division staff have the right to participate at the proceeding. This is necessary because a probable cause proceeding is not intended to have the same requirements or formality as an administrative hearing. A finding of probable cause does not mean a violation has necessarily occurred. Rather, a violation must be proved in the subsequent administrative hearing.

Subsection (c)(3) provides that if the alleged violator fails to participate or appear at the probable cause proceeding, the alleged violator waives the right to further probable cause proceedings and Agency staff shall determine whether there is probable cause based on the notice and any information or argument provided by the Enforcement Division. This is necessary because Civil Code section 1798.199.50 provides an alleged violator with the right to participate in a probable cause proceeding, but they are not required to participate. If the alleged violator elects not to participate, the probable cause determination is made based on the notice and any information or argument provided by the Enforcement Division.

Subsection (d) provides that Agency staff will issue a written decision with their probable cause determination and serve it on the alleged violator. This is necessary to inform the alleged violator of the Agency's probable cause determination. The subsection further provides that the Agency's probable cause determination is final and not subject to appeal. This is necessary because an appeal would delay the initiation of an administrative hearing if probable cause is found. There is no reason for a violator to have a right to appeal because a finding of probable cause does not mean a violation has necessarily occurred.

Subsection (e) provides that notices of probable cause and probable cause determinations are not be open to the public nor admissible in evidence in any action or special proceeding other than one enforcing the CCPA. This is necessary because disclosure of the information could harm the Agency's investigation. Confidentiality also protects the alleged violator, who is presumed innocent until a violation is proved in an administrative hearing.

§ 7303. Stipulated Orders.

Subsection (a) provides that the Head of Enforcement and the person who is the subject of the investigation may stipulate to the entry of an order before or during an administrative hearing. This subsection further provides that if a stipulation has been agreed upon and the scheduled date of the hearing is set to occur before the next Board meeting, the Enforcement Division will apply for a continuance of the hearing. This is necessary to allow the parties to settle matters, and thus preserve the resources of the parties and Administrative Law Judge.

Subsection (b) provides that any stipulated order must be approved by the Board. This is necessary because only the Board has the authority to resolve enforcement actions. (Civ. Code, § 1798.199.35.)

Subsection (c) provides that any stipulated order shall be public and have the force of an order of the Board. This is necessary because the public should have the right to know the results of the Agency's enforcement actions. Public orders also provide important information to the public and regulated parties about what conduct violates the CCPA, which increases understanding and compliance.

§ 7304. Agency Audits.

Subsection (a) explains that the Agency may audit a business, service provider, contractor, or person to ensure compliance with any provision of the CCPA. Civil Code section 1798.199.40, subdivision (f), authorizes the Agency to audit businesses to ensure compliance with the CCPA pursuant to regulations adopted pursuant to section 1798.185, subdivision (a)(18). Including this statutory requirement in the regulations is necessary for clarity so that all procedures are in one place.

Subsection (b) provides the Agency's criteria for selecting the subject of an audit. The Agency may conduct an audit to investigate possible violations of the CCPA. An investigation may result from complaints submitted to the Agency, self-disclosed violations, media or news reports, or any other evidence gathered by the Agency. An audit is an investigative tool that can be used to determine whether a violation occurred.

Alternatively, the Agency may conduct an audit if the subject's collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject

has a history of noncompliance with the CCPA or any other privacy protection law. The Agency should be allowed to audit a business if the business's collection or processing of personal information presents a significant risk to consumer privacy or security to ensure the business's practices adequately protect consumer privacy. The Agency should also be allowed to audit a business with a history of noncompliance with the CCPA to ensure that the business has changed its practices and resolved previously identified issues. Similarly, the Agency should be allowed to audit a business with a history of noncompliance with another privacy law because non-compliance may indicate a lack of understanding or disregard of the CCPA.

Subsection (c) provides that audits may be announced or unannounced as determined by the Agency. Providing notice to the business ensures that the auditor arrives at a time when the personnel required to conduct the audit are present. However, the Agency retains the right to conduct unannounced audits to verify compliance.

Subsection (d) explains that a subject's failure to cooperate during the Agency's audit may result in the Agency issuing a subpoena, seeking a warrant, or otherwise exercising its powers to ensure compliance with the CCPA. This is necessary to encourage cooperation and provide notice to businesses of the consequences of failure to cooperate.

Subsection (e) explains that consumer personal information disclosed to the Agency during an audit shall be maintained in compliance with the Information Practices Act of 1977 (IPA), Civil Code section 1798, et seq. The IPA prohibits state agencies from disclosing any personal information in a manner that would link the information disclosed to the individual to whom it pertains, unless the disclosure of the information is otherwise authorized by law. Including this statutory requirement in the regulations is necessary for clarity so that consumers are aware that the Agency will protect the security and confidentiality of any personal information disclosed during an audit.

ECONOMIC IMPACT ASSESSMENT / ANALYSIS

The below analysis is limited to the economic impact incurred as a result of these proposed regulations. The analysis does not contemplate the economic impact resulting from legal obligations already imposed by the CCPA of 2018 and subsequent amendments, the CCPA regulations codified at California Code of Regulations, title 11 sections 7000 through 7102, or the new obligations created by the self-executing provisions as amended by the CPRA of 2020. This analysis also does not calculate the impact on those entities that have not undertaken full compliance obligations since the CCPA went into effect on January 1, 2020. To the extent that the proposed regulations incorporate existing statutory or regulatory requirements for clarity, this reiteration is also excluded from the economic analysis because pre-existing requirements are part of the baseline.

As required by Government Code section 11346.3, the Agency provides the following economic impact assessment:

(1) It is unlikely that the proposed regulations would create or eliminate jobs within the state. Businesses are already required to comply with many existing privacy laws, including the CCPA

and the existing CCPA regulations. Any new impact on jobs within the state would primarily result from the amended statute, and not the proposed regulations.

(2) It is unlikely that the proposed regulations would create new businesses or eliminate existing businesses within the state. Businesses are already required to comply with many existing privacy laws, including the CCPA and the existing CCPA regulations. Any new impact on businesses within the state would primarily result from the amended statute, and not the proposed regulations.

(3) It is unlikely that the proposed regulations would result in the expansion of businesses currently doing business within the state. Businesses are already required to comply with many existing privacy laws, including the CCPA and the existing CCPA regulations. Any new impact on businesses within the state would primarily result from the amended statute, and not the proposed regulations.

The Agency also concludes that:

(1) The proposed regulations would benefit the health and welfare of California residents by operationalizing the CPRA amendments to the CCPA, thus ensuring California residents are afforded greater privacy protections.

(2) The proposed regulations would not benefit worker safety because it does not regulate worker safety standards.

(3) The proposed regulations would not benefit the state's environment because it does not change any applicable environmental standards.

TECHNICAL, THEORETICAL, AND/OR EMPIRICAL STUDIES, REPORTS OR DOCUMENTS RELIED UPON

The documents and other materials relied on in connected with this rulemaking package are attached to this ISOR as Appendix A.

EVIDENCE SUPPORTING DETERMINATION OF NO SIGNIFICANT STATEWIDE ADVERSE ECONOMIC IMPACT DIRECTLY AFFECTING BUSINESS

The Agency has made an initial determination that the proposed action would not have a significant, statewide adverse economic impact directly affecting business, including the ability of California businesses to compete with businesses in other states. Businesses are already required to comply with many existing privacy laws, including the CCPA and the existing CCPA regulations. Any adverse economic impact affecting business results from the amended statute, and not the proposed regulations.

REASONABLE ALTERNATIVES TO THE PROPOSED REGULATORY ACTION THAT WOULD LESSEN ANY ADVERSE IMPACT ON SMALL BUSINESS

The Agency finds that no reasonable alternatives were presented to, or considered by, the Agency that would lessen any adverse impact on small business.

REASONABLE ALTERNATIVES TO THE PROPOSED ACTION AND THE AGENCY'S REASON FOR REJECTING THOSE ALTERNATIVES

The Agency considered several alternatives in drafting the proposed regulations. In considering the following alternatives, the Agency 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 7012, subdivisions (e) and (g) – Notice at Collection

Alternatives: The Agency considered and rejected the alternative of requiring a business to list the names of all third parties that control the collection of personal information in its notice at or before the point of collection.

Reasoning: The CPRA's amendments to the CCPA requires new obligations on third parties that control the collection of personal information to post a notice at collection on their websites. (Civ. Code, § 1798.100, subd. (a), (b).) However, without some disclosure of the identities of those third parties that control the collection of personal information, consumers do not know which third party websites to visit for their notices at collection. The Agency considered and rejected requiring businesses to identify the names of all third parties that control the collection of personal information in their notices at collection and instead provided businesses the option of either identifying those third parties or providing information about those third parties' data practices within its notice at collection. The Agency's approach here balances a mechanism by which the first party gives complete notice about all of the data collection that occurs, including by a third party, but does not require that that a consumer receive notice from multiple parties when interacting with one specific, first-party business. The Agency considered the alternative of how to best effectuate notice from the standpoint of the consumer receiving the notice, the burden on the business acting as a first party, and the relationship of the third party that is controlling the collection of personal information, and determined that the regulation required additional flexibility to satisfy the new notice obligations amended by the law.

Section 7015 – Alternative Opt-Out Link

Alternative: The Agency considered and rejected less prescriptive alternatives of allowing businesses to determine their own descriptive title and placement for the Alternative Opt-Out Link.

Reasoning: The Agency rejected the alternative of allowing businesses to craft their own descriptive title for the Alternative Opt-Out Link to avoid consumer confusion and to provide clear, prescriptive guidance to ensure uniformity. The Agency also determined that the single, opt-out link required specific language that referenced "privacy choices," and to the extent desired, "California," to avoid scenarios in which businesses created titles that could deter consumers from exercising their right to opt-out. For example, it would not further the purpose and intent of the law if businesses could name the Alternative Opt-Out Link, "No Data For Third Parties," because this title does not clearly reference that a consumer may exercise a privacy choice. (See Cranor et al., Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA, *supra*; Cranor et al., CCPA Opt-Out Icon Testing – Phase 2, *supra*.) The Agency also rejected a regulation that did not include

prescriptive language on the appropriate location, placement, and icon associated with the link, because it would be confusing for consumers who are searching for a link on a business's page, as well as more costly for businesses that already comply with existing requirements. (See Habib et al., An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites, which was presented at the Fifteenth Symposium on Usability and Security (August 12-13, 2019) p. 397; Mahoney, *supra*, pp. 21-23.) The rejected alternative would not advance the purpose and intent of the statute to give consumers meaningful control over businesses' use, sale, and sharing of their personal information.

Section 7022, subdivision (h) – Requests to Delete

Alternative: The Agency considered and rejected the alternative of requiring businesses to offer consumers the option to delete select categories of personal information.

Reasoning: The Agency rejected mandating businesses to offer consumers the option to delete select categories of personal information, and instead proposes language requiring businesses to inform consumers of their ability to delete select categories of personal information if that option is available to the consumer in other contexts. Giving businesses the flexibility to provide an option, as opposed to a requirement, balances the burden on businesses to implement this guidance, which for some businesses, may be costly. For businesses that have the capability to offer this choice, the regulation requires businesses to provide clear instructions to the consumers on how to exercise this right. This approach reduces burden on businesses, while providing consumers with knowledge and ability to control their personal information.

Section 7023 – Requests to Correct

Alternative: The Agency considered and rejected the following alternatives: (1) not applying the right to correct to unstructured data or information that is subjective in nature; (2) allowing businesses an absolute option to delete, not correct, information; (3) limiting requests to correct to only businesses that were the source of information; and (4) requiring businesses to accept and maintain a written statement from the consumer for contested personal information that the business has determined is correct.

***Reasoning*:** The Agency considered and rejected these alternative approaches because they were not less burdensome and equally effective in achieving the purposes of the CCPA. With respect to (1), completely barring a consumer's right to correct subjective or unstructured data may undermine the purpose of the right to correct, particularly when such incorrect personal information has a material impact on the consumer. That being said, the Agency recognizes that there may be instances in which subjective cannot be proven correct or incorrect, and the objective costs of correcting unstructured data may outweigh any benefit provided to the consumer. Accordingly, the Agency determined that the business is permitted to consider the nature of the information, including if it is unstructured or subjective, as part of its analysis in processing the request to correct. Instead of taking a prescriptive approach, the Agency reasoned that a business is required to consider the totality of the circumstances, including those that are unique to the business, in determining how to best effectuate the consumer's request.

With respect to (2), the Agency determined that a business may delete information that a consumer requests to be corrected, but limited this option to cases in which deletion would not negatively impact the consumer, or the consumer consents to the deletion should be corrected. This balances the consumer's right to have correct information in the business's possession, with the burden on the business to effectuate the consumer's request, including in a manner which is easiest for both the consumer and the business.

With respect to (3), the Agency determined that limiting this right to the source of the inaccurate information does not reflect the intent of the statute, nor the way in which a consumer's information is traded or purchased by other businesses. Both the source of the information and the source of the inaccuracy may not be known to the consumer, and in some cases, the source of the inaccuracy may not be known to the business. Limiting a consumer's ability to exercise the right to a correct to only the source of the information is too narrow to effectuate the purpose of the statute, and could also negatively impact businesses that maintain inaccurate information.

With respect to (4), the Agency considered allowing a consumer to provide a written addendum for all kinds of contested personal information, and not only personal information concerning a consumer's health as described in Civil Code section 1798.185, subdivision (a)(8)(D). The Agency weighed the burden on businesses in accepting and maintaining written addendums and determined that requiring businesses to maintain a notation in their system of the contested nature of the personal information is less burdensome to the business yet similarly effective in flagging the personal information as potentially less reliable, both to the business and downstream if the business were to sell or share that personal information with others. The balance struck here weighs the burden to the business with the effectiveness of the requirement.

Sections 7025 – Opt-Out Preference Signal

Alternative: The Agency considered and rejected the requirement that the opt-out preference signal express the consumer's request to limit the use and disclosure of sensitive personal information.

Reasoning: The Agency rejected this alternative to prioritize drafting regulations that operationalize and assist in the immediate implementation of the law. Technology already exists that expresses the opt-out preference signal as an expression of a consumer's right to stop the sale and sharing of personal information and businesses are required to comply with existing regulations that mandate processing a request to opt-out via a user-enabled global privacy control as set forth in California Code of Regulations, title 11, section 7026, subdivision (c). To conserve a business's resources to implement its response that complies with these new regulations, the Agency determined that the opt-out preference signal should remain narrow in scope. The Agency did not include regulations that addressed how consumers could express limiting the use and disclosure of sensitive personal information, or how a consumer may opt-in to the sale or sharing of personal information if the consumer is between the ages of 13 and 16 years or that consumer's parent or guardian if the consumer is less than 13 years of age. By focusing only on the sale or sharing of personal information, the Agency endeavors to reduce the burden on businesses to respond to new preference signals, and to allow innovation that communicate or signal the expression of these rights. It was also to prioritize the Agency's

limited resources in promulgating regulations as quickly as possible as required by the CPRA amendments.

No Revisions to Definition of Personal Information or Unique Identifiers

Alternative: The Agency considered and rejected alternatives to the definition of "personal information" or "unique identifiers" provided for in Civil Code section 1798.185, subdivisions (a)(1) and (a)(2).

Reasoning: Civil Code section 1798.185, subdivision (a)(1) and (a)(2), provide that the Agency shall adopt regulations that modify the definitions of personal information and unique identifiers "as needed" in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns. The Agency proposes these regulations in close proximity to the passage of the CPRA amendments, and no intervening technological changes or data collection practices warrant updating these definitions.

Performance Standard as Alternative:

Some of the proposed regulations mandate the use of specific technologies or equipment or prescribe specific actions or procedures. In those circumstances, the Agency rejected a performance standard as an alternative because a performance standard would not provide sufficient guidance for businesses.

Additional explanation regarding the Agency's mandate of a prescriptive standard is found in the following sections: 7003, 7004, 7012, 7013, 7014, 7015, 7023, 7025, and 7300.