TEXT OF REGULATIONS

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

ARTICLE 1. GENERAL PROVISIONS

§ 7001. Definitions.

In addition to the definitions set forth in Civil Code section 1798.140, for purposes of these regulations:

(a) "Agency" means the California Privacy Protection Agency established by Civil Code section 1798.199.10 et seq.

(b) "Alternative Opt-out Link" means the alternative opt-out link that a business may provide instead of posting the two separate "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links as set forth in Civil Code section 1798.135, subdivision (a)(3), and specified in section 7015.

(c) "Attorney General" means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General.

(d) "Authorized agent" means a natural person or a business entity that a consumer has authorized to act on their behalf subject to the requirements set forth in section 7063.

(e) "Automated decisionmaking technology" or "ADMT" means any technology that processes personal information and uses computation to replace human decisionmaking or substantially replace human decisionmaking.

(1) For purposes of this definition, to "substantially replace human decisionmaking" means a business uses the technology's output to make a decision without human involvement. Human involvement requires the human reviewer to:

(A) Know how to interpret and use the technology's output to make the decision;

(B) Review and analyze the output of the technology, and any other information that is relevant to make or change the decision; and

(C) Have the authority to make or change the decision based on their analysis in subsection (B).

(2) ADMT includes profiling that replaces human decisionmaking or substantially replaces human decisionmaking.

(3) ADMT does not include web hosting, domain registration, networking, caching, website-loading, data storage, firewalls, anti-virus, anti-malware, spam- and robocall-filtering, spellchecking, calculators, databases, and spreadsheets, provided that they do not replace human decisionmaking.

(f) ~~(e)~~ "Categories of sources" means types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

(g) ~~(f)~~ "Categories of third parties" means types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

(h) ~~(g)~~ "CCPA" means the California Consumer Privacy Act of 2018, Civil Code section 1798.100 et seq.

(i) ~~(h)~~ "COPPA" means the Children's Online Privacy Protection Act, 15 U.S.C. sections 6501 to 6506 and 16 Code of Federal Regulations part 312.

(j) "Cybersecurity audit" means the annual cybersecurity audit that every business whose processing of consumers' personal information presents

significant risk to consumers' security as set forth in section 7120, subsection (b), is required to complete.

(k) "Cybersecurity program" means the policies, procedures, and practices that protect personal information from unauthorized access, destruction, use, modification, or disclosure; and protect against unauthorized activity resulting in the loss of availability of personal information.

(*l*) "Cybersecurity audit report" means the document that every business must create as part of its cybersecurity audit. The cybersecurity audit report includes the information set forth in section 7123, subsection (e).

(m) ~~(i)~~ "Disproportionate effort" within the context of a business, service provider, contractor, or third party responding to a consumer request means the time and/or resources expended by the business, service provider, contractor, or third party to respond to the individualized request significantly outweighs the reasonably foreseeable impact to the consumer by not responding, taking into account applicable circumstances, such as the size of the business, service provider, contractor, or third party, the nature of the request, and the technical limitations impacting their ability to respond. For example, responding to a consumer request to know may require disproportionate effort when the personal information that is the subject of the request is not in a searchable or readily-accessible format, is maintained only for legal or compliance purposes, is not sold or used for any commercial purpose, and there is no reasonably foreseeable material impact to the consumer by not responding. By contrast, the impact to the consumer of denying a request to correct inaccurate information that the business uses and/or sells may outweigh the burden on the business, service provider, contractor, or third party in honoring the request when the reasonably foreseeable consequence of denying the request would be the denial of services or opportunities to the consumer. A business, service provider, contractor, or third party that has failed to put in place adequate processes and procedures to receive and process consumer requests in accordance with the CCPA and these regulations cannot claim that responding to a consumer's request requires disproportionate effort.

(n) ~~(j)~~ "Employment benefits" means retirement, health, and other benefit programs, services, or products to which consumers and their dependents or their beneficiaries receive access through the consumer's employer.

(o) ~~(k)~~ "Employment-related information" means personal information that is collected by the business about a natural person for the reasons identified in Civil Code section 1798.145, subdivision (m)(1). The collection of employment-related information, including for the purpose of administering employment benefits, shall be considered a business purpose.

(p) ~~(l)~~ "Financial incentive" means a program, benefit, or other offering, including payments to consumers, for the collection, retention, sale, or sharing of personal information. Price or service differences are types of financial incentives.

(q) ~~(m)~~ "First party" means a consumer-facing business with which the consumer intends and expects to interact.

(r) ~~(n)~~ "Frictionless manner" means a business's processing of an opt-out preference signal that complies with the requirements set forth in section 7025, subsection (f).

(s) ~~(o)~~ "Information practices" means practices regarding the collection, use, disclosure, sale, sharing, and retention of personal information.

(t) "Information system" means the resources (e.g., network, hardware, and software) organized for the processing of personal information or that can provide access to personal information. The business's information system includes the resources organized for the business's processing of personal information, regardless of whether the business owns those resources.

(u) "Multi-factor authentication" means authentication through verification of at least two of the following types of authentication factors: (1) knowledge factors, such as a password; (2) possession factors, such as a token; or (3) inherence factors, such as a biometric characteristic.

(v) ~~(p)~~ "Nonbusiness" means a person or entity that does not meet the definition of a "business" as defined in Civil Code section 1798.140, subdivision (d). For example, ~~non-profits and~~ government entities and many non-profits are nonbusinesses because ~~"business" is defined, among other things, to include only entities~~ they are not "organized or operated for the profit or financial benefit of its shareholders or other owners."

(w) ~~(q)~~ "Notice at Collection" means the notice given by a business to a consumer at or before the point at which a business collects personal information from the consumer as required by Civil Code section 1798.100, subdivisions (a) and (b), and specified in these regulations.

(x) ~~(r)~~ "Notice of Right to Limit" means the notice given by a business informing consumers of their right to limit the use or disclosure of the consumer's sensitive personal information as required by Civil Code sections 1798.121 and 1798.135 and specified in these regulations.

(y) ~~(s)~~ "Notice of Right to Opt-out of Sale/Sharing" means the notice given by a business informing consumers of their right to opt-out of the sale or sharing of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations.

(z) ~~(t)~~ "Notice of Financial Incentive" means the notice given by a business explaining each financial incentive or price or service difference as required by Civil Code section 1798.125, subdivision (b), and specified in these regulations.

(aa) ~~(u)~~ "Opt-out preference signal" means a signal that is sent by a platform, technology, or mechanism, on behalf of the consumer, that 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).

(bb) "Penetration testing" means testing the security of an information system by attempting to circumvent or defeat its security features by authorizing attempted penetration of the information system.

(cc) "Performance at work" means the performance of job duties for which the consumer has been hired or has applied to be hired. The following are not "performance at work": a consumer's union membership or interest in unionizing; a consumer's interest in seeking other employment opportunities; a consumer's location when off-duty or on breaks; or a consumer's use of a personal account (e.g., email, text messages, or social media) unless solely to prevent or limit the use of these accounts on the business's information system or to prevent the disclosure of confidential information.

(dd) "Performance in an educational program" means the performance of coursework in an educational program in which the consumer is enrolled or has

applied to be enrolled. The following are not "performance in an educational program": a consumer's use of a personal account (e.g., email, text messages, or social media) unless solely to prevent or limit the use of these accounts on the educational program provider's information system, including to prevent the disclosure of confidential information or to prevent cheating; or a consumer's location when they are not performing coursework.

(ee) "Physical or biological identification or profiling" means identifying or profiling a consumer using automated measurements or analysis of their physical or biological characteristics, or automated measurements or analysis of or relating to their body. This includes using biometric information, vocal intonation, facial expression, and gesture (e.g., to identify or infer emotion). This does not include processing physical or biological characteristics that do not identify, and cannot reasonably be linked with, a particular consumer.

(ff) ~~(v)~~ "Price or service difference" means (1) any difference in the price or rate charged for any goods or services to any consumer related to the collection, retention, sale, or sharing of personal information, or (2) any difference in the level or quality of any goods or services offered to any consumer related to the collection, retention, sale, or sharing of personal information, including the denial of goods or services to the consumer.

(gg) ~~(w)~~ "Privacy policy," as referred to in Civil Code sections 1798.130, subdivision (a)(5), and 1798.135, subdivision (c)(2), means the statement that a business shall make available to consumers describing the business's online and offline information practices, and the rights of consumers regarding their own personal information.

(hh) "Privileged account" means any authorized user account (i.e., an account designed to be used by an individual) or service account (i.e., an account designed to be used only by a service, not by an individual) that can be used to perform functions that other user accounts are not authorized to perform, including but not limited to the ability to add, change, or remove other accounts, or make configuration changes to an information system.

(ii) "Profiling" means any form of automated processing of personal information to evaluate certain personal aspects (including intelligence, ability, aptitude, predispositions) relating to a natural person and in particular to analyze or

predict aspects concerning that natural person's performance at work, economic situation, health (including mental health), personal preferences, interests, reliability, predispositions, behavior, location, or movements.

(jj) "Request to access ADMT" means a consumer request that a business provide information to the consumer about the business's use of ADMT with respect to the consumer, pursuant to Civil Code section 1798.185(a)(15) and Article 11.

(kk) "Request to appeal ADMT" means a consumer request to appeal the business's use of ADMT for a significant decision as set forth in section 7221, subsection (b)(1).

(*ll*) ~~(x)~~ "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.

(mm) ~~(y)~~ "Request to delete" means a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105.

(nn) ~~(z)~~ "Request to know" means a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections 1798.110 or 1798.115. It includes a request for any or all of the following:

(1) Specific pieces of personal information that a business has collected about the consumer;

(2) Categories of personal information it has collected about the consumer;

(3) Categories of sources from which the personal information is collected;

(4) Categories of personal information that the business sold, shared, or disclosed for a business purpose about the consumer;

(5) Categories of third parties to whom the personal information was sold, shared, or disclosed ~~for a business purpose~~; and

(6) The business or commercial purpose for collecting, ~~or~~ selling, or sharing personal information.

(oo) ~~(aa)~~ "Request to limit" means a consumer request that a business limit the use and disclosure of the consumer's sensitive personal information, pursuant to Civil Code section 1798.121, subdivision (a).

(pp) ~~(bb)~~ "Request to opt-in to sale/sharing" means an action demonstrating that the consumer has consented to the business's sale or sharing of personal information about the consumer by a parent or guardian of a consumer less than 13 years of age or by a consumer at least 13 years of age.

(qq) "Request to opt-out of ADMT" means a consumer request that a business not use ADMT with respect to the consumer, pursuant to Civil Code section 1798.185(a)(15) and Article 11.

(rr) ~~(cc)~~ "Request to opt-out of sale/sharing" means a consumer request that a business neither sell nor share the consumer's personal information to third parties, pursuant to Civil Code section 1798.120, subdivision (a).

(ss) "Right to access ADMT" means a consumer's right to request that a business provide information to the consumer about the business's use of ADMT with respect to the consumer as set forth in Civil Code section 1798.185(a)(15) and Article 11.

(tt) ~~(dd)~~ "Right to correct" means the consumer's right to request that a business correct inaccurate personal information that it maintains about the consumer as set forth in Civil Code section 1798.106.

(uu) ~~(ee)~~ "Right to delete" means the consumer's right to request that a business delete any personal information about the consumer that the business has collected from the consumer as set forth in Civil Code section 1798.105.

(vv) ~~(ff)~~ "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.

(ww) ~~(gg)~~ "Right to limit" means the consumer's right to request that a business limit the use and disclosure of a consumer's sensitive personal information as set forth in Civil Code section 1798.121.

(xx) "Right to opt-out of ADMT" means a consumer's right to direct that a business not use ADMT with respect to the consumer as set forth in Civil Code section 1798.185(a)(15) and Article 11.

(yy) ~~(hh)~~ "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.

(zz) "Risk assessment report" means the document that every business that is required to conduct a risk assessment must create as part of its risk assessment. The risk assessment report includes the information set forth in section 7152, subsections (a)(1)–(3), (6)–(9).

(aaa) "Sensitive location" means any of the following physical places: healthcare facilities including hospitals, doctors' offices, urgent care facilities, and community health clinics; pharmacies; domestic violence shelters; food pantries; housing/emergency shelters; educational institutions; political party offices; legal services offices; union offices; and places of worship.

(bbb) "Sensitive personal information" means:

(1) Personal information that reveals:

(A) A consumer's social security, driver's license, state identification card, or passport number.

(B) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

(C) A consumer's precise geolocation.

(D) A consumer's racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.

(E) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

(F) A consumer's genetic data.

(G) A consumer's neural data, which means information that is generated by measuring the activity of a consumer's central or peripheral nervous system, and that is not inferred from nonneural information.

(2) The processing of biometric information for the purpose of uniquely identifying a consumer.

(3) Personal information collected and analyzed concerning a consumer's health, sex life, or sexual orientation.

(4) Personal information of consumers that the business has actual knowledge are less than 16 years of age. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.

Sensitive personal information does not include information that is "publicly available" pursuant to Civil Code section 1798.140, subdivision (v)(2).

(ccc) ~~(ii)~~ "Signed" means that the written attestation, declaration, or permission has either been physically signed or provided electronically in accordance with the Uniform Electronic Transactions Act, Civil Code section 1633.1 et seq.

(ddd) "Significant decision" means a decision that results in the provision or denial of financial or lending services, housing, education enrollment or opportunities, employment or independent contracting opportunities or compensation, or healthcare services. For purposes of this definition:

(1) "Financial or lending services" means the extension of credit or a loan, transmitting or exchanging funds, the provision of deposit or checking accounts, check cashing, or installment payment plans.

(2) "Housing" means any building, structure, or portion thereof that is used or occupied as, or designed, arranged, or intended to be used or occupied as, a home, residence, or sleeping place by one or more consumers including for permanent or temporary occupancy. The use of ADMT that provides or denies housing to a consumer based solely on the availability or vacancy of the housing or the successful receipt of payment for housing from the consumer is not making a significant decision.

(3) "Education enrollment or opportunities" means:

(A) Admission or acceptance into academic or vocational programs;

(B) Educational credentials (e.g., a degree, diploma, or certificate); and

(C) Suspension and expulsion.

(4) "Employment or independent contracting opportunities or compensation" means:

(A) Hiring;

(B) Allocation or assignment of work for employees; or salary, hourly or per-assignment compensation, incentive compensation such as a bonus, or another benefit ("allocation/assignment of work and compensation");

(C) Promotion; and

(D) Demotion, suspension, and termination.

(5) "Healthcare services" means services related to the diagnosis, prevention, or treatment of human disease or impairment, or the assessment or care of an individual's health.

(6) Significant decision does not include advertising to a consumer.

(eee) "Systematic observation" means methodical and regular or continuous observation. This includes, for example, methodical and regular or continuous observation using Wi-Fi or Bluetooth tracking, radio frequency identification, drones, video or audio recording or live-streaming, technologies that enable physical or biological identification or profiling; and geofencing, location trackers, or license-plate recognition.

(fff) "Train" for the purposes of sections 7150, subsection (b)(6), and 7153 means the process through which a technology discovers underlying patterns, learns a series of actions, or is taught to generate a desired output. Examples of training include adjusting the parameters of an algorithm used for ADMT, improving the algorithm that determines how a machine-learning model learns, and iterating the datasets fed into ADMT.

(ggg) ~~(jj)~~ "Third-party identity verification service" means a security process offered by an independent third party that verifies the identity of the consumer making a request to the business. Third-party identity verification services are subject to the requirements set forth in Article 5 regarding requests to delete, requests to correct, or requests to know.

(hhh) ~~(kk)~~ "Unstructured" as it relates to personal information means personal information that is not organized in a pre-defined manner and could not be retrieved or organized in a pre-defined manner without disproportionate effort on behalf of the business, service provider, contractor, or third party.

(iii) ~~(ll)~~ "Value of the consumer's data" means the value provided to the business by the consumer's data as calculated under section 7081.

(jjj) ~~(mm)~~ "Verify" means to determine that the consumer making a request to delete, request to correct, ~~or~~ request to know, or request to access ADMT is the consumer about whom the business has collected information, or if that consumer is less than 13 years of age, the consumer's parent or legal guardian.

Note: Authority cited: Section~~s 1798.175 and~~ 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.175, 1798.185, 1798.199.40, 1798.199.45, 1798.199.50~~, 1798.199.55~~ and 1798.199.65, Civil Code.

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

(a) In accordance with Civil Code section 1798.100, subdivision (c), a business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve:

(1) The purpose(s) for which the personal information was collected or processed, which shall comply with the requirements set forth in subsection (b); or

(2) Another disclosed purpose that is compatible with the context in which the personal information was collected, which shall comply with the requirements set forth in subsection (c).

(b) The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s) whose

personal information is collected or processed. The consumer's (or consumers') reasonable expectations concerning the purpose for which their personal information will be collected or processed shall be based on the following:

(1) The relationship between the consumer(s) and the business. For example, if the consumer is intentionally interacting with the business on its website to purchase a good or service, the consumer likely expects that the purpose for collecting or processing the personal information is to provide that good or service. By contrast, for example, the consumer of a business's mobile flashlight application would not expect the business to collect the consumer's geolocation information to provide the flashlight service.

(2) The type, nature, and amount of personal information that the business plans ~~seeks~~ to collect or process. For example, if a business's mobile communication application requests access to the consumer's contact list in order to call a specific individual, the consumer who is providing their contact list likely expects that the purpose of the business's use of that contact list will be to connect the consumer with the specific contact they selected. Similarly, if a business collects the consumer's fingerprint in connection with setting up the security feature of unlocking the device using the fingerprint, the consumer likely expects that the business's use of the consumer's fingerprint is only for the purpose of unlocking their mobile device.

(3) The source of the personal information and the business's method for collecting or processing it. For example, if the consumer is providing their personal information directly to the business while using the business's product or service, the consumer likely expects that the business will use the personal information to provide that product or service. However, the consumer may not expect that the business will use that same personal information for a different product or service offered by the business or the business's subsidiary.

(4) The specificity, explicitness, prominence, and clarity of disclosures to the consumer(s) about the purpose for collecting or processing their personal information, such as in the Notice at Collection and in the marketing

materials to the consumer(s) about the business's good or service. For example, the consumer who receives a pop-up notice that the business wants to collect the consumer's phone number to verify their identity when they log in likely expects that the business will use their phone number for the purpose of verifying the consumer's identity and not for marketing purposes. Similarly, the consumer may expect that a mobile application that markets itself as a service that finds gas prices near the consumer's location will collect and use the consumer's geolocation information for that specific purpose when they are using the service.

(5) The degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer(s). For example, the consumer likely expects an online retailer's disclosure of the consumer's name and address to a delivery service provider in order for that service provider to deliver a purchased product, because that service provider's involvement is apparent to the consumer. By contrast, the consumer may not expect the disclosure of personal information to a service provider if the consumer is not directly interacting with the service provider or the service provider's role in the processing is not apparent to the consumer.

(c) Whether another disclosed purpose is compatible with the context in which the personal information was collected shall be based on the following:

(1) At the time of collection of the personal information, the reasonable expectations of the consumer(s) whose personal information is collected or processed concerning the purpose for which their personal information will be collected or processed, based on the factors set forth in subsection (b).

(2) The other disclosed purpose for which the business plans ~~seeks~~ to further collect or process the consumer's personal information, including whether it is a business purpose listed in Civil Code section 1798.140, subdivisions (e)(1) ~~through~~ – (e)(8).

(3) The strength of the link between subsection (c)(1) and subsection (c)(2). For example, a strong link exists between the consumer's reasonable expectations that the personal information will be used to provide them

with a requested service at the time of collection, and the use of the information to repair errors that impair the intended functionality of that requested service. This would weigh in favor of compatibility. By contrast, for example, a weak link exists between the consumer's reasonable expectations that the personal information will be collected to provide a requested cloud storage service at the time of collection, and the use of the information to research and develop an unrelated facial recognition service.

(d) For each purpose identified in compliance with subsection (a)(1) or (a)(2), the collection, use, retention, and/or sharing of a consumer's personal information to achieve that purpose shall be reasonably necessary and proportionate. The business's collection, use, retention, and/or sharing of a consumer's personal information shall also be reasonably necessary and proportionate to achieve any purpose for which the business obtains the consumer's consent in compliance with subsection (e). Whether a business's collection, use, retention, and/or sharing of a consumer's personal information is reasonably necessary and proportionate to achieve the purpose identified in compliance with subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent, shall be based on the following:

(1) The minimum personal information that is necessary to achieve the purpose identified in compliance with subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent. For example, to complete an online purchase and send an email confirmation of the purchase to the consumer, an online retailer may need the consumer's order information, payment and shipping information, and email address.

(2) The possible negative impacts on consumers posed by the business's collection or processing of the personal information. For example, a possible negative impact of collecting precise geolocation information is that it may reveal other sensitive personal information about the consumer, such as health information based on visits to healthcare providers.

(3) The existence of additional safeguards for the personal information to specifically address the possible negative impacts on consumers considered by the business in subsection (d)(2). For example, a business

may consider encryption or automatic deletion of personal information within a specific window of time as potential safeguards.

(e) A business shall obtain the consumer's consent in accordance with section 7004 before collecting or processing personal information for any purpose that does not meet the requirements set forth in subsection (a). Except as set forth Civil Code section 1798.145, subdivision (r), or as otherwise prohibited by the CCPA, a consumer must be able to withdraw consent at any time.

(f) A business shall not collect categories of personal information other than those disclosed in its Notice at Collection in accordance with the CCPA and section 7012. If the business intends to collect additional categories of personal information or intends to use the personal information for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, the business shall provide a new Notice at Collection. However, any additional collecting or processing of personal information shall comply with subsections (a) – (e).

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.106, 1798.121, 1798.130, 1798.135 and 1798.185, Civil Code.

§ 7003. Requirements for Disclosures and Communications to Consumers.

(a) Disclosures and communications to consumers shall be easy to read and understandable to consumers. For example, they shall use plain, straightforward language and avoid technical or legal jargon.

(b) Disclosures required under Article 2 shall also:

(1) Use a format that makes the disclosure readable, including on smaller screens, if applicable.

(2) Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.

(3) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated

herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the policy in an alternative format.

(c) For websites, a conspicuous link required under the CCPA or these regulations shall appear in a similar manner as other similarly-posted links used by the business on its homepage(s). For example, the business shall use a font size and color that is at least the approximate size or color as other links next to it that are used by the business on ~~its homepage(s)~~ any internet webpage where personal information is collected.

(d) For mobile applications, a conspicuous link shall be included in the business's privacy policy, which must be accessible through the mobile application's platform page or download page. It ~~may~~ must also be accessible through a link within the application, such as through the application's settings menu.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130 and 1798.135, Civil Code.

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

(a) Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles:

(1) Easy to understand. The methods shall use language that is easy for consumers to read and understand. When applicable, they shall comply with the requirements for disclosures to consumers set forth in section 7003.

(2) Symmetry in choice. The path for a consumer to exercise a more privacy-protective option shall not be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option because that would impair or interfere with the consumer's ability to make a choice. Illustrative examples and requirements follow.

(A) It is not symmetrical when a business's process for submitting a request to opt-out of sale/sharing requires more steps than that business's process for ~~a consumer to~~ opting-in to the sale of personal information ~~after having previously opted out~~. For example, the ~~The~~ number of steps for submitting a request to opt-out of sale/sharing as ~~is~~ measured from when the consumer clicks on the "Do Not Sell or Share My Personal Information" link to completion of the request should be the same or fewer than the ~~The.~~ number of steps for submitting a request to opt-in to the sale of personal information where the business offers a link for consumers to learn more about opting-in to the business's sale or sharing of their personal information ~~is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request~~.

(B) A choice to opt-in to the sale of personal information that provides only the two options, "Yes" and "Ask me later," is not equal or symmetrical because there is no option to decline the opt-in. "Ask me later" implies that the consumer has not declined but delayed the decision and that the business will continue to ask the consumer to opt-in. Framing the consumer's options in this manner impairs the consumer's ability to make a choice. An equal or symmetrical choice could be between "Yes" and "No."

(C) A website banner that provides only the two options, "Accept All" and "More Information," or, "Accept All" and "Preferences," when seeking the consumer's consent to use their personal information is not equal or symmetrical because the method allows the consumer to "Accept All" in one step, but requires the consumer to take additional steps to exercise their rights over their personal information. Framing the consumer's options in this manner impairs the consumer's ability to make a choice. An equal or symmetrical choice could be between "Accept All" and "Decline All."

(D) A choice where the "yes" button is more prominent (e.g., larger in size or in a more eye-catching color) than the "no" button is not equal or symmetrical.

(E) A choice where the option to participate in a financial incentive program is selected by default or featured more prominently (e.g., larger in size or in a more eye-catching color) than the choice not to participate in the program is neither equal nor symmetrical.

(3) ~~Avoid~~ Do not use language or interactive elements that are confusing to the consumer. The methods ~~should~~ must not use double negatives, misleading statements or omissions, affirmative misstatements, or deceptive language. Toggles or buttons must clearly indicate the consumer's choice. A consumer's silence or failure to act affirmatively does not constitute consent. Illustrative examples of prohibited methods follow.

(A) Giving the choice of "Yes" or "No" next to the statement "Do Not Sell or Share My Personal Information" is a double negative and a confusing choice for a consumer.

(B) Toggles or buttons that state "on" or "off" ~~may be~~ are confusing to a consumer ~~and may require~~ if they do not include further clarifying language.

(C) The u~~U~~nintuitive placement of buttons to confirm a consumer's choice ~~may be~~ is confusing to the consumer. For example, it is confusing to the consumer when a business at first consistently offers choices in the order of "Yes," then "No," but then offers choices in the opposite order—"No," then "Yes"—when asking the consumer something that would contravene the consumer's expectation.

(D) A consumer closing or navigating away from a pop-up window on a website that requests consent without first affirmatively selecting the equivalent of an "I accept" button shall not constitute consent. Such a method for obtaining consent is confusing to the consumer.

(E) Choices driven by a false sense of urgency are misleading. A countdown clock displayed next to a consent choice which states "time is running out to consent to this data use and receive a limited discount" where the discount is not actually limited by time or availability is misleading.

(4) ~~Avoid~~ Do not use choice architecture that impairs or interferes with the consumer's ability to make a choice. Businesses ~~should also~~ must not design their methods in a manner that would impair the consumer's ability to exercise their choice because consent must be freely given, specific, informed, and unambiguous. Illustrative examples and requirements follow.

(A) Requiring the consumer to click through disruptive screens before they are able to submit a request to opt-out of sale/sharing is a choice architecture that impairs or interferes with the consumer's ability to exercise their choice.

(B) Bundling choices so that the consumer is only offered the option to consent to using personal information for purposes that meet the requirements set forth in section 7002, subsection (a), together with purposes that are incompatible with the context in which the personal information was collected is a choice architecture that impairs or interferes with the consumer's ability to make a choice. For example, a business that provides a location-based service, such as a mobile application that finds gas prices near the consumer's location, shall not require the consumer to consent to incompatible uses (e.g., sale of the consumer's geolocation to data brokers) together with a reasonably necessary and proportionate use of geolocation information for providing the location-based services, which does not require consent. This type of choice architecture does not allow consent to be freely given, specific, informed, or unambiguous because it requires the consumer to consent to incompatible uses in order to obtain the expected service. The business ~~should~~ must provide the consumer a separate option to consent to the business's use of personal information that does not meet the requirements set forth in section 7002, subsection (a).

(C) Acceptance of general or broad terms of use, or a similar document, that contains descriptions of personal information processing along with other, unrelated information. This type of choice architecture prevents consent from being freely given, specific, and informed, or from signifying agreement for a narrowly defined particular purpose.

(5) Easy to execute. The business shall not add unnecessary burden or friction to the process by which the consumer submits a CCPA request or provides or withdraws consent. Methods ~~should~~ must be tested to ensure that they are functional and do not undermine the consumer's choice to submit the request. Illustrative examples and requirements follow.

(A) Upon clicking the "Do Not Sell or Share My Personal Information" link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out of sale/sharing.

(B) A business that knows of, but does not remedy, circular or broken links, or nonfunctional email addresses, such as inboxes that are not monitored or have aggressive filters that screen emails from the public, may be in violation of this regulation.

(C) Businesses that require the consumer to unnecessarily wait on a webpage as the business processes the request or require consumers to fill out multiple or duplicative forms or impose unnecessary waiting periods between form submissions may be in violation of this regulation.

(D) Businesses that require the consumer to call a toll-free telephone number to submit a CCPA request must ensure that the individuals handling those phone calls have the knowledge and ability to process the consumer's CCPA requests.

(b) A method that does not comply with subsection (a) may be ~~considered~~ a dark pattern. The illustrative examples provided in subsection (a) constitute a non-exhaustive list of dark patterns. Any agreement obtained through the use of dark patterns shall not constitute consumer consent. For example, a business that uses dark patterns to obtain consent from a consumer to sell their personal information shall be in the position of never having obtained the consumer's consent to do so.

(c) A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice. A business's intent in designing the interface is not determinative in whether the user

interface is a dark pattern, but a factor to be considered. If a business did not intend to design the user interface to subvert or impair user choice, but the business knows of and does not remedy a user interface that has that effect, the user interface is ~~may~~ still ~~be~~ a dark pattern. ~~Similarly, a business's deliberate ignorance of the effect of its user interface may also weigh in favor of establishing a dark pattern.~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

ARTICLE 2. REQUIRED DISCLOSURES TO CONSUMERS

§ 7010. Overview of Required Disclosures.

(a) Every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and section 7011.

(b) A business that controls the collection of a consumer's personal information from a consumer shall provide a Notice at Collection in accordance with the CCPA and section 7012.

(c) A business that uses ADMT as set forth in section 7200, subsection (a), must provide consumers with a Pre-use Notice in accordance with section 7220.

(d) Except as set forth in section 7221, subsection (b), a business that uses ADMT as set forth in section 7200, subsection (a), must include in its Pre-use Notice a link through which consumers can opt-out of the business's use of ADMT, in accordance with section 7221, subsection (c)(1).

(e) ~~(c)~~ Except as set forth in section 7025, subsection (g), a business that sells or shares personal information shall provide a Notice of Right to Opt-out of Sale/Sharing or the Alternative Opt-out Link in accordance with the CCPA and sections 7013 and 7015.

(f) ~~(d)~~ A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in section 7027, subsection (m), shall provide a Notice of Right to Limit or the Alternative Opt-out Link in accordance with the CCPA and sections 7014 and 7015.

(g) ~~(e)~~ A business that offers a financial incentive or price or service difference shall provide a Notice of Financial Incentive in accordance with the CCPA and section 7016.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, ~~and~~ 1798.135, and 1798.185, Civil Code.

§ 7011. Privacy Policy.

(a) The purpose of the privacy policy is to provide consumers with a comprehensive description of a business's online and offline information practices. It shall also inform consumers about the rights they have regarding their personal information and provide any information necessary for them to exercise those rights.

(b) The privacy policy shall comply with section 7003, subsections (a) and (b).

(c) The privacy policy shall be available in a format that allows a consumer to print it out as a document.

(d) The privacy policy shall be posted online and accessible through a conspicuous link that complies with section 7003, subsections (c) and (d), using the word "privacy" on the business's website homepage(s) or on the download or landing page of a mobile application. If the business has a California-specific description of consumers' privacy rights on its website, then the privacy policy shall be included in that description. A business that does not operate a website shall make the privacy policy conspicuously available to consumers. A mobile application ~~may~~ must also include a link to the privacy policy in the application's settings menu.

(e) The privacy policy shall include the following information:

(1) A comprehensive description of the business's online and offline information practices, which includes the following:

(A) Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described using the specific terms set forth in Civil Code section 1798.140, subdivisions (v)(1)(A) ~~to~~ – (K) and (ae)(1)

~~to~~ – (2). To the extent that the business has discretion in its description, the business shall describe the category in a manner that provides consumers a meaningful understanding of the information being collected.

(B) Identification of the categories of sources from which the personal information is collected. The categories shall be described in a manner that provides consumers a meaningful understanding of where the information is collected.

(C) Identification of the specific business or commercial purpose for collecting personal information from consumers. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected.

(D) Identification of the categories of personal information, if any, that the business has sold or shared to third parties in the preceding 12 months. If the business has not sold or shared consumers' personal information in the preceding 12 months, the business shall disclose that fact.

(E) For each category of personal information identified in subsection (e)(1)(D), the categories of third parties to whom the information was sold or shared. The categories of third parties shall be described in a manner that provides consumers a meaningful understanding of the parties to whom the information is sold or shared.

(F) Identification of the specific business or commercial purpose for selling or sharing consumers' personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is sold or shared.

(G) A statement regarding whether the business has actual knowledge that it sells or shares the personal information of consumers under 16 years of age.

(H) Identification of the categories of personal information, if any, that the business has disclosed to a service provider or contractor for a business purpose ~~to third parties~~ in the preceding 12 months. If the

business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(I) ~~For each category of personal information identified in subsection (c)(1)(H), the categories of third parties to whom the information was disclosed. (J)~~ Identification of the specific business or commercial purpose for disclosing the consumer's personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is disclosed.

(J) ~~(K)~~ A statement regarding whether the business uses or discloses sensitive personal information for purposes other than those specified in section 7027, subsection (m).

(2) An explanation of the rights that the CCPA confers on consumers regarding their personal information, which includes all of the following:

(A) The right to know what personal information the business has collected about the consumer, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom the business discloses personal information, and the specific pieces of personal information the business has collected about the consumer.

(B) The right to delete personal information that the business has collected from the consumer, subject to certain exceptions.

(C) The right to correct inaccurate personal information that a business maintains about a consumer.

(D) If the business sells or shares personal information, the right to opt-out of the sale or sharing of their personal information by the business.

(E) If the business uses or discloses sensitive personal information for reasons other than those set forth in section 7027, subsection (m),

the right to limit the use or disclosure of sensitive personal information by the business.

(F) Except as set forth in section 7221, subsection (b), if the business uses ADMT as set forth in section 7200, subsection (a), the right to opt-out of ADMT.

(G) If the business uses ADMT as set forth in section 7200, subsection (a), the right to access ADMT.

(H) The right not to be retaliated against ~~receive discriminatory treatment by the business for the exercise of~~ for exercising privacy rights conferred by the CCPA, including when a consumer is an applicant to an educational program, a job applicant, a student, an employee~~'s, applicant's~~, or an independent contractor~~'s right not to be retaliated against for the exercise of their CCPA rights~~.

(3) An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes all of the following:

(A) An explanation of the methods by which the consumer can exercise their CCPA rights.

(B) Instructions for submitting a request under the CCPA, including any links to an online request form or portal for making such a request, if offered by the business.

(C) If the business sells or shares personal information, and is required to provide a Notice of Right to Opt-out of Sale/Sharing, the contents of the Notice of Right to Opt-out of Sale/Sharing or a link to that notice in accordance with section 7013, subsection (f).

(D) If the business uses or discloses sensitive personal information for purposes other than those specified in section 7027, subsection (m), and is required to provide a Notice of Right to Limit, the contents of the Notice of Right to Limit or a link to that notice in accordance with section 7014, subsection (f).

(E) A general description of the process the business uses to verify a consumer request to know, request to delete, ~~and~~ request to correct, and request to access ADMT, when applicable, including any information the consumer must provide.

(F) Explanation of how an opt-out preference signal will be processed for the consumer (i.e., whether the signal applies to the device, browser, consumer account, and/or offline sales, and in what circumstances) and how the consumer can use an opt-out preference signal.

(G) If the business processes opt-out preference signals in a frictionless manner, information on how consumers can implement opt-out preference signals for the business to process in a frictionless manner.

(H) Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf.

(I) If the business has actual knowledge that it sells the personal information of consumers under 16 years of age, a description of the processes required by sections 7070 and 7071.

(J) A contact for questions or concerns about the business's privacy policies and information practices using a method reflecting the manner in which the business primarily interacts with the consumer.

(4) Date the privacy policy was last updated.

(5) If subject to the data reporting requirements set forth in section 7102, the information required under section 7102, or a link to that information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, ~~and~~ 1798.135, and 1798.185, Civil Code.

§ 7012. Notice at Collection of Personal Information.

(a) The purpose of the Notice at Collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal

information to be collected from them, the purposes for which the personal information is collected or used, and whether that information is sold or shared, so that consumers have a tool to exercise meaningful control over the business's use of their personal information. For example, upon receiving the Notice at Collection, the consumer can use the information in the notice as a tool to choose whether 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 their sensitive personal information.

(b) The Notice at Collection shall comply with section 7003, subsections (a) and (b).

(c) The Notice at Collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information. Illustrative examples follow.

(1) When a business collects consumers' personal information online, it may post a conspicuous link to the notice on the introductory page of the business's website and on all webpages where personal information is collected.

(2) When a business collects consumers' personal information through a webform, it may post a conspicuous link to the notice in close proximity to the fields in which the consumer inputs their personal information, or in close proximity to the button by which the consumer submits their personal information to the business.

(3) When a business collects personal information through a mobile application, it may provide a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu.

(4) When a business collects consumers' personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online.

(5) When a business collects personal information over the telephone or in person, it may provide the notice orally.

(d) If a business does not give the Notice at Collection to the consumer at or before the point of collection of their personal information, the business shall not collect personal information from the consumer.

(e) A business shall include the following in its Notice at Collection:

(1) A list of the categories of personal information about consumers, including categories of sensitive personal information, to be collected. Each category of personal information shall be written in a manner that provides consumers a meaningful understanding of the information being collected.

(2) The purpose(s) for which the categories of personal information, including categories of sensitive personal information, are collected and used.

(3) Whether each category of personal information identified in subsection (e)(1) is sold or shared.

(4) The length of time the business intends to retain each category of personal information identified in subsection (e)(1), or if that is not possible, the criteria used to determine the period of time it will be retained.

(5) If the business sells or shares personal information, the link to the Notice of Right to Opt-out of Sale/Sharing, or in the case of offline notices, where the webpage can be found online.

(6) A link to the business's privacy policy, or in the case of offline notices, where the privacy policy can be found online.

(f) If a business collects personal information from a consumer online, the Notice at Collection may be given to the consumer 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 subsections (e)(1) ~~through~~ – (6). Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain the required information, so that the consumer is required to scroll through other information ~~in order~~ to determine

the categories of personal information to be collected and/or whether the business sells or shares the personal information collected, does not satisfy this standard.

(g) Third Parties that Control the Collection of Personal Information. This subsection shall not affect the first party's obligations under the CCPA to comply with a consumer's request to opt-out of sale/sharing.

(1) For purposes of giving Notice at Collection, more than one business may control the collection of a consumer's personal information, and thus, have an obligation to provide a Notice at Collection in accordance with the CCPA and these regulations. For example, a first party may allow another business, acting as a third party, to control the collection of personal information from consumers browsing the first party's website. Both the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall provide a Notice at Collection. The first party and third parties may provide a single Notice at Collection that includes the required information about their collective information practices.

(2) A business that, acting as a third party, controls the collection of personal information on another business's physical premises, such as in a retail store or in a vehicle, shall provide a Notice at Collection in a conspicuous manner at the physical location(s) where it is collecting the personal information.

(3) Illustrative examples follow.

(A) Business F allows Business G, a third party ad network, to collect consumers' personal information through Business F's website. Business F may post a conspicuous link to its Notice at Collection on its homepage(s). Business G shall provide a Notice at Collection on its homepage(s) or include the required information about its information practices in Business F's Notice at Collection.

(B) Business H, a coffee shop, allows Business I, a business providing Wi-Fi services, to collect personal information from consumers using Business I's services on Business H's premises. Business H may post conspicuous signage at the entrance of the store or at the point-of-

sale directing consumers to where the Notice at Collection for Business H can be found online. In addition, Business I shall post its own Notice at Collection on the first webpage or other interface consumers see before connecting to the Wi-Fi services offered.

(C) Business J, a car rental business, allows Business K to collect personal information from consumers within the vehicles Business J rents to consumers. Business J may give its Notice at Collection to the consumer at the point of sale (i.e., at the rental counter) either in writing or orally. Business K may provide its own Notice at Collection within the vehicle, such as through signage on the vehicle's dashboard directing consumers to where the notice can be found online.

(h) A business that neither collects nor controls the collection of personal information directly from the consumer does not need to provide a Notice at Collection to the consumer if it neither sells nor shares the consumer's personal information.

(i) A data broker registered with the Attorney General pursuant to Civil Code section 1798.99.80 et seq. that collects personal information from a source other than directly from the consumer does not need to provide a Notice at Collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out of sale/sharing.

Note: Authority: Section 1798.185, Civil Code. Reference: Sections 1798.99.82, 1798.100, 1798.115, 1798.120, 1798.121, 1798.145 and 1798.185, Civil Code.

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

(a) The purpose of the Notice of Right to Opt-out of Sale/Sharing is to inform consumers of their right to direct a business that sells or shares their personal information to stop selling or sharing their personal information and to provide them with the opportunity to exercise that right. The purpose of the "Do Not Sell or Share My Personal Information" link is to immediately effectuate the consumer's right to opt-out of sale/sharing, or in the alternative, direct the consumer to the Notice of Right to Opt-out of Sale/Sharing. Accordingly,

clicking the business's "Do Not Sell or Share My Personal Information" link will either have the immediate effect of opting the consumer out of the sale or sharing of personal information or lead the consumer to a webpage where the consumer can learn about and make that choice.

(b) The Notice of Right to Opt-out of Sale/Sharing shall comply with section 7003, subsections (a) and (b).

(c) The "Do Not Sell or Share My Personal Information" link shall be a conspicuous link that complies with section 7003, subsections (c) and (d) and is located at either the header or footer of the business's internet homepage(s).

(d) In lieu of posting the "Do Not Sell or Share My Personal Information" link, a business may provide the Alternative Opt-out Link in accordance with section 7015 or process opt-out preference signals in a frictionless manner in accordance with section 7025, subsections (f) and (g). The business must still post a Notice of Right to Opt-out of Sale/Sharing in accordance with these regulations.

(e) A business that sells or shares the personal information of consumers shall provide the Notice of Right to Opt-out of Sale/Sharing to consumers as follows:

(1) A business shall post the Notice of Right to Opt-out of Sale/Sharing on the internet webpage to which the consumer is directed after clicking on the "Do Not Sell or Share My Personal Information" link. The notice shall include the information specified in subsection (f) or be a link that takes the consumer directly to the specific section of the business's privacy policy that contains the same information. 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 opt-out preference signals in a frictionless manner and chooses not to post a link, the business shall provide the notice within its privacy policy.

(2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to opt-out of sale/sharing. That method shall comply with the requirements set forth in section 7003.

(3) A business shall also provide the notice to opt-out of sale/sharing in the same manner in which it collects the personal information that it sells or shares. Illustrative examples and requirements follow.

(A) A business that sells or shares personal information that it collects in the course of interacting with consumers offline, such as in a brick-and-mortar store, shall provide notice through an offline method, e.g., on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the notice can be found online.

(B) A business that sells or shares personal information that it collects over the phone shall provide notice orally during the call when the information is collected.

(C) A business that sells or shares personal information that it collects through a connected device (e.g., a smart television or a smart watch) shall provide notice in a manner that ensures that the consumer will encounter the notice before or at the time the device begins collecting the personal information that it sells or shares.

(D) A business that sells or shares personal information that it collects in augmented or virtual reality, such as through gaming devices or mobile applications, shall provide notice in a manner that ensures that the consumer will encounter the notice either: (1) before or at the time the consumer enters the augmented or virtual reality environment; or (2) before or at the time the consumer encounters the business within the augmented or virtual reality environment.

(f) A business shall include the following in its Notice of Right to Opt-out of Sale/Sharing:

(1) A description of the consumer's right to opt-out of the sale or sharing of their personal information by the business; and

(2) Instructions on how the consumer can submit a request to opt-out of sale/sharing. If notice is provided online, the notice shall include the interactive form by which the consumer can submit their request to opt-

out of sale/sharing online, as required by section 7026, subsection (a)(1). If the business does not operate a website, the notice shall explain the offline method by which the consumer can submit their request to opt-out of sale/sharing.

(g) A business does not need to provide a Notice of Right to Opt-out of Sale/Sharing or the "Do Not Sell or Share My Personal Information" link if:

(1) It does not sell or share personal information; and

(2) It states in its privacy policy that it does not sell or share personal information.

(h) A business shall not sell or share the personal information it collected during the time the business did not have a Notice of Right to Opt-out of Sale/Sharing posted unless it obtains the consent of the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

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

(a) The purpose of the Notice of Right to Limit is to inform consumers of their right to limit a business's use and disclosure of their sensitive personal information and to provide them with the opportunity to exercise that right. The purpose of the "Limit the Use of My Sensitive Personal Information" link is to immediately effectuate the consumer's right to limit, or in the alternative, direct the consumer to the Notice of Right to Limit. Accordingly, clicking the business's "Limit the Use of My Sensitive Personal Information" link will either have the immediate effect of limiting the use and disclosure of the consumer's sensitive personal information or lead the consumer to a webpage where the consumer can learn about and make that choice.

(b) The Notice of Right to Limit shall comply with section 7003, subsections (a) and (b).

(c) The "Limit the Use of My Sensitive Personal Information" link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and

is located at either the header or footer of the business's internet homepage(s).

(d) In lieu of posting the "Limit the Use of My Sensitive Personal Information" link, a business may provide the Alternative Opt-out Link in accordance with section 7015. The business shall still post a Notice of Right to Limit in accordance with these regulations.

(e) A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in section 7027, subsection (m), shall provide the Notice of Right to Limit to consumers as follows:

(1) A business shall post the Notice of Right to Limit on the internet webpage to which the consumer is directed after clicking on the "Limit the Use of My Sensitive Personal Information" link. The notice shall include the information specified in subsection (f) or be a link that takes the consumer directly to the specific section of the business's privacy policy that contains the same information. If clicking on the "Limit the Use of My Sensitive Personal Information" link immediately effectuates the consumer's right to limit, the business shall provide the notice within its privacy policy.

(2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to limit. That method shall comply with the requirements set forth in section 7003.

(3) A business shall also provide the Notice of Right to Limit in the same manner in which it collects the sensitive personal information that it uses or discloses for purposes other than those specified in Section 7027, subsection (m). Illustrative examples and requirements follow.

(A) A business that uses or discloses sensitive personal information that it collects in the course of interacting with consumers offline, such as in a brick-and-mortar store, for purposes other than those specified in section 7027, subsection (m), shall provide notice through an offline method (e.g., on the paper forms that collect the sensitive personal information or by posting signage in the area

where the sensitive personal information is collected directing consumers to where the notice can be found online).

(B) A business that uses or discloses sensitive personal information that it collects over the phone for purposes other than those specified in section 7027, subsection (m), shall provide notice orally during the call when the information is collected.

(C) A business that uses or discloses sensitive personal information that it collects through a connected device (e.g., a smart television or a smart watch) for purposes other than those specified in section 7027, subsection (m), shall provide notice in a manner that ensures that the consumer will encounter the notice before or at the time the device begins collecting the personal information that it uses or discloses for those purposes.

(D) A business that uses or discloses sensitive personal information that it collects in augmented or virtual reality, such as through gaming devices or mobile applications, for purposes other than those specified in section 7027, subsection (m), shall provide notice in a manner that ensures that the consumer will encounter the notice either: (1) before the consumer enters the augmented or virtual reality environment; or (2) before or at the time the business collects the personal information within the augmented or virtual reality environment.

(f) A business shall include the following in its Notice of Right to Limit:

(1) A description of the consumer's right to limit; and

(2) Instructions on how the consumer can submit a request to limit. If notice is provided online, the notice shall include the interactive form by which the consumer can submit their request to limit online, as required by section 7027, subsection (b)(1). If the business does not operate a website, the notice shall explain the offline method by which the consumer can submit their request to limit.

(g) A business does not need to provide a Notice of Right to Limit or the "Limit the Use of My Sensitive Personal Information" link if:

(1) It only uses and discloses sensitive personal information that it collected about the consumer for the purposes specified in section 7027, subsection (m), and states so in its privacy policy; or

(2) It only collects or processes sensitive personal information without the purpose of inferring characteristics about a consumer, and states so in its privacy policy.

(h) A business shall not use or disclose sensitive personal information it collected during the time the business did not have a Notice of Right to Limit posted for purposes other than those specified in section 7027, subsection (m), unless it obtains the consent of the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.121, 1798.135 and 1798.185, Civil Code.

§ 7015. Alternative Opt-out Link.

(a) The purpose of the Alternative Opt-out Link is to provide businesses the option of providing consumers with a single, clearly-labeled link that allows consumers to easily exercise both their right to opt-out of sale/sharing and right to limit, instead of posting the two separate "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links. The Alternative Opt-out Link shall direct the consumer to a webpage that informs them of both their right to opt-out of sale/sharing and right to limit and provides them with the opportunity to exercise both rights.

(b) A business that chooses to use an Alternative Opt-out Link shall title the link, "Your Privacy Choices," or, "Your California Privacy Choices," and shall include the following opt-out icon adjacent to the title.

(1) The link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business's internet homepage(s).

(2) The icon shall be approximately the same size as other icons used by the business in the header or footer of its webpage.

(3) Businesses may adjust the color of the icon to ensure that the icon is conspicuous. For example, if the webpage background is the same color

of blue as the icon, the business may invert or change the colors of the icon to ensure visibility.

(c) The Alternative Opt-out Link shall direct the consumer to a webpage that includes the following information:

(1) A description of the consumer's right to opt-out of sale/sharing and right to limit, which shall comply with section 7003, subsections (a) and (b); and

(2) The interactive form or mechanism by which the consumer can submit their request to opt-out of sale/sharing and their right to limit online. The method shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.121, 1798.135 and 1798.185, Civil Code.

ARTICLE 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

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

(a) A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to delete, requests to correct, and requests to know.

(b) A business that does not fit the description in subsection (a) shall provide two or more designated methods for submitting requests to delete, requests to correct, and requests to know. One of those methods must be a toll-free telephone number. If the business maintains an internet website, one of the methods for submitting these requests shall be through its website, such as through a webform. Other methods for submitting requests to delete, requests to correct, and requests to know may include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.

(c) A business shall consider the methods by which it primarily interacts with consumers when determining which methods to provide for submitting requests to delete, requests to correct, and requests to know. If the business interacts with consumers in person, the business shall consider providing an in-person method such as a printed form the consumer can directly submit or send by mail, a tablet or computer portal that allows the consumer to complete and submit an online form, or a telephone with which the consumer can call the business's toll-free number.

(d) A business may use a two-step process for online requests to delete where the consumer must first, submit the request to delete and then second, separately confirm that they want their personal information deleted provided that the business otherwise complies with section 7004.

(e) If a business maintains personal information for longer than 12 months, its method for consumers to submit requests to know shall include a means by which the consumer can request that the business provide personal information collected prior to the 12-month period preceding the business's receipt of the consumer's request. For example, the business may ask the consumer to select or input the date range for which the consumer is making the request to know or present the consumer with an option to request all personal information the business has collected about the consumer. Use of this method is not required for personal information collected prior to January 1, 2022, pursuant to Civil Code section 1798.130, subdivision (a)(2)(B).

(f) If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either:

(1) Treat the request as if it had been submitted in accordance with the business's designated manner, or

(2) Provide the consumer with information on how to submit the request or remedy any deficiencies with the request, if applicable.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.

§ 7021. Timelines for Responding to Requests to Delete, Requests to Correct, ~~and~~ Requests to Know, Requests to Access ADMT, and Requests to Appeal ADMT.

(a) No later than 10 business days after receiving a request to delete, request to correct, ~~or~~ request to know, request to access ADMT, or request to appeal ADMT, a business shall confirm receipt of the request and provide information about how the business will process the request. The information provided shall describe in general the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request. The confirmation may be given in the same manner in which the request was received. For example, if the request is made over the phone, the confirmation may be given orally during the phone call.

(b) Businesses shall respond to a request to delete, request to correct, ~~and~~ request to know, request to access ADMT, and request to appeal ADMT no later than 45 calendar days after receipt of the request. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request. If the business cannot verify the consumer within the 45-day time period, the business may deny the request. If necessary, businesses may take up to an additional 45 calendar days to respond to the consumer's request, for a maximum total of 90 calendar days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.

§ 7022. Requests to Delete.

(a) For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 5, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified.

(b) A business shall comply with a consumer's request to delete their personal information by doing all of the following:

(1) Permanently and completely erasing the personal information from its existing systems except archived or backup systems, deidentifying the personal information, or aggregating the consumer information.;

(2) Notifying the business's service providers or contractors of the need to delete from their records the consumer's personal information that they collected pursuant to their written contract with the business, or if enabled to do so by the service provider or contractor, the business shall delete the personal information that the service provider or contractor collected pursuant to their written contract with the business.; ~~and~~

(3) Notifying all third parties to whom the business has sold or shared the personal information of the need to delete the consumer's personal information unless this proves impossible or involves disproportionate effort. If a business claims that notifying some or all third parties would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot notify all third parties. The business shall not simply state that notifying all third parties is impossible or would require disproportionate effort.

(c) A service provider or contractor shall, with respect to personal information that they collected pursuant to their written contract with the business and upon notification by the business, cooperate with the business in responding to a request to delete by doing all of the following:

(1) Permanently and completely erasing the personal information from its existing systems except archived or backup systems, deidentifying the personal information, aggregating the consumer information, or enabling the business to do so.

(2) To the extent that an exception applies to the deletion of personal information, deleting or enabling the business to delete the consumer's personal information that is not subject to the exception and refraining from using the consumer's personal information retained for any purpose other than the purpose provided for by that exception.

(3) Notifying any of its own service providers or contractors of the need to delete from their records in the same manner the consumer's personal information that they collected pursuant to their written contract with the service provider or contractor.

(4) Notifying any other service providers, contractors, or third parties that may have accessed personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, of the need to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.

(d) If a business, service provider, or contractor stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose.

(e) In responding to a request to delete, a business shall inform the consumer whether it has complied with the consumer's request. The business shall also inform the consumer that it will maintain a record of the request as required by section 7101, subsection (a). A business, service provider, contractor, or third party may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from its records.

(f) In cases where a business denies a consumer's request to delete in whole or in part, the business shall do all of the following:

(1) Provide to the consumer a detailed explanation of the basis for the denial, including any conflict with federal or state law, exception to the CCPA, or factual basis for contending that compliance would be impossible or involve disproportionate effort, unless prohibited from doing so by law.

(2) Delete the consumer's personal information that is not subject to the exception.

(3) Not use the consumer's personal information retained for any other purpose than provided for by that exception; and

(4) Instruct its service providers and contractors to delete the consumer's personal information that is not subject to the exception and to not use the consumer's personal information retained for any purpose other than the purpose provided for by that exception.

(g) If a business that denies a consumer's request to delete sells or shares personal information and the consumer has not already made a request to opt-out of sale/sharing, the business shall ask the consumer if they would like to opt-out of the sale or sharing of their personal information and shall include either the contents of, or a link to, the Notice of Right to Opt-out of Sale/Sharing in accordance with section 7013.

(h) In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information as long as a single option to delete all personal information is also offered. A business that provides consumers the ability to delete select categories of personal information in other contexts (e.g., purchase history, browsing history, voice recordings), however, must inform consumers of their ability to do so and direct them to how they can do so. For example, a business may provide the consumer with a link to a support page or other resource that explains consumers' data deletion options.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.130 and 1798.185, Civil Code.

§ 7023. Requests to Correct.

(a) For requests to correct, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 5, the business may deny the request to correct. The business shall inform the requestor that their identity cannot be verified.

(b) In determining the accuracy of the personal information that is the subject of a consumer's request to correct, the business shall consider the totality of the circumstances relating to the contested personal information. A business may deny a 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.

(1) Considering the totality of the circumstances includes, but is not limited to, considering:

(A) The nature of the personal information (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).

(B) How the business obtained the contested information.

(C) Documentation relating to the accuracy of the information whether provided by the consumer, the business, or another source. Requirements regarding documentation are set forth in subsection (d).

(2) If the business is not the source of the personal information and has no documentation in support of the accuracy of the information, the consumer's assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate.

(c) A business that complies with a consumer's request to correct shall correct the personal information at issue on its existing systems and ensure that the information remains corrected. The business shall also instruct all service providers and contractors that maintain the personal information at issue pursuant to their written contract with the business to make the necessary corrections in their respective systems. Service providers and contractors shall comply with the business's instructions to correct the personal information or enable the business to make the corrections and shall also ensure that the information remains corrected. If a business, service provider, or contractor stores any personal information that is the subject of the request to correct on archived or backup systems, it may delay compliance with the consumer's request to correct, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or used. Illustrative examples follow:

(1) Business L maintains personal information about consumers that it receives from data brokers on a regular basis. Business L refreshes the personal information it maintains about consumers whenever it receives an update from a data broker. Business L receives a request to correct from a consumer and determines that the information is inaccurate. To comply with the consumer's request, Business L corrects the inaccurate

information in its system and ensures that the corrected personal information is not overridden by inaccurate personal information subsequently received from a data broker.

(2) Business M stores personal information about consumers on archived or backup systems. Business M receives a request to correct from a consumer, determines that the information is inaccurate, and makes the necessary corrections within its active system. Business M may delay compliance with the consumer's request to correct with respect to data stored on the archived or backup system until the archived or backup system relating to the personal information at issue is restored to an active system or next accessed or used for a sale, disclosure, or commercial purpose.

(d) Documentation.

(1) A business shall accept, review, and consider any documentation that the consumer provides in connection with their right to correct whether provided voluntarily or as required by the business. Consumers should make a good-faith effort to provide businesses with all necessary information available at the time of the request.

(2) A business may require the consumer to provide documentation if necessary to rebut its own documentation that the personal information is accurate. In determining the necessity of the documentation requested, the business shall consider the following:

(A) The nature of the personal information at issue (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).

(B) The nature of the documentation upon which the business considers the personal information to be accurate (e.g., whether the documentation is from a trusted source, whether the documentation is verifiable, etc.)

(C) The purpose for which the business collects, maintains, or uses the personal information. For example, if the personal information is essential to the functioning of the business, the business may require more documentation.

(D) The impact on the consumer. For example, if the personal information has a negative impact on the consumer, the business may require less documentation.

(3) Any documentation provided by the consumer in connection with their request to correct shall only be used and/or maintained by the business for the purpose of correcting the consumer's personal information and to comply with the record-keeping obligations under section 7101.

(4) The business shall implement and maintain reasonable security procedures and practices in maintaining any documentation relating to the consumer's request to correct.

(e) A business may delete the contested personal information as an alternative to correcting the information if the deletion of the personal information does not negatively impact the consumer, or the consumer consents to the deletion. For example, if deleting instead of correcting inaccurate personal information would make it harder for the consumer to obtain a job, housing, credit, education, or other type of opportunity, the business shall process the request to correct or obtain the consumer's consent to delete the information.

(f) In responding to a request to correct, a business shall inform the consumer whether it has complied with the consumer's request. If the business denies a consumer's request to correct in whole or in part, the business shall do the following:

(1) Explain the basis for the denial, including any conflict with federal or state law, exception to the CCPA, inadequacy in the required documentation, or contention that compliance proves impossible or involves disproportionate effort.

(2) If a business claims that complying with the consumer's request to correct would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot comply with the request. The business shall not simply state that it is impossible or would require disproportionate effort.

(3) If a business denies a consumer's request to correct personal information collected and analyzed concerning a consumer's health, the business shall also inform the consumer that they may provide a written statement to the business to be made part of the consumer's record pursuant to Civil Code section 1798.185, subdivision (a)(7~~8~~)(D). The business shall explain to the consumer that the written statement is limited to 250 words per alleged inaccurate piece of personal information and shall include that the consumer must request that the statement be made part of the consumer's record. Upon receipt of such a statement, the business shall include it with the consumer's record. Upon the consumer's request, the business shall make the statement available to any person with whom it discloses, shares, or sells the personal information that is the subject of the request to correct.

(4) If the personal information at issue can be deleted pursuant to a request to delete, inform the consumer that they can make a request to delete the personal information and provide instructions on how the consumer can make a request to delete.

(g) A business may deny a consumer's request to correct if the business has denied the consumer's request to correct the same alleged inaccuracy within the past six months of receiving the request. However, the business must treat the request to correct as new if the consumer provides new or additional documentation to prove that the information at issue is inaccurate.

(h) A business may deny a request to correct if it has a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. The business shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent or abusive.

(i) Where the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer's request, the business ~~may~~ must provide the consumer with the name of the source from which the business received the alleged inaccurate information, or in the alternative, inform the source that the information provided is incorrect and must be corrected.

(j) Upon request, a business shall disclose specific pieces of personal information that the business maintains and has collected about the consumer to allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer's request to correct. This disclosure shall not be considered a response to a request to know that is counted towards the limitation of two requests within a 12-month period as set forth in Civil Code section 1798.130, subdivision (b). With regard to a correction to a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics, a business shall not disclose this information, but ~~may~~ must provide a way to confirm that the personal information it maintains is the same as what the verified consumer has provided. For example, the business can have the consumer use its toll-free phone number and provide the information that they seek to confirm. After verifying the consumer, the business can confirm whether the information provided by the consumer matches what they have in their system.

(k) Whether a business, service provider, or contractor has implemented measures to ensure that personal information that is the subject of a request to correct remains corrected factors into whether that business, service provider, or contractor has complied with a consumer's request to correct in accordance with the CCPA and these regulations. For example, if a business, service provider, or contractor ~~may~~ supplements personal information it maintains about consumers with information obtained from a data broker, f~~. F~~ailing to consider and address the possibility that corrected information may be overridden by inaccurate information subsequently received from a data broker ~~may~~ factors into whether that business, service provider, or contractor has adequately complied with a consumer's request to correct.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.81.5, 1798.106, 1798.130 and 1798.185, Civil Code.

§ 7024. Requests to Know.

(a) For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the

request pursuant to the regulations set forth in Article 5, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (b).

(b) For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 5, the business may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall provide or direct the consumer to its information practices set forth in its privacy policy.

(c) In responding to a request to know, a business is not required to search for personal information if all of the following conditions are met:

(1) The business does not maintain the personal information in a searchable or reasonably accessible format.

(2) The business maintains the personal information solely for legal or compliance purposes.

(3) The business does not sell the personal information and does not use it for any commercial purpose.

(4) The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.

(d) A business shall not disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. However, the ~~The~~ business shall:~~, however,~~

(1) ~~i~~Inform the consumer with sufficient particularity that it has collected the type of information. For example, a business shall respond that it collects "unique biometric data including a fingerprint scan" without disclosing the actual fingerprint scan data~~.~~; and

(2) Provide a way for the consumer to confirm that the personal information the business maintains is the same as what the verified consumer provides. For example, the business can have the consumer use its toll-free phone number and provide the information that they seek to confirm. After verifying the consumer, the business can confirm whether the information provided by the consumer matches what they have in their system.

(e) If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, ~~because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business shall disclose the other information sought by the consumer.~~ the business shall do all of the following:

(1) Provide to the consumer a detailed explanation of the basis for the denial, including any conflict with federal or state law or exception to the CCPA, unless prohibited from doing so by law; and

(2) Disclose the consumer's personal information that is not subject to the exception.

(f) A business shall use reasonable security measures when transmitting personal information to the consumer.

(g) If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 5.

(h) In response to a request to know, a business shall provide all the personal information it has collected and maintains about the consumer during the 12-month period preceding the business's receipt of the consumer's request. A consumer may request that the business provide personal information that the business collected beyond the 12-month period, as long as it was collected on or after January 1, 2022, and the business shall be required to provide that information unless doing so proves impossible or would involve disproportionate effort. That information shall include any personal information that the business's service providers or contractors collected pursuant to their written contract with the business. If a business claims that providing personal information beyond the 12-month period preceding the business's receipt of the consumer's request would be impossible or would involve disproportionate effort, the business shall not be required to provide it as long as the business provides the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot provide personal information beyond the 12-month period. The business shall not simply state that it is impossible or would require disproportionate effort.

(i) A service provider or contractor shall provide assistance to the business in responding to a verifiable consumer request to know, including by providing the business the consumer's personal information it has in its possession that it collected pursuant to their written contract with the business, or by enabling the business to access that personal information.

(j) In responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response to the consumer as required by the CCPA. It shall not refer the consumer to the businesses' information practices outlined in its privacy policy unless its response would be the same for all consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories.

(k) In responding to a verified request to know categories of personal information, the business shall provide all of the following:

(1) The categories of personal information the business has collected about the consumer.

(2) The categories of sources from which the personal information was collected.

(3) The business or commercial purpose for which it collected, ~~or~~ sold, or shared the personal information.

(4) The categories of third parties with whom the business ~~shares~~ discloses personal information.

(5) The categories of personal information that the business sold or shared about the consumer, and for each category identified, the categories of third parties to whom it sold or shared that particular category of personal information.

(6) The categories of personal information that the business disclosed for a business purpose, and for each category identified, the categories of service providers or contractors ~~third parties~~ to whom it disclosed that particular category of personal information.

(*l*) A business shall identify the categories of personal information, categories of sources of personal information, ~~and~~ categories of third parties to whom a business sold or shared ~~disclosed~~ personal information, and categories of service providers or contractors to whom a business disclosed personal information, in a manner that provides consumers a meaningful understanding of the categories listed.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.81.5, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.

§ 7025. Opt-out Preference Signals.

(a) The purpose of an opt-out preference signal is to provide consumers with a simple and easy-to-use method by which consumers interacting with businesses online can automatically exercise their right to opt-out of sale/sharing. Through an opt-out preference signal, a consumer can opt-out of sale and sharing of their personal information with all businesses they interact with online without having to make individualized requests with each business.

(b) A business that sells or shares personal information shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:

(1) The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field or JavaScript object.

(2) The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information. The configuration or disclosure does not need to be tailored only to California or to refer to California.

(c) When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b):

(1) The business shall treat the opt-out preference signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device and any consumer profile associated with that browser or device, including pseudonymous profiles. If known, the business shall also treat the opt-out preference signal as a valid request to opt-out of sale/sharing for the consumer. This is not required for a business that does not sell or share personal information.

(2) The business shall not require a consumer to provide additional information beyond what is necessary to send the signal. However, a business may provide the consumer with an option to provide additional information if it will help facilitate the consumer's request to opt-out of sale/sharing. Any information provided by the consumer shall not be used, disclosed, or retained for any purpose other than processing the request to opt-out of sale/sharing. For example, a business may give the consumer the option to provide information that identifies the consumer so that the request to opt-out of sale/sharing can apply to offline sale or sharing of personal information. However, if the consumer does not respond, the business shall still process the opt-out preference signal as a valid

request to opt-out of sale/sharing for that browser or device and any consumer profile the business associates with that browser or device, including pseudonymous profiles.

(3) If the opt-out preference signal conflicts with a consumer's business-specific privacy setting that allows the business to sell or share their personal information, the business shall process the opt-out preference signal as a valid request to opt-out of sale/sharing, but may notify the consumer of the conflict and provide the consumer with an opportunity to consent to the sale or sharing of their personal information. The business shall comply with section 7004 in obtaining the consumer's consent to the sale or sharing of their personal information. If the consumer 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, but the business must display the status of the consumer's choice in accordance with section 7025, subsection (c)(6), and section 7026, subsection (g).

(4) If the opt-out preference signal conflicts with the consumer's participation in a business's financial incentive program that requires the consumer to consent to the sale or sharing of personal information, the business may notify the consumer that processing the opt-out preference signal as a valid request to opt-out of sale/sharing would withdraw the consumer from the financial incentive program and ask the consumer to affirm that they intend to withdraw from the financial incentive program. If the consumer affirms that they intend to withdraw from the financial incentive program, the business shall process the consumer's request to opt-out of sale/sharing. If the business asks and the consumer does not affirm their intent to withdraw, the business may ignore the opt-out preference signal with respect to that consumer's participation in the financial incentive program for as long as the consumer is known to the business. If the business does not ask the consumer to affirm their intent with regard to the financial incentive program, the business shall still process the opt-out preference signal as a valid request to opt-out of sale/sharing for that browser or device and any consumer profile the business associates with that browser or device. In either situation, the

business must display the status of the consumer's choice in accordance with section 7025, subsection (c)(6), and section 7026, subsection (g).

(5) Where the consumer is known to the business, the business shall not interpret the absence of an opt-out preference signal after the consumer previously sent an opt-out preference signal as consent to opt-in to the sale or sharing of personal information.

(6) A business ~~may~~ must display whether it has processed the consumer's opt-out preference signal as a valid request to opt-out of sale/sharing on its website. For example, the business may display on its website "Opt-Out Request ~~Preference Signal~~ Honored" when a browser, device, or consumer using an opt-out preference signal visits the website, ~~or~~ and display through a toggle or radio button that the consumer has opted out of the sale/sharing of their personal information in accordance with section 7026, subsection (g).

(7) Illustrative examples follow.

(A) Caleb visits Business N's website using a browser with an opt-out preference signal enabled, but he is not otherwise logged into his account and the business cannot otherwise associate Caleb's browser with a consumer profile the business maintains. Business N collects and shares Caleb's personal information tied to his browser identifier for cross-context behavioral advertising. Upon receiving the opt-out preference signal, Business N shall stop selling and sharing Caleb's information linked to Caleb's browser identifier for cross-context behavioral advertising, but it would not be able to apply the request to opt-out of the sale/sharing to Caleb's account information because the connection between Caleb's browser and Caleb's account is not known to the business.

(B) Noelle has an account with Business O, an online retailer who manages consumer's privacy choices through a settings menu. Noelle's privacy settings default to allowing Business O to sell and share her personal information with the business's marketing partners. Noelle enables an opt-out preference signal on her browser and then visits Business O's website. Business O recognizes that

Noelle is visiting its website because she is logged into her account. Upon receiving Noelle's opt-out preference signal, Business O shall treat the signal as a valid request to opt-out of sale/sharing and shall apply it to her device and/or browser and also to her account and any offline sale or sharing of personal information. Business O may inform Noelle that her opt-out preference signal differs from her current privacy settings and provide her with an opportunity to consent to the sale or sharing of her personal information, but it must process the request to opt-out of sale/sharing unless Noelle instructs otherwise. Business O must also wait at least 12 months before asking Noelle to opt-in to the sale or sharing of her personal information in accordance with section 7026, subsection (k). In addition, Business O's notification would not allow it to fall within the exception set forth in Civil Code section 1798.135, subdivision (b)(1), because it would not be complying with the requirements set forth in subsection (f).

(C) Angela also has an account with Business O and has enabled an opt-out preference signal on her browser while logged into her account. Business O applies the opt-out preference signal as a valid request to opt-out of sale/sharing not only to Angela's current browser, but also to Angela's account because she is known to the business while making the request. Angela later logs into her account with Business O using a different device that does not have the opt-out preference signal enabled. Business O shall not interpret the absence of the opt-out preference signal as consent to opt-in to the sale of personal information.

(D) Ramona participates in Business P's financial incentive program where she receives coupons in exchange for allowing the business to pseudonymously track and share her online browsing habits with marketing partners. Ramona enables an opt-out preference signal on her browser and then visits Business P's website. Business P knows that it is Ramona through a cookie that has been placed on her browser, but also detects the opt-out preference signal. Business P may ignore the opt-out preference signal and notify Ramona that her opt-out preference signal conflicts with her participation in the

financial incentive program and ask whether she intends to withdraw from the financial incentive program. If Ramona does not affirm her intent to withdraw, Business P may ignore the opt-out preference signal and place Ramona on a whitelist so that Business P does not have to notify Ramona of the conflict again.

(E) Ramona clears her cookies and revisits Business P's website with the opt-out preference signal enabled. Business P no longer knows that it is Ramona visiting its website. Business P shall honor Ramona's opt-out preference signal as it pertains to her browser or device and any consumer profile the business associates with that browser or device.

(d) The business and the platform, technology, or mechanism that sends the opt-out preference signal shall not use, disclose, or retain any personal information collected from the consumer in connection with the sending or processing the request to opt-out of sale/sharing for any purpose other than sending or processing the opt-out preference signal.

(e) Civil Code section 1798.135, subdivisions (b)(1) and (3), provide a business the choice between (1) processing opt-out preference signals and providing the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links or the Alternative Opt-out Link; or (2) processing opt-out preference signals in a frictionless manner in accordance with these regulations and not having to provide the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links or the Alternative Opt-out Link. They do not give the business the choice between posting the above-referenced links or honoring opt-out preference signals. Even if the business posts the above-referenced links, the business must still process opt-out preference signals, though it may do so in a non-frictionless manner. If a business processes opt-out preference signals in a frictionless manner in accordance with subsections (f) and (g), then it may, but is not required to, provide the above-referenced links.

(f) Except as allowed by these regulations, processing an opt-out preference signal in a frictionless manner as required by Civil Code section 1798.135, subdivision (b)(1), means that the business shall not:

(1) Charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal.

(2) Change the consumer's experience with the product or service offered by the business. For example, the consumer who uses an opt-out preference signal shall have the same experience with regard to how the business's product or service functions compared to a consumer who does not use an opt-out preference signal.

(3) Display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal. However, a business's display of whether the consumer visiting their website has opted out of the sale or sharing their personal information shall not be considered a violation of this regulation. The business may also provide a link to a privacy settings page, menu, or similar interface that enables the consumer to consent to the business ignoring the opt-out preference signal with respect to the business's sale or sharing of the consumer's personal information provided that it complies with subsections (f)(1) ~~through~~ – (3).

(g) A business meeting the requirements of Civil Code section 1798.135, subdivision (b)(1) is not required to post the "Do Not Sell or Share My Personal Information" link or the Alternative Opt-out Link if it meets all of the following additional requirements:

(1) Processes the opt-out preference signal in a frictionless manner in accordance with the CCPA and these regulations.

(2) Includes in its privacy policy the following information:

(A) A description of the consumer's right to opt-out of the sale or sharing of their personal information by the business;

(B) A statement that the business processes opt-out preference signals in a frictionless manner;

(C) Information on how consumers can implement opt-out preference signals for the business to process in frictionless manner; and

(D) Instructions for any other method by which the consumer may submit a request to opt-out of sale/sharing.

(3) Allows the opt-out preference signal to fully effectuate the consumer's request to opt-out of sale/sharing. For example, if the business sells or shares personal information offline and needs to request from the consumer additional information that is not provided by the opt-out preference signal in order to apply the request to opt-out of sale/sharing to offline sales and sharing of personal information, then the business has not fully effectuated the consumer's request to opt-out of sale/sharing. Illustrative examples follow.

(A) Business Q collects consumers' online browsing history and shares it with third parties for cross-context behavioral advertising purposes. Business Q also sells consumers' personal information offline to marketing partners. Business Q cannot fall within the exception set forth in Civil Code section 1798.135, subdivision (b)(1), because a consumer's opt-out preference signal would only apply to Business Q's online sharing of personal information about the consumer's browser or device; the consumer's opt-out preference signal would not apply to Business Q's offline selling of the consumer's information because Business Q could not apply it to the offline selling without additional information provided by the consumer, i.e., the logging into an account.

(B) Business R only sells and shares personal information online for cross-context behavioral advertising purposes. Business R may use the exception set forth in Civil Code section 1798.135, subdivision (b)(1), and not post the "Do Not Sell or Share My Personal Information" link because a consumer using an opt-out preference signal would fully effectuate their right to opt-out of the sale or sharing of their personal information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140 and 1798.185, Civil Code.

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

(a) A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the personal information that it makes available to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow.

(1) A business that collects personal information from consumers online shall, at a minimum, allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and at least one of the following methods: an interactive form accessible via the "Do Not Sell or Share My Personal Information" link, the Alternative Opt-out Link, or the business's privacy policy if the business processes an opt-out preference signal in a frictionless manner.

(2) A business that interacts with consumers in person and online may provide an in-person method for submitting requests to opt-out of sale/sharing in addition to the opt-out preference signal.

(3) Other methods for submitting requests to opt-out of the sale/sharing include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, and a form submitted through the mail.

(4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to opt-out of sale/sharing because cookies concern the collection of personal information and not the sale or sharing of personal information. An acceptable method for submitting requests to opt-out of sale/sharing must address the sale and sharing of personal information.

(b) A business's methods for submitting requests to opt-out of sale/sharing shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004.

(c) A business shall not require a consumer submitting a request to opt-out of sale/sharing to create an account or provide additional information beyond what is necessary to direct the business not to sell or share the consumer's personal information.

(d) A business shall not require a verifiable consumer request for a request to opt-out of sale/sharing. A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information shall cease to be sold or shared by the business. However, to the extent that the business can comply with a request to opt-out of sale/sharing without additional information, it shall do so.

(e) If a business has a good-faith, reasonable, and documented belief that a request to opt-out of sale/sharing is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide to the requestor an explanation why it believes the request is fraudulent.

(f) A business shall comply with a request to opt-out of sale/sharing by:

(1) Ceasing to sell to and/or share with third parties the consumer's personal information as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. Service providers or contractors collecting personal information pursuant to the written contract with the business required by the CCPA and these regulations does not constitute a sale or sharing of personal information.

(2) Notifying all third parties to whom the business has sold or shared the consumer's personal information, after the consumer submits the request to opt-out of sale/sharing and before the business complies with that request, that the consumer has made a request to opt-out of sale/sharing and directing them to comply with the consumer's request and forward the request to any other person to whom the third party has made the personal information available during that time period.

(3) Illustrative examples follow.

(A) Business U uses programmatic advertising technology on its website that instantaneously sells and shares personal information of

consumers viewing its website through real-time bidding. Business U can restrict the transfer of personal information instantaneously, and thus, stop the sale and sharing personal information immediately. Accordingly, when Maya visits Business U's website and submits a request to opt-out of sale/sharing through the "Do Not Sell or Share My Personal Information" link, Business U shall immediately comply with Maya's request by ceasing to sell or share Maya's personal information with any third parties. Business U shall not take 15 business days to comply with Maya's request because it is feasibly possible to comply with the request sooner.

(B) Business V is a marketing company that discloses consumers' personal information to its clients via a batched upload every Friday. Business V's disclosure of personal information is a sale because it receives valuable consideration in exchange for the information. Siobhan submits a request to opt-out of sale/sharing to Business V through the mail, which Business V receives on Thursday. Business V finishes processing Siobhan's request on Tuesday because it requires a few days to update all internal systems and databases with Siobhan's request. Accordingly, Siobhan's personal information was not removed from the disclosure that occurred on the first Friday after receiving her request, though it was removed from the disclosure that occurred on the second Friday. Business V must notify all its clients that received Siobhan's information on the first Friday after Siobhan made her request to opt-out of sale/sharing and direct them to comply with her request and forward the request to any other person to whom they made Siobhan's personal information available.

(g) A business ~~may~~ must provide a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business. For example, the business may display on its website "Opt-Out Request Honored ~~Consumer Opted Out of Sale/Sharing~~" in accordance with section 7025, subsection (b)(6), and ~~or~~ display in the consumer's privacy settings through a toggle or radio button that the consumer has opted out of the sale/sharing of their personal information.

(h) In responding to a request to opt-out of sale/sharing, a business may present the consumer with the choice 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 also offered. However, doing so in response to an opt-out preference signal will prevent the business from using the exception set forth in Civil Code section 1798.135, subdivision (b)(1).

(i) A business that responds to a request to opt-out of sale/sharing by informing the consumer of a charge for the use of any product or service shall comply with Article 7 and shall provide the consumer with a Notice of Financial Incentive that complies with section 7016 in its response. However, doing so in response to an opt-out preference signal will prevent the business from using the exception set forth in Civil Code section 1798.135, subdivision (b)(1).

(j) A consumer may use an authorized agent to submit a request to opt-out of sale/sharing on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. The requirement to obtain and provide written permission from the consumer does not apply to requests made by an opt-out preference signal.

(k) Except as allowed by these regulations, a business shall wait at least 12 months from the date of the consumer's request before asking a consumer who has opted out of the sale or sharing of their personal information to consent to the sale or sharing of their personal information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140 and 1798.185, Civil Code.

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

(a) The unauthorized use or disclosure of sensitive personal information creates a heightened risk of harm for the consumer. The purpose of the request to limit is to give consumers meaningful control over how their sensitive personal information is collected, used, and disclosed. It gives the consumer the ability to limit the business's use of sensitive personal information to that which is necessary to perform the services or provide the goods reasonably expected

by an average consumer who requests those goods or services, with some narrowly tailored exceptions, which are set forth in subsection (m). Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to requests to limit.

(b) A business that uses or discloses sensitive personal information for purposes other than those set forth in subsection (m) shall provide two or more designated methods for submitting requests to limit. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the sensitive personal information that it uses for purposes other than those set forth in subsection (m), available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to limit. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow.

(1) A business that collects sensitive personal information from consumers online shall, at a minimum, allow consumers to submit requests to limit through an interactive form accessible via the "Limit the Use of My Sensitive Personal Information" link or the Alternative Opt-out Link.

(2) A business that interacts with consumers in person and online may provide an in-person method for submitting requests to limit in addition to the online form.

(3) Other methods for submitting requests to limit include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, and a form submitted through the mail.

(4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to limit because cookies concern the collection of personal information and not necessarily the use and disclosure of sensitive personal information. An acceptable method for submitting requests to limit must address the specific right to limit.

(c) A business's methods for submitting requests to limit shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004.

(d) A business shall not require a consumer submitting a request to limit 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.

(e) A business shall not require a verifiable consumer request for a request to limit. A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer to whom the request ~~should be~~ applies~~d~~. However, to the extent that the business can comply with a request to limit without additional information, it shall do so.

(f) If a business has a good-faith, reasonable, and documented belief that a request to limit is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide to the requestor an explanation why it believes the request is fraudulent.

(g) A business shall comply with a request to limit by:

(1) Ceasing to use and disclose the consumer's sensitive personal information for purposes other than those set forth in subsection (m) as soon as feasibly possible, but no later than 15 business days from the date the business receives the request.

(2) Notifying all the business's service providers or contractors that use or disclose the consumer's sensitive personal information for purposes other than those set forth in subsection (m) that the consumer has made a request to limit and instructing them to comply with the consumer's request to limit within the same time frame.

(3) Notifying all third parties to whom the business has disclosed or made available the consumer's sensitive personal information for purposes other than those set forth in subsection (m), after the consumer submitted their request and before the business complies with that request, that the consumer has made a request to limit and direct them 1) to comply with the consumer's request and 2) to forward the request to any other person with whom the third party has disclosed or made available ~~shared~~ the sensitive personal information during that time period.

(h) A business ~~may~~ must provide a means by which the consumer can confirm that their request to limit has been processed by the business. For example, the business may display through a toggle or radio button that the consumer has limited the business's use and disclosure of their sensitive personal information.

(i) In responding to a request to limit, a business may present the consumer with the choice to allow specific uses for the sensitive personal information as long as a single option to limit the use of the personal information is also offered.

(j) A consumer may use an authorized agent to submit a request to limit on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf.

(k) A business that responds to a request to limit by informing the consumer of a charge for the use of any product or service shall comply with Article 7 and shall provide the consumer with a Notice of Financial Incentive that complies with section 7016 in its response.

(*l*) Except as allowed by these regulations, a business shall wait at least 12 months from the date the consumer's request to limit is received before asking a consumer who has exercised their right to limit to consent to the use or disclosure of their sensitive personal information for purposes other than those set forth in subsection (m).

(m) The purposes identified in Civil Code section 1798.121, subdivision (a), for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit are as follows. A business that only uses or discloses sensitive personal information for these purposes, provided that the use or disclosure is reasonably necessary and proportionate for those purposes, is not required to post a Notice of Right to Limit or provide a method for submitting a request to limit.

(1) To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services. For example, a consumer's precise geolocation may be used by a mobile application that

is providing the consumer with directions on how to get to a specific location. A consumer's precise geolocation may not, however, be used by a gaming application where the average consumer would not expect the application to need this piece of sensitive personal information.

(2) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information. Illustrative examples follow.

(A) ~~For example, a~~ A business may disclose a consumer's log-in information to a data security company that it has hired to investigate and remediate a data breach that involved that consumer's account.

(B) A business may scan employees' outgoing emails to prevent employees from leaking sensitive personal information outside of the business. However, scanning the emails for other purposes would not fall within this exception to the consumer's right to limit.

(3) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business or at consumers, or ~~and~~ to prosecute those responsible for those actions. Illustrative examples follow.

(A) ~~For example, a~~ A business may use information about a consumer's ethnicity and/or the contents of email and text messages to investigate claims of racial discrimination or hate speech.

(B) A business may collect and use the biometric information of its employees to authenticate them for access into secured areas of their business and to prevent access by unauthorized persons. However, the business would not be able to retain the biometric information indefinitely or use it for unrelated purposes, such as the development of commercial products, under this exception to the consumer's right to limit.

(4) To ensure the physical safety of natural persons. For example, a business may disclose a consumer's geolocation information to law enforcement to investigate an alleged kidnapping.

(5) For short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business. For example, a business that sells religious books can use information about its customers' interest in its religious content to serve contextual advertising for other kinds of religious merchandise within its store or on its website, so long as the business does not use sensitive personal information to create a profile about an individual consumer or disclose personal information that reveals consumers' religious beliefs to third parties.

(6) To perform services on behalf of the business. For example, a business may use information for maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.

(7) To verify or maintain the quality or safety of a product, service, or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the business. For example, a car rental business may use a consumer's driver's license for the purpose of testing that its internal text recognition software accurately captures license information used in car rental transactions.

(8) To collect or process sensitive personal information where the collection or processing is not for the purpose of inferring characteristics about a consumer. For example, a business that includes a search box on their website by which consumers can search for articles related to their health condition may use the information provided by the consumer for the purpose of providing the search feature without inferring characteristics about the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.121, 1798.135, 1798.140 and 1798.185, Civil Code.

§ 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.

(a) Requests to opt-in to sale or sharing of personal information and requests to opt-in to the use and disclosure of sensitive personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

(b) If a consumer who has opted-out of the sale or sharing of their personal information initiates a transaction or attempts to use a product or service that requires the sale or sharing of their personal information, the business may inform the consumer that the transaction, product, or service requires the sale or sharing of their personal information and provide instructions on how the consumer can provide consent to opt-in to the sale or sharing of their personal information. The business shall comply with section 7004 when obtaining the consumer's consent.

(c) If a consumer who has exercised their right to limit initiates a transaction or attempts to use a product or service that requires the use or disclosure of sensitive personal information for purposes other than those set forth in section 7027, subsection (m), the business may inform the consumer that the transaction, product, or service requires the use or disclosure of sensitive personal information for additional purposes and provide instructions on how the consumer can provide consent for the business to use or disclose sensitive personal information for those additional purposes. The business shall comply with section 7004 when obtaining the consumer's consent.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.121, 1798.135 and 1798.185, Civil Code.

ARTICLE 4. SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES

§ 7050. Service Providers and Contractors.

(a) A service provider or contractor shall not retain, use, or disclose personal information collected pursuant to its written contract with the business except: for the following purposes, provided that the retention, use, or disclosure is reasonably necessary and proportionate for those purposes.

(1) For the specific business purpose(s) set forth in the written contract between the business and the service provider or contractor that is required by the CCPA and these regulations.

(2) To retain and employ another service provider or contractor as a subcontractor, where the subcontractor meets the requirements for a service provider or contractor under the CCPA and these regulations.

(3) For internal use by the service provider or contractor to build or improve the quality of the services it is providing to the business, even if this business purpose is not specified in the written contract required by the CCPA and these regulations, provided that the service provider or contractor does not use the personal information to perform services on behalf of another person. Illustrative examples follow.

(A) An email marketing service provider can send emails on a business's behalf using the business's customer email list. The service provider could analyze those customers' interactions with the marketing emails to improve its services and offer those improved services to everyone. But the service provider cannot use the original email list to send marketing emails on behalf of another business.

(B) A shipping service provider that delivers businesses' products to their customers may use the addresses received from their business clients and their experience delivering to those addresses to identify faulty or incomplete addresses, and thus, improve their delivery services. However, the shipping service provider cannot compile the addresses received from one business to send advertisements on behalf of another business, or compile addresses received from businesses to sell to data brokers.

(4) To prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent or illegal activity, even if this business purpose is not specified in the written contract required by the CCPA and these regulations. For example, a service provider or contractor may use IP addresses that have been associated with malicious activity (e.g., distributed denial of service attacks) to detect and prevent such malicious activity.

(5) For the purposes enumerated in Civil Code section 1798.145, subdivisions (a)(1) ~~through (a)(7)~~.

(b) A service provider or contractor cannot contract with a business to provide cross-context behavioral advertising. Pursuant to Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but the service provider or contractor shall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or collects from its own interaction with consumers. A person who contracts with a business to provide cross-context behavioral advertising is a third party and not a service provider or contractor with respect to cross-context behavioral advertising services. Illustrative examples follow.

(1) Business S, a clothing company, hires a social media company as a service provider for the purpose of providing Business S's advertisements on the social media company's platform. The social media company can serve Business S by providing non-personalized advertising services on its platform based on aggregated or demographic information (e.g., advertisements to women, 18-30 years old, that live in Los Angeles). However, it cannot use a list of customer email addresses provided by Business S to identify users on the social media company's platform to serve advertisements to them.

(2) Business T, a company that sells cookware, hires an advertising company as a service provider for the purpose of advertising its services. The advertising agency can serve Business T by providing contextual advertising services, such as placing advertisements for Business T's products on websites that post recipes and other cooking tips.

(c) If a service provider or contractor receives a request made pursuant to the CCPA directly from the consumer, the service provider or contractor shall either act on behalf of the business in accordance with the business's instructions for responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider or contractor.

(d) A service provider or contractor that is a business 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.

(e) A person who does not have a contract that complies with section 7051, subsection (a), is not a service provider or a contractor under the CCPA. For example, a business's disclosure of personal information to a person who does not have a contract that complies with section 7051, subsection (a), may be considered a sale or sharing of personal information for which the business must provide the consumer with the right to opt-out of sale/sharing.

(f) A service provider or a contractor shall comply with the terms of the contract required by the CCPA and these regulations.

(g) Whether an entity that provides services to a nonbusiness must comply with a consumer's CCPA request depends upon whether the entity is a "business," as defined by Civil Code section 1798.140, subdivision (d).

(h) A service provider or contractor shall, with respect to personal information that they collected pursuant to their written contract with the business, cooperate with the business:

(1) In the business's completion of its cybersecurity audit pursuant to Article 9, including making available to the business's auditor all relevant information that the auditor requests to complete the business's cybersecurity audit and that is in the service provider's or contractor's possession, custody, or control, and not misrepresenting any fact that the auditor deems relevant to the business's cybersecurity audit; and

(2) In conducting the business's risk assessment pursuant to Article 10, including making available to the business all facts necessary to conduct the risk assessment that are in the service provider's or contractor's possession, custody, or control, and not misrepresenting any fact necessary to conduct the risk assessment.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

§ 7051. Contract Requirements for Service Providers and Contractors.

(a) The contract required by the CCPA for service providers and contractors shall:

(1) Prohibit the service provider or contractor from selling or sharing personal information it collects pursuant to the written contract with the business.

(2) Identify the specific business purpose(s) for which the service provider or contractor is processing personal information pursuant to the written contract with the business, and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified business purpose(s) set forth within the contract. The business purpose(s) shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.

(3) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it collected pursuant to the written contract with the business for any purpose other than the business purpose(s) specified in the contract or as otherwise permitted by the CCPA and these regulations.

(4) ~~Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it collected pursuant to the written contract with the business for any commercial purpose other than the business purpose(s) specified in the contract, unless expressly permitted by the CCPA or these regulations.~~

~~(5)~~ Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it collected pursuant to the written contract with the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information that it collected pursuant to the written contract with the business with personal information that it received from another source or collected from its own interaction with the consumer, unless expressly permitted by the CCPA or these regulations.

(5) ~~(6)~~ Require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including — with respect to the personal information that it collected pursuant to the written contract with the business — providing the same level of privacy protection as required of businesses by the CCPA and these regulations. For example, the contract may require the service provider or contractor to cooperate with the business in responding to and complying with consumers' requests made pursuant to the CCPA, to assist the business in completing the business's cybersecurity audit pursuant to Article 9, to assist the business in conducting the business's risk assessment pursuant to Article 10, to assist the business in complying with the business's ADMT requirements pursuant to Article 11, and to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.

(6) ~~(7)~~ Grant the business the right to take reasonable and appropriate steps to ensure that the service provider or contractor uses the personal information that it collected pursuant to the written contract with the business in a manner consistent with the business's obligations under the CCPA and these regulations. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months.

(7) ~~(8)~~ Require the service provider or contractor to notify the business after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

(8) ~~(9)~~ Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider or contractor's unauthorized use of personal information. For example, the business may require the service provider or contractor to provide documentation that verifies that they no longer retain or use the personal information of consumers that have made a valid request to delete with the business.

(9) ~~(10)~~ Require the service provider or contractor to enable the business to comply with consumer requests made pursuant to the CCPA or require the business to inform the service provider or contractor of any consumer request made pursuant to the CCPA that they must comply with and provide the information necessary for the service provider or contractor to comply with the request.

(b) A service provider or contractor that subcontracts with another person in providing services to the business for whom it is a service provider or contractor shall have a contract with the subcontractor that complies with the CCPA and these regulations, including subsection (a).

(c) Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. For example, ~~depending on the circumstances,~~ 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 might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

§ 7053. Contract Requirements for Third Parties.

(a) A business that sells or shares a consumer's personal information with a third party shall enter into an agreement with the third party that:

(1) Identifies the limited and specified purpose(s) for which the personal information is made available to the third party. The purpose(s) shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.

(2) Specifies that the business is making the personal information available to the third party only for the limited and specified purpose(s) set forth

within the contract and requires the third party to use it only for that limited and specified purpose(s).

(3) Requires the third party to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that the business makes available to the third party—providing the same level of privacy protection as required of businesses by the CCPA and these regulations. For example, the contract may require the third party to comply with a consumer's request to opt-out of sale/sharing forwarded to it by a first-party business and to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.

(4) Grants the business the right—with respect to the personal information that the business makes available to the third party—to take reasonable and appropriate steps to ensure that the third party uses it in a manner consistent with the business's obligations under the CCPA and these regulations. For example, the business may require the third party to attest that it treats the personal information the business made available to it in the same manner that the business is obligated to treat it under the CCPA and these regulations.

(5) Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information made available to the third party. For example, the business may require the third party to provide documentation that verifies that it no longer retains or uses the personal information of consumers who have had their requests to opt-out of sale/sharing forwarded to it by the first party business.

(6) Requires the third party to notify the business after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

(b) Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using

personal information in violation of the CCPA and these regulations. For example, ~~depending on the circumstances,~~ a business that never enforces the terms of the contract might not be able to rely on the defense that it did not have reason to believe that the third party intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the third party.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

ARTICLE 5. VERIFICATION OF REQUESTS

§ 7060. General Rules Regarding Verification.

(a) A business shall establish, document, and comply with a reasonable method for verifying that the person making a request to delete, request to correct, ~~or~~ request to know, or request to access ADMT is the consumer about whom the business has collected information.

(b) A business shall not require a consumer to verify their identity to make a request to opt-out of sale/sharing, ~~or~~ to make a request to limit, or to make a request to opt-out of ADMT. A business may ask the consumer for information necessary to complete the request; however, it shall not be burdensome on the consumer. For example, a business may ask the consumer for their name, but it shall not require the consumer to take a picture of themselves with their driver's license.

(c) In determining the method by which the business will verify the consumer's identity, the business shall:

(1) ~~Whenever feasible, m~~Match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business before requesting additional information, or use a third-party identity verification service that complies with this section.

(2) Avoid collecting the types of personal information identified in Civil Code section 1798.81.5, subdivision (d), unless necessary for the purpose of verifying the consumer.

(3) Consider the following factors:

(A) The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive personal information shall warrant a more stringent verification process.

(B) The risk of harm to the consumer posed by any unauthorized deletion, correction, or access. A greater risk of harm to the consumer by unauthorized deletion, correction, or access shall warrant a more stringent verification process.

(C) The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be.

(D) Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated.

(E) The manner in which the business interacts with the consumer.

(F) Available technology for verification.

(d) A business shall ~~generally~~ avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, security, or fraud-prevention. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 7101.

(e) A business shall not require the consumer or the consumer's authorized agent to pay a fee for the verification of their request to delete, request to correct, or request to know. For example, a business ~~may~~ must not require a consumer to provide a notarized affidavit to verify their identity unless the business pays for or compensates the consumer for the cost of notarization. A business that compensates the consumer for the cost of the notarization shall provide the

consumer with instructions on how they will be reimbursed prior to the consumer's submission of the notarized affidavit.

(f) A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized deletion, correction, or access ~~of~~ to a consumer's personal information, or access to information about a business's use of ADMT with respect to a consumer.

(g) If a business maintains consumer information that is deidentified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request.

(h) For requests to correct, the business must ~~shall make an effort to~~ verify the consumer based on personal information that is not the subject of the request to correct. For example, if the consumer is contending that the business has the wrong address for the consumer, the business shall not use address as a means of verifying the consumer's identity.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

§ 7062. Verification for Non-Accountholders.

(a) If a consumer does not have or cannot access a password-protected account with a business, the business shall comply with this section, in addition to section 7060.

(b) A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business that it has determined to be reliable for the purpose of verifying the consumer.

(c) A business's compliance with a request to know specific pieces of personal information, or a request to access ADMT, requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal

information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. If a business uses this method for verification, the business shall maintain all signed declarations as part of its record-keeping obligations.

(d) A business's compliance with a request to delete or a request to correct may require that the business verify the identity of the consumer to a reasonable or reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion or correction. For example, the deletion of family photographs or the correction of contact information may require a reasonably high degree of certainty, while the deletion of browsing history or correction of marital status may require only a reasonable degree of certainty. A business shall act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with these regulations.

(e) Illustrative examples follow:

(1) *Example 1:* If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if a retailer maintains a record of purchases made by a consumer, the business may require the consumer to identify items that they recently purchased from the store or the dollar amount of their most recent purchase to verify their identity to a reasonable degree of certainty.

(2) *Example 2:* If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the personal information. For example, a business may have a mobile application that collects personal information about the consumer but does not require an account. The business may determine whether, based on the facts and considering the factors set forth in section 7060, subsection ~~(b)~~(c)(3), it may reasonably verify a consumer by asking them to provide information that only the person who

used the mobile application may know or by requiring the consumer to respond to a notification sent to their device.

(f) A business shall deny a request to know specific pieces of personal information, or a request to access ADMT, if it cannot verify the identity of the requestor pursuant to these regulations.

(g) If there is no reasonable method by which a business can verify the identity of the consumer to the degree of certainty required by this section, the business shall state so in response to any request and explain why it has no reasonable method by which it can verify the identity of the requestor. If the business has no reasonable method by which it can verify any consumer, the business shall explain why it has no reasonable verification method in its privacy policy. The business shall evaluate and document whether a reasonable method can be established at least once every 12 months, in connection with the requirement to update the privacy policy set forth in Civil Code section 1798.130, subdivision (a)(5).

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.

§ 7063. Authorized Agents.

(a) When a consumer uses an authorized agent to submit a request to delete, request to correct, or a request to know, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do either of the following:

(1) Verify their own identity directly with the business.

(2) Directly confirm with the business that they provided the authorized agent permission to submit the request.

However, businesses shall not require the consumer to resubmit their request in their individual capacity.

(b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4121 to 4130.

A business shall not require power of attorney in order for a consumer to use an authorized agent to act on their behalf.

(c) An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information.

(d) An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.

ARTICLE 6. SPECIAL RULES REGARDING CONSUMERS ~~UNDER~~ LESS THAN 16 YEARS OF AGE

§ 7070. Consumers Less Than 13 Years of Age.

(a) Process for Opting-In to Sale or Sharing of Personal Information

(1) A business that has actual knowledge that it sells or shares the personal information of a consumer less than the age of 13 shall establish, document, and comply with a reasonable method for determining that the person consenting to the sale or sharing of the personal information about the child is the parent or guardian of that child. This consent to the sale or sharing of personal information is in addition to any verifiable parental consent required under COPPA.

(2) Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to:

(A) Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;

(B) Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

(C) Having a parent or guardian call a toll-free telephone number staffed by trained personnel;

(D) Having a parent or guardian connect to trained personnel via video-conference;

(E) Having a parent or guardian communicate in person with trained personnel; and

(F) Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information, as long as the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.

(b) When a business receives consent to the sale or sharing of personal information pursuant to subsection (a), the business shall inform the parent or guardian of the right to opt-out of sale/sharing and of the process for doing so on behalf of their child pursuant to section 7026, subsections (a) – (f).

(c) A business shall establish, document, and comply with a reasonable method, in accordance with the methods set forth in subsection (a)(2), for determining that a person submitting a request to delete, request to correct, or request to know the personal information of a child under the age of 13 is the parent or guardian of that child.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

ARTICLE 7. NON-DISCRIMINATION

§ 7080. Discriminatory Practices.

(a) A price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations.

(b) A business may offer a price or service difference that is non-discriminatory. A price or service difference is non-discriminatory if it is reasonably related to the value of the consumer's data. If a business is unable to calculate a good-

faith estimate of the value of the consumer's data or cannot show that the price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the price or service difference.

(c) A business's denial of a consumer's request to delete, request to correct, request to know, request to access ADMT, ~~or~~ request to opt-out of sale/sharing, or request to opt-out of ADMT for reasons permitted by the CCPA or these regulations shall not be considered discriminatory.

(d) Illustrative examples follow:

(1) Example 1: A music streaming business offers a free service as well as a premium service that costs $5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale or sharing of their personal information, then the practice is discriminatory, unless the $5-per-month payment is reasonably related to the value of the consumer's data to the business.

(2) Example 2: A clothing business offers a loyalty program whereby customers receive a $5-off coupon by email after spending $100 with the business. A consumer submits a request to delete all personal information the business has collected about them but also informs the business that they want to continue to participate in the loyalty program. The business may deny their request to delete with regard to their email address and the amount the consumer has spent with the business because that information is necessary for the business to provide the loyalty program requested by the consumer and is reasonably anticipated within the context of the business's ongoing relationship with them pursuant to Civil Code section 1798.105, subdivision (d)(1).

(3) Example 3: A grocery store offers a loyalty program whereby consumers receive coupons and special discounts when they provide their phone numbers. A consumer submits a request to opt-out of the sale/sharing of their personal information. The retailer complies with their request but no longer allows the consumer to participate in the loyalty program. This practice is discriminatory unless the grocery store can demonstrate that the value of the coupons and special discounts are reasonably related to the value of the consumer's data to the business.

(4) Example 4: An online bookseller collects information about consumers, including their email addresses. It offers coupons to consumers through browser pop-up windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information that the bookseller has collected about them, including their email address and their browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide coupons is discriminatory unless the value of the coupons is reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete with regard to the email address because the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(e) A business shall notify consumers of any financial incentive or price or service difference subject to Civil Code section 1798.125 that it offers in accordance with section 7016.

(f) A business's charging of a reasonable fee pursuant to Civil Code section 1798.145, subdivision (h)(3), shall not be considered a financial incentive subject to these regulations.

(g) A price or service difference that is the direct result of compliance with a state or federal law shall not be considered discriminatory.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130 and 1798.185, Civil Code.

ARTICLE 8. TRAINING AND RECORD-KEEPING

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

(a) A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, shares, or otherwise makes available for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall:

(1) Compile the following metrics for the previous calendar year:

(A) The number of requests to delete that the business received, complied with in whole or in part, and denied;

(B) The number of requests to correct that the business received, complied with in whole or in part, and denied;

(C) The number of requests to know that the business received, complied with in whole or in part, and denied;

(D) The number of requests to access ADMT that the business received, complied with in whole or in part, and denied;

(E) The number of requests to opt-out of sale/sharing that the business received, complied with in whole or in part, and denied;

(F) ~~(E)~~ The number of requests to limit that the business received, complied with in whole or in part, and denied; ~~and~~

(G) The number of requests to opt-out of ADMT that the business received, complied with in whole or in part, and denied; and

(H) ~~(F)~~ The median or mean number of days within which the business substantively responded to requests to delete, requests to correct, requests to know, requests to opt-out of sale/sharing, and requests to limit.

(2) Disclose, by July 1 of every calendar year, the information compiled in subsection (a)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy. In its disclosure, a business may choose to disclose the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.

(b) A business may choose to compile and disclose the information required by subsection (a)(1) for requests received from all individuals, rather than requests received from consumers. The business shall state whether it has done so in its disclosure and shall, upon request, compile and provide to the

Attorney General the information required by subsection (a)(1) for requests received from consumers.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135 and 1798.185, Civil Code.

ARTICLE 9. CYBERSECURITY AUDITS

§ 7120. Requirement to Complete a Cybersecurity Audit.

(a) Every business whose processing of consumers' personal information presents significant risk to consumers' security as set forth in subsection (b) must complete a cybersecurity audit.

(b) A business's processing of consumers' personal information presents significant risk to consumers' security if any of the following is true:

(1) The business meets the threshold set forth in Civil Code section 1798.140, subdivision (d)(1)(C), in the preceding calendar year; or

(2) The business meets the threshold set forth in Civil Code section 1798.140, subdivision (d)(1)(A); and

(A) Processed the personal information of 250,000 or more consumers or households in the preceding calendar year; or

(B) Processed the sensitive personal information of 50,000 or more consumers in the preceding calendar year.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7121. Timing Requirements for Cybersecurity Audits and Audit Reports.

(a) A business must complete its first cybersecurity audit report no later than:

(1) April 1, 2028, if the business's annual gross revenue for 2026 was more than one hundred million dollars ($100,000,000) as of January 1, 2027. The business's audit would cover the period from January 1, 2027, through January 1, 2028.

(2) April 1, 2029, if the business's annual gross revenue for 2027 was between fifty million dollars ($50,000,000) and one hundred million dollars ($100,000,000) as of January 1, 2028. The business's audit would cover the period from January 1, 2028, through January 1, 2029.

(3) April 1, 2030, if the business's annual gross revenue for 2028 was less than fifty million dollars ($50,000,000). The business's audit would cover the period from January 1, 2029, through January 1, 2030.

(b) After April 1, 2030, if on January 1 of one year, a business meets the criteria of section 7120 for the preceding year, the business must complete a cybersecurity audit that covers the next 12 months, and the business must complete its cybersecurity audit report for that period by April 1 of the following year. For example, if Business A meets the criteria in section 7120 as of January 1, 2035, Business A's audit would cover the period from January 1, 2035, through January 1, 2036, and Business A would have to complete its cybersecurity audit report by April 1, 2036.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7122. Thoroughness and Independence of Cybersecurity Audits.

(a) Every business required to complete a cybersecurity audit pursuant to this Article must do so using a qualified, objective, independent professional ("auditor") using procedures and standards accepted in the profession of auditing, such as procedures and standards provided or adopted by the American Institute of Certified Public Accountants, the Public Company Accountability Oversight Board, the Information Systems Audit and Control Association, or the International Organization for Standardization.

(1) To be qualified, an auditor must have knowledge of cybersecurity and how to audit a business's cybersecurity program.

(2) The auditor may be internal or external to the business but must exercise objective and impartial judgment on all issues within the scope of the cybersecurity audit, must be free to make decisions and assessments without influence by the business being audited, including the business's owners, managers, or employees; and must not participate in activities that may compromise the auditor's independence. For example, the auditor must not participate in business activities that the auditor may assess in the current or subsequent cybersecurity audits, including developing procedures, preparing the business's documents, making recommendations regarding the business's cybersecurity program

(separate from articulating audit findings), or implementing or maintaining the business's cybersecurity program.

(3) If a business uses an internal auditor, to maintain the auditor's independence, the highest-ranking auditor must report directly to a member of the business's executive management team who does not have direct responsibility for the business's cybersecurity program. A member of the business's executive management team who does not have direct responsibility for the business's cybersecurity program must conduct the highest-ranking auditor's performance evaluation, if any, and determine the auditor's compensation.

(b) The business must make available to the auditor all information in the business's possession, custody, or control that the auditor requests as relevant to the cybersecurity audit (e.g., information about the business's cybersecurity program and information system and the business's use of service providers or contractors). For example, the auditor may request information to determine the scope of the cybersecurity audit and the criteria the cybersecurity audit will use.

(c) The business must make good-faith efforts to disclose to the auditor all facts relevant to the cybersecurity audit and must not misrepresent any fact relevant to the cybersecurity audit.

(d) No finding of any cybersecurity audit may rely primarily on assertions or attestations by the business's management. Cybersecurity audit findings must rely primarily upon the specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) that the auditor deems appropriate.

(e) The cybersecurity audit report must include the information set forth in section 7123, subsection (e).

(f) The cybersecurity audit report must be provided to a member of the business's executive management team who has direct responsibility for the business's cybersecurity program.

(g) The business and the auditor must retain all documents relevant to each cybersecurity audit for a minimum of five (5) years after completion of the cybersecurity audit.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7123. Scope of Cybersecurity Audit and Audit Report.

(a) The cybersecurity audit must assess how the business's cybersecurity program: protects personal information from unauthorized access, destruction, use, modification, or disclosure; and protects against unauthorized activity resulting in the loss of availability of personal information.

(b) The cybersecurity audit must assess:

(1) The business's establishment, implementation, and maintenance of its cybersecurity program, including the related written documentation thereof (e.g., policies and procedures), that is appropriate to the business's size and complexity and the nature and scope of its processing activities, taking into account the state of the art and cost of implementing the components of a cybersecurity program; and

(2) Each of the components of a cybersecurity program listed in subsection (c) that the auditor deems applicable to the business's information system.

(3) How the business implements and enforces compliance with its cybersecurity program as described in subsection (b)(1), the applicable components in subsection (c), and any additional components as set forth in subsection (d).

(c) The cybersecurity audit must assess the following components, if applicable:

(1) Authentication, including:

(A) Multi-factor authentication (including multi-factor authentication that is resistant to phishing attacks for employees, independent contractors, and any other personnel, service providers, and contractors); and

(B) If the business uses passwords or passphrases, strong unique passwords or passphrases (e.g., passwords that are at least eight characters in length, not on the business's disallowed list of commonly used passwords, and not reused).

(2) Encryption of personal information, at rest and in transit.

(3) Account management and access controls, including:

(A) Restricting each person's, account's, or application's privileges and access to personal information to what is necessary for that person, account, or application to perform their duties. For example:

(i) If the person is an employee, independent contractor, or any other personnel, restricting their privileges and access to personal information to what is necessary to perform the respective job functions of each individual, and revoking their privileges and access when their job functions no longer require them, including when their employment or contract is terminated;

(ii) If the person is a service provider or contractor, restricting their privileges and access to personal information to what is necessary for the specific business purpose(s) set forth in, and in compliance with, the written contract between the business and the service provider or contractor required by the CCPA and section 7051; and

(iii) Restricting the privileges and access of third parties to whom the business sells or shares personal information to the personal information that is necessary for the limited and specified purpose(s) set forth within the contract between the business and the third party required by the CCPA and section 7053.

(B) Restricting the number of privileged accounts, restricting those privileged accounts' access functions to only those necessary to perform the account-holder's job, restricting the use of privileged accounts to when they are necessary to perform functions, and using

a privileged-access management solution (e.g., to ensure just-in-time temporary assignment of privileged access).

(C) Restricting and monitoring the creation of new accounts for employees, independent contractors, or other personnel; service providers or contractors; and privileged accounts, and ensuring that the accounts' access and privileges are limited as set forth in subsections (c)(3)(A) and (B).

(D) Restricting and monitoring physical access to personal information (e.g., through the use of badges, secure physical file locations, and enforcement of clean-desk policies).

(4) Inventory and management of personal information and the business's information system, including:

(A) Personal information inventories (e.g., maps and flows identifying where personal information is stored, and how it can be accessed) and the classification and tagging of personal information (e.g., how personal information is tagged and how those tags are used to control the use and disclosure of personal information);

(B) Hardware and software inventories, and the use of allowlisting (i.e., discrete lists of authorized hardware and software to control what is permitted to connect to and execute on the business's information system); and

(C) Hardware and software approval processes, and preventing the connection of unauthorized hardware and devices to the business's information system.

(5) Secure configuration of hardware and software, including:

(A) Software updates and upgrades;

(B) Securing on-premises and cloud-based environments;

(C) Masking (i.e., systematically removing or replacing with symbols such as asterisks or bullets) the sensitive personal information set forth in Civil Code section 1798.145, subdivisions (ae)(1)(A) and (B)

and other personal information as appropriate by default in applications;

(D) Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and

(E) Change management (i.e., processes and procedures to ensure that changes to information system(s) do not undermine existing safeguards).

(6) Internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting (e.g., bug bounty and ethical hacking programs).

(7) Audit-log management, including the centralized storage, retention, and monitoring of logs.

(8) Network monitoring and defenses, including the deployment of:

(A) Technologies, such as bot-detection, intrusion-detection, and intrusion-prevention, which a business may use to detect unsuccessful login attempts, monitor the activity of authorized users, and detect and prevent unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information; and

(B) Data-loss-prevention systems (e.g., software to detect and prevent unauthorized access, use, or disclosure of personal information).

(9) Antivirus and antimalware protections.

(10) Segmentation of an information system (e.g., via properly configured firewalls, routers, switches).

(11) Limitation and control of ports, services, and protocols.

(12) Cybersecurity awareness, including how the business maintains current knowledge of changing cybersecurity threats and countermeasures.

(13) Cybersecurity education and training, including training for each employee, independent contractor, and any other personnel to whom the business provides access to its information system (e.g., when their employment or contract begins, annually thereafter, and after a personal information security breach, as described in Civil Code section 1798.150).

(14) Secure development and coding best practices, including code-reviews and testing.

(15) Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.

(16) Retention schedules and proper disposal of personal information no longer required to be retained, by (A) shredding, (B) erasing, or (C) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

(17) How the business manages its responses to security incidents (i.e., its incident response management).

(A) For the purposes of subsection (17), "security incident" means an occurrence that actually or imminently jeopardizes the confidentiality, integrity, or availability of the business's information system or the personal information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of the business's cybersecurity program; unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information is a security incident.

(B) The business's incident response management includes:

(i) The business's documentation of predetermined instructions or procedures to detect, respond to, limit the consequences of, and recover from malicious attacks against its information system (i.e., the business's incident response plan); and

(ii) How the business tests its incident-response capabilities; and

(18) Business-continuity and disaster-recovery plans, including data-recovery capabilities and backups.

(d) Nothing in this section prohibits a cybersecurity audit from assessing components of a cybersecurity program that are not set forth in subsections (b) or (c).

(e) The cybersecurity audit report must:

(1) Describe the business's information system; and identify (A) the policies, procedures, and practices that the cybersecurity audit assessed; (B) the criteria used for the cybersecurity audit; and (C) the specific evidence examined to make decisions and assessments, such as documents reviewed, sampling and testing performed, and interviews conducted. The cybersecurity audit report must also explain why assessing those policies, procedures, and practices; using those criteria; and examining that specific evidence justify the auditor's findings.

(2) Identify the applicable components in subsection (c), and any additional component assessed in accordance with subsection (d); describe how the business implements and enforces compliance with the policies and procedures in subsection (b)(1), the applicable components in subsection (c), and any additional component assessed in accordance with subsection (d); and explain their effectiveness in preventing unauthorized access, destruction, use, modification, or disclosure of personal information; and preventing unauthorized activity resulting in the loss of availability of personal information.

(3) Identify and describe in detail the status of any gaps or weaknesses of the policies and procedures in subsection (b)(1), the applicable components in subsection (c), and any additional component assessed in accordance with subsection (d), that the auditor deemed to increase the risk of unauthorized access, destruction, use, modification, or disclosure of consumers' personal information; or increase the risk of unauthorized activity resulting in the loss of availability of personal information.

(4) Document the business's plan to address the gaps and weaknesses identified and described pursuant to subsection (e)(3), including the timeframe in which it will resolve them.

(5) Identify any corrections or amendments to any prior cybersecurity audit reports.

(6) Include the title of up to three qualified individuals responsible for the business's cybersecurity program.

(7) Include the auditor's name, affiliation, and relevant qualifications.

(8) Include a statement that is signed and dated by the highest-ranking auditor that certifies that they completed an independent review of the business's cybersecurity program and information system, exercised objective and impartial judgment on all issues within the scope of the cybersecurity audit, and did not rely primarily on assertions or attestations by the business's management.

(9) If the business provided notification to affected consumer(s) pursuant to Civil Code section 1798.82, subdivision (a), include a sample copy of the notification(s), excluding any personal information; or a description of the notification(s).

(10) If the business was required to notify any agency with jurisdiction over privacy laws in California of unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information, include a sample copy of the notification(s), excluding any personal information; or a description of the required notification(s), the date(s) and details of the activity that gave rise to the required notification(s), and any related remediation measures taken by the business.

(f) A business may utilize a cybersecurity audit, assessment, or evaluation that it has prepared for another purpose, provided that it meets all of the requirements of this Article, either on its own or through supplementation. For example, a business may have engaged in an audit that uses the National Institute of Standards and Technology Cybersecurity Framework 2.0 and meets all of the requirements of this Article.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7124. Certification of Completion.

(a) Each calendar year that a business is required to complete a cybersecurity audit pursuant to this Article, it must submit to the Agency a written certification that the business completed the cybersecurity audit as required by this Article.

(b) The business must submit the certification no later than April 1 following any year that the business is required to complete a cybersecurity audit.

(c) The written certification must be completed by a member of the business's executive management team who:

(1) Is directly responsible for the business's cybersecurity-audit compliance;

(2) Has sufficient knowledge of the business's cybersecurity audit to provide accurate information; and

(3) Has the authority to submit the business's certification to the Agency.

(d) The written certification must be completed and submitted to the Agency via its website at https://cppa.ca.gov/. The certification must include:

(1) The business's name and point of contact for the business, including the contact's name, phone number, and email address.

(2) A statement that the business has completed the cybersecurity audit.

(3) The time period covered by the cybersecurity audit, by month and year.

(4) An electronically signed attestation to the following statement: "I attest that I meet the requirements of California Code of Regulations, Title 11, section 7124, subsection (c), to submit this certification. Under penalty of perjury under the laws of the state of California, I hereby declare that the information contained within and submitted with this certification is true and correct and that the business has not made any attempt to influence the auditor's decisions or assessments regarding the cybersecurity audit."

(5) The name and business title of the person submitting the certification, and the date of the certification.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

ARTICLE 10. RISK ASSESSMENTS

§ 7150. When a Business Must Conduct a Risk Assessment.

(a) Every business whose processing of consumers' personal information presents significant risk to consumers' privacy as set forth in subsection (b) must conduct a risk assessment before initiating that processing.

(b) Each of the following processing activities presents significant risk to consumers' privacy:

(1) Selling or sharing personal information.

(2) Processing sensitive personal information.

(A) A business that processes the sensitive personal information of its employees or independent contractors solely and specifically for purposes of administering compensation payments, determining and storing employment authorization, administering employment benefits, providing reasonable accommodation as required by law, or wage reporting as required by law, is not required to conduct a risk assessment for the processing of sensitive personal information for these purposes. Any other processing of consumers' sensitive personal information is subject to the risk-assessment requirements set forth in this Article.

(3) Using ADMT for a significant decision concerning a consumer.

(4) Using automated processing to infer or extrapolate a consumer's intelligence, ability, aptitude, performance at work, economic situation, health (including mental health), personal preferences, interests, reliability, predispositions, behavior, location, or movements, based upon systematic observation of that consumer when they are acting in their capacity as an educational program applicant, job applicant, student, employee, or independent contractor for the business.

(5) Using automated processing to infer or extrapolate a consumer's intelligence, ability, aptitude, performance at work, economic situation, health (including mental health), personal preferences, interests, reliability, predispositions, behavior, or movements, based upon that

consumer's presence in a sensitive location. "Infer or extrapolate" does not include a business using a consumer's personal information solely to deliver goods to, or provide transportation for, that consumer at a sensitive location.

(6) Processing the personal information of consumers, which the business intends to use to train an ADMT for a significant decision concerning a consumer; or train a facial-recognition, emotion-recognition, or other technology that verifies a consumer's identity, or conducts physical or biological identification or profiling of a consumer. For purposes of this paragraph, "intends to use" means the business is using, plans to use, permits others to use, plans to permit others to use, is advertising or marketing the use of, or plans to advertise or market the use of.

(c) Illustrative examples of when a business must conduct a risk assessment follow:

(1) Business A is hiring a new employee. Business A plans to videotape job interviews, then use emotion-recognition technology without human involvement to decide who to hire. Business A must conduct a risk assessment because it plans to use ADMT for a significant decision concerning a consumer.

(2) Business B provides a mobile dating application. Business B plans to disclose consumers' precise geolocation and the ethnicity and medical information the consumers provided in their dating profiles to Business B's analytics service provider. Business B must conduct a risk assessment because it plans to process sensitive personal information of consumers.

(3) Business C provides a personal-budgeting application into which consumers enter their financial information, including income. Business C plans to display advertisements to these consumers on different websites for payday loans that are based on evaluations of these consumers' personal preferences, interests, and reliability from their financial information. Business C must conduct a risk assessment because it plans to share personal information.

(4) Business D is a technology provider. Business D plans to extract faceprints from consumers' photographs to train Business D's facial-

recognition technology. Business D must conduct a risk assessment because it plans to process consumers' personal information to train a facial-recognition technology.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7151. Stakeholder Involvement for Risk Assessments.

(a) A business's employees whose job duties include participating in the processing of personal information that would be subject to a risk assessment must be included in the business's risk assessment process for that processing activity. For example, an individual who determines the method by which the business plans to collect consumers' personal information for one of the processing activities in section 7150, subsection (b), must provide that information to the individuals conducting the risk assessment.

(b) In conducting the risk assessment, a business may include external parties in the process. For example, a business may utilize or gather information from service providers, contractors, experts in detecting and mitigating bias in ADMT, a subset of the consumers whose personal information the business plans to process, or stakeholders that represent consumers' or others' interests, including consumer advocacy organizations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7152. Risk Assessment Requirements.

(a) A business must conduct a risk assessment to determine whether the risks to consumers' privacy from the processing of personal information outweigh the benefits to the consumer, the business, other stakeholders, and the public from that same processing. The risk assessment must:

(1) Identify and document in a risk assessment report the business's purpose for processing consumers' personal information. The purpose must not be identified or described in generic terms, such as "to improve our services" or for "security purposes." By contrast, if a business is "improving the service" by decreasing consumers' wait times when processing their

privacy rights requests, the business may identify this decrease of wait times to process privacy rights requests as the relevant purpose.

(2) Identify and document in a risk assessment report the categories of personal information to be processed, including any categories of sensitive personal information. This must include the minimum personal information that is necessary to achieve the purpose of processing consumers' personal information.

(3) Identify and document in a risk assessment report the following operational elements of the processing:

(A) The business's planned method for collecting, using, disclosing, retaining, or otherwise processing personal information, and the sources of the personal information.

(B) How long the business plans to retain each category of personal information, or if unknown, the criteria the business plans to use to determine that retention period.

(C) The business's method of interacting with the consumers whose personal information the business plans to process (e.g., via websites, applications, or offline) and the purpose of the interaction (e.g., to provide a good or service).

(D) The approximate number of consumers whose personal information the business plans to process.

(E) What disclosures the business has made or plans to make to the consumer about the processing of their personal information and how these disclosures were or will be made (e.g., via a just-in-time notice).

(F) The names or categories of the service providers, contractors, or third parties to whom the business discloses or makes available the consumers' personal information for the processing; and the purpose for which the business discloses or makes the consumers' personal information available to them.

(G) For the uses of ADMT set forth in section 7150, subsections (b)(3), the business must identify:

(i) The logic of the ADMT, including any assumptions or limitations of the logic; and

(ii) The output of the ADMT, and how the business will use the output to make a significant decision.

(4) Identify the benefits to the business, the consumer, other stakeholders, and the public from the processing of the personal information, as applicable. The benefits must not be identified in generic terms, such as "improving our service." By contrast, if a benefit of a processing activity is to reduce the response time to a consumer's right to know request, a business may identify the relevant benefit as enabling consumers to receive the personal information they requested on a quicker timeline.

(5) Identify the negative impacts to consumers' privacy associated with the processing. The business must identify the sources and causes of these negative impacts.

For example, negative impacts to consumers' privacy that a business may consider include the following:

(A) Unauthorized access, destruction, use, modification, or disclosure of personal information; and unauthorized activity resulting in the loss of availability of personal information.

(B) Discrimination upon the basis of protected characteristics that would violate federal or state law.

(C) Impairing consumers' control over their personal information, such as by providing insufficient information for consumers to make an informed decision regarding the processing of their personal information, or by interfering with consumers' ability to make choices consistent with their reasonable expectations.

(D) Coercing or compelling consumers into allowing the processing of their personal information, such as by conditioning consumers' acquisition or use of an online service upon their disclosure of

personal information that is unnecessary to the expected functionality of the service, or requiring consumers to consent to processing when such consent cannot be freely given (e.g., because it was obtained through the use of a dark pattern).

(E) Economic harms, including limiting or depriving consumers of economic opportunities, charging consumers higher prices, or compensating consumers at lower rates based upon profiling; or imposing additional costs upon consumers, including costs associated with the unauthorized access to consumers' personal information.

(F) Physical harms to consumers or to property, including processing that creates the opportunity for physical or sexual violence.

(G) Reputational harms, including stigmatization, that could negatively impact an average consumer, such as stigmatization of a consumer as a result of a mobile dating application's disclosure of the consumer's sexual or other preferences in a partner outside of the dating application.

(H) Psychological harms, including emotional distress, stress, anxiety, embarrassment, fear, frustration, shame, and feelings of violation, that could negatively impact an average consumer. Examples of such harms include emotional distress resulting from disclosure of nonconsensual intimate imagery or disclosure of a consumer's purchase of pregnancy tests or emergency contraception for non-medical purposes.

(6) Identify and document in a risk assessment report any safeguards that the business plans to implement for the processing, such as safeguards to address the negative impacts identified in subsection (a)(5).

(A) For example, safeguards that a business may consider include the following:

(i) Encryption, segmentation of information systems, physical and logical access controls, change management, network monitoring and defenses, and data and integrity monitoring;

(ii) Use of privacy-enhancing technologies, such as trusted execution environments, federated learning, homomorphic encryption, and differential privacy;

(iii) Consulting external parties, such as those described in section 7151, subsection (b), to ensure that the business maintains current knowledge of emergent privacy risks and countermeasures; and using that knowledge to identify, assess, and mitigate risks to consumers' privacy; and

(iv) Implementing policies, procedures, and training to ensure that the business's ADMT works for the business's purpose and does not unlawfully discriminate based upon protected characteristics.

(7) Identify and document in a risk assessment report whether it will initiate the processing subject to the risk assessment.

(8) Identify and document in a risk assessment report the individuals who provided the information for the risk assessment, except for legal counsel who provided legal advice.

(9) Identify and document in a risk assessment report the date the assessment was reviewed and approved, and the names and positions of the individuals who reviewed or approved the assessment, except for legal counsel who provided legal advice. An individual who has the authority to participate in deciding whether the business will initiate the processing that is the subject of the risk assessment must review and approve the assessment.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7153. Additional Requirements for Businesses that Process Personal Information to Train Automated Decisionmaking Technology.

(a) A business that makes ADMT available to another business ("recipient-business") to make a significant decision as set forth in section 7150, subsection (b)(3), must provide to the recipient-business all facts available to

the business that are necessary for the recipient-business to conduct its own risk assessment.

(b) The requirements of this section apply only to ADMT trained using personal information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7154. Goal of a Risk Assessment.

(a) The goal of a risk assessment is restricting or prohibiting the processing of personal information if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7155. Timing and Retention Requirements for Risk Assessments.

(a) A business must comply with the following timing requirements for conducting and updating its risk assessments:

(1) A business must conduct and document a risk assessment in accordance with the requirements of this Article before initiating any processing activity identified in section 7150, subsection (b).

(2) At least once every three years, a business must review, and update as necessary, its risk assessments to ensure that they remain accurate in accordance with the requirements of this Article.

(3) Notwithstanding subsection (a)(2) of this section, a business must update a risk assessment whenever there is a material change relating to the processing activity, as soon as feasibly possible, but no later than 45 calendar days from the date of the material change. A change relating to the processing activity is material if it creates new negative impacts or increases the magnitude or likelihood of previously identified negative impacts as set forth in section 7152, subsection (a)(5), or diminishes the

effectiveness of the safeguards as set forth in section 7152, subsection (a)(6).

Material changes may include, for example, changes to the purpose of the processing; the minimum personal information necessary to achieve the purpose of the processing; or the risks to consumers' privacy raised by consumers (e.g., numerous consumers complain to a business about the risks that the business's processing poses to their privacy).

(b) For any processing activity identified in section 7150, subsection (b), that the business initiated prior to [OAL to fill in the effective date of these regulations] and that continues after [OAL to fill in the effective date of these regulations], the business must conduct, and document as set forth in section 7152, a risk assessment in accordance with the requirements of this Article no later than December 31, 2027. The business must comply with the submission requirements set forth in section 7157, subsection (a)(1).

(c) A business must retain its risk assessments, including original and updated versions, for as long as the processing continues or for five years after the completion of the risk assessment, whichever is later.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7156. Conducting Risk Assessments for a Comparable Set of Processing Activities or in Compliance with Other Laws or Regulations.

(a) A business may conduct a single risk assessment for a comparable set of processing activities. A "comparable set of processing activities" that can be addressed by a single risk assessment is a set of similar processing activities that present similar risks to consumers' privacy.

(1) For example, Business E sells toys to children and is considering using in-store paper forms to collect names, mailing addresses, and birthdays from children that visit their stores, and to use that information to mail a coupon and list of age-appropriate toys to each child during the child's birth month and every November. Business E uses the same service providers and technology for each category of mailings across all stores. Business E must conduct a risk assessment, including documenting

required information in its risk assessment report, because it is processing sensitive personal information. Business E may use a single risk assessment for processing the personal information for the birthday mailing and November mailing across all stores because in each case it is collecting the same personal information in the same way for the purpose of sending coupons and age-appropriate toy lists to children, and this processing presents similar risks to consumers' privacy.

(b) A business may utilize a risk assessment that it has prepared for another purpose to meet the requirements in section 7152, provided that the risk assessment contains the information that must be included in, or is paired with the outstanding information necessary for, compliance with section 7152.

(1) For example, Business F plans to sell consumers' personal information. Business F conducts a risk assessment for that processing activity using a data protection assessment that is compliant with another state law. That state law requires the information that must be in section 7152, but does not explicitly require some of the information in subsections (a)(2)-(3), (7), or require the name and position of the individual who has the authority to participate in deciding whether the business will initiate the processing that is subject to the risk assessment. Business F must also include this information in its risk assessment to meet the requirements in section 7152.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7157. Submission of Risk Assessments to the Agency.

(a) Timing of Risk Assessment Submissions.

(1) For risk assessments conducted in 2026 and 2027, the business must submit to the Agency the information required by subsection (b) no later than April 1, 2028.

(2) For risk assessments conducted after 2027, the business must submit to the Agency the information required by subsection (b) no later than April 1 following any year during which the business conducted the risk assessments. For example, for risk assessments conducted in 2028, the

business must submit to the Agency the information required by subsection (b) no later than April 1, 2029.

(b) A business must submit to the Agency the following risk assessment information:

(1) The business's name and a point of contact for the business, including the contact's name, phone number, and email address.

(2) The time period covered by the submission, by month and year.

(3) The number of risk assessments conducted or updated by the business during the time period covered by the submission, in total and for each of the processing activities identified in section 7150, subsection (b).

(4) Whether the risk assessments conducted or updated by the business during the time period covered by the submission involved the processing of each of the categories of personal information and sensitive personal information identified in Civil Code section 1798.140, subdivisions (v)(1)(A)-(L), (ae)(1)(A)-(G), and (ae)(2)(A)-(C).

(5) Attestation to the following statement: "I attest that the business has conducted a risk assessment for the processing activities set forth in California Code of Regulations, Title 11, section 7150, subsection (b), during the time period covered by this submission, and that I meet the requirements of section 7157, subsection (c). Under penalty of perjury under the laws of the state of California, I hereby declare that the risk assessment information submitted is true and correct."

(6) The name and business title of the person submitting the risk assessment information, and the date of the certification.

(c) The individual submitting the information set forth in subsection (b) must be a member of the business's executive management team who:

(1) Is directly responsible for the business's risk-assessment compliance;

(2) Has sufficient knowledge of the business's risk assessment to provide accurate information; and

(3) Has the authority to submit the risk assessment information to the Agency.

(d) The risk assessment information must be submitted to the Agency via the Agency's website at https://cppa.ca.gov/.

(e) The Agency or the Attorney General may require a business to submit its risk assessment reports to the Agency or to the Attorney General at any time. A business must submit its risk assessment reports within 30 calendar days of the Agency's or the Attorney General's request.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

ARTICLE 11. AUTOMATED DECISIONMAKING TECHNOLOGY

§ 7200. When a Business's Use of Automated Decisionmaking Technology is Subject to the Requirements of This Article.

(a) A business that uses ADMT to make a significant decision concerning a consumer must comply with the requirements of this Article.

(b) A business that uses ADMT for a significant decision prior to January 1, 2027, must be in compliance with the requirements of this Article no later than January 1, 2027. A business that uses ADMT on or after January 1, 2027, must be in compliance with the requirements of this Article any time it is using ADMT for a significant decision.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7220. Pre-use Notice Requirements.

(a) A business that uses ADMT as set forth in section 7200, subsection (a), must provide consumers with a Pre-use Notice. The Pre-use Notice must inform consumers about the business's use of ADMT and consumers' rights to opt-out of ADMT and to access ADMT, as set forth in this section. A business may provide a Pre-use Notice in its Notice at Collection, provided that the Notice at Collection complies with, and includes the information required by, subsections (b) and (c).

(b) The Pre-use Notice must:

(1) Comply with section 7003, subsections (a)–(b).

(2) Be presented prominently and conspicuously to the consumer at or before the point when the business collects the consumer's personal information that the business plans to process using ADMT. If a business has already collected the consumer's personal information for a different purpose and subsequently plans to process it using ADMT for the purpose set forth in section 7200, subsection (a), the business must provide a Pre-use Notice before processing the consumer's personal information for that purpose.

(3) Be presented in the manner in which the business primarily interacts with the consumer.

(c) The Pre-use Notice must include the following:

(1) A plain language explanation of the specific purpose for which the business plans to use the ADMT. The business must not describe the purpose in generic terms, such as "to make a significant decision" without further information, because this does not describe to the consumer the specific decision for which the business plans to use ADMT with respect to them.

(2) A description of the consumer's right to opt-out of ADMT and how the consumer can submit a request to opt-out of ADMT.

(A) If the business is not required to provide the ability to opt-out because it is relying upon the human appeal exception set forth in section 7221, subsection (b)(1), the business must instead inform the consumer of their ability to appeal the decision and provide instructions to the consumer on how to submit their appeal.

(B) If the business is not required to provide the ability to opt-out because it is relying upon another exception set forth in section 7221, subsection (b), the business must identify the specific exception it is relying upon.

(3) A description of the consumer's right to access ADMT with respect to the consumer and how the consumer can submit their request to access ADMT to the business.

(4) That the business is prohibited from retaliating against consumers for exercising their CCPA rights.

(5) Additional information about how the ADMT works to make a significant decision about consumers, and how the significant decision would be made if a consumer opts out. The business may provide this information via a simple and easy-to-use method (e.g., a layered notice or hyperlink). The additional information must include a plain language explanation of the following:

(A) How the ADMT processes personal information to make a significant decision about consumers, including the categories of personal information that affect the output generated by the ADMT. An "output" may include predictions, decisions, and recommendations (e.g., numerical scores of compatibility).

(B) The type of output generated by the ADMT, and how that output is used to make a significant decision. For example, this may include whether the output is the sole factor in the decisionmaking process or what the other factors are in that decisionmaking process; and to the extent that a human is part of the decisionmaking process in a manner that does not meet the requirements of "human involvement" in section 7001, subsection (e)(1), what that human's role is in the decisionmaking process.

(C) What the alternative process for making a significant decision is for consumers who opt out, unless an exception to providing the opt-out of ADMT set forth in section 7221, subsection (b), applies.

(d) In providing the information required by subsection (c)(5), a business's Pre-use Notice is not required to include:

(1) Trade secrets, as defined in Civil Code section 3426.1, subdivision (d); or

(2) Information that would compromise the business's ability to:

(A) Prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information;

(B) Resist malicious, deceptive, fraudulent, or illegal actions directed at the business or at consumers, or to prosecute those responsible for those actions; or

(C) Ensure the physical safety of natural persons.

(e) A business may provide a consolidated Pre-use Notice as set forth below, provided that the consolidated Pre-use Notice includes the information required by this Article for each of the business's proposed uses of ADMT:

(1) The business's use of a single ADMT for multiple purposes. For example, an employer may provide a consolidated Pre-use Notice to an employee that addresses the employer's proposed use of productivity monitoring software to determine the employee's allocation/assignment of work and compensation, and to determine which employees will be demoted.

(2) The business's use of multiple ADMTs for a single purpose. For example, a business may provide a consolidated Pre-use Notice to a job applicant that addresses the business's proposed use of: (1) software to screen applicants' resumes to determine which applicants it will hire, and (2) software to evaluate applicants' vocal intonation, facial expression, and gestures to determine which applicants to hire.

(3) The business's use of multiple ADMTs for multiple purposes. For example, an educational provider may provide a consolidated Pre-use Notice to a new student that addresses the educational provider's proposed use of: (A) software that automatically screens students' work for plagiarism to determine whether they will be suspended, and (B) software that automatically assesses students' exams to determine whether to grant them a diploma or certificate.

(4) The systematic use of a single ADMT. For example, a business may provide a consolidated Pre-use Notice to an employee that addresses the business's methodical and regular use of ADMT to allocate work to its employees, rather than providing a Pre-use Notice to the same employees each time it proposes to use the same ADMT for the same purpose.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7221. Requests to Opt-Out of ADMT.

(a) A business must provide consumers with the ability to opt-out of the use of ADMT to make a significant decision concerning the consumer, except as set forth in subsection (b).

(b) A business is not required to provide consumers with the ability to opt-out of a business's use of ADMT to make a significant decision in the following circumstances:

(1) The business provides the consumer with a method to appeal the decision to a human reviewer who has the authority to overturn the decision. To qualify for this exception, the business must do the following:

(A) Designate a human reviewer to review and analyze the output of the ADMT and any other information that is relevant to change the significant decision at issue. This human reviewer must consider the information provided by the consumer in support of their appeal and may consider any other sources of information about the significant decision. The human reviewer must know how to interpret and use the output of the ADMT that made the significant decision being appealed and must have the authority to change the decision based on their analysis.

(B) Clearly describe to the consumer how to submit an appeal and enable the consumer to provide information to the human reviewer in support of their appeal. The method of appeal must be easy for the consumers to execute, require minimal steps, and comply with section 7004. Disclosures and communications with consumers concerning the appeal must comply with section 7003, subsections (a)–(b). The timeline for requests to appeal ADMT must comply with section 7021. Businesses must comply with the verification requirements set forth in Article 5 when a consumer submits an appeal.

(2) For admission, acceptance, or hiring decisions as set forth in section 7001, subsections (ddd)(3)(A) and (ddd)(4)(A), if the following are true:

(A) The business uses the ADMT solely for the business's assessment of the consumer's ability to perform at work or in an educational program to determine whether to admit, accept, or hire them; and

(B) The ADMT works for the business's purpose and does not unlawfully discriminate based upon protected characteristics.

(3) For allocation/assignment of work and compensation decisions as set forth in section 7001, subsection (ddd)(4)(B), if the following are true:

(A) The business uses the ADMT solely for the business's allocation/assignment of work or compensation; and

(B) The ADMT works for the business's purpose and does not unlawfully discriminate based upon protected characteristics.

(c) A business that uses ADMT as set forth in subsection (a) must provide two or more designated methods for submitting requests to opt-out of ADMT. A business must consider the methods by which it interacts with consumers, the manner in which the business uses the ADMT, and the ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of the business's use of the ADMT. At least one method offered must reflect the manner in which the business primarily interacts with the consumer. Illustrative examples and requirements follow.

(1) A business that interacts with consumers online must, at a minimum, allow consumers to submit requests to opt-out through an interactive form accessible via an opt-out link that is provided in the Pre-use Notice. The link title must state what the consumer is opting out of, such as "Opt-out of Automated Decisionmaking Technology."

(2) A business that interacts with consumers in person and online may provide an in-person method for submitting requests to opt-out in addition to the online form.

(3) Other methods for submitting requests to opt-out include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, and a form submitted through the mail.

(4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to opt-out of the business's use of ADMT because cookies concern the collection of personal information and not necessarily the use of ADMT. An acceptable method for submitting requests to opt-out must be specific to the right to opt-out of the business's use of the ADMT.

(d) A business's methods for submitting requests to opt-out of ADMT must be easy for consumers to execute, must require minimal steps, and must comply with section 7004.

(e) A business must not require a consumer submitting a request to opt-out of ADMT to create an account or provide additional information beyond what is necessary to direct the business to opt-out the consumer.

(f) A business must not require a verifiable consumer request for a request to opt-out of ADMT set forth in subsection (a). A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information is subject to the business's use of ADMT. However, to the extent that the business can comply with a request to opt-out of ADMT without additional information, it must do so.

(g) If a business has a good-faith, reasonable, and documented belief that a request to opt-out of ADMT is fraudulent, the business may deny the request. The business must inform the requestor that it will not comply with the request and must provide to the requestor an explanation why it believes the request is fraudulent.

(h) A business must provide a means by which the consumer can confirm that the business has processed their request to opt-out of ADMT.

(i) In responding to a request to opt-out of ADMT, a business may present the consumer with the choice to allow specific uses of ADMT as long as the business also offers a single option to opt-out of all of the business's uses of ADMT set forth in subsection (a).

(j) A consumer may use an authorized agent to submit a request to opt-out of ADMT as set forth in subsection (a) on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf.

(k) Except as allowed by these regulations, a business must wait at least 12 months from the date the business receives the consumer's request to opt-out of ADMT before asking a consumer who has exercised their right to opt-out of ADMT, to consent to the business's use of the ADMT for which the consumer previously opted out.

(*l*) A business must not retaliate against a consumer because the consumer exercised their opt-out right as set forth in Civil Code section 1798.125 and Article 7.

(m) If the consumer submits a request to opt-out of ADMT before the business has initiated that processing, the business must not initiate processing of the consumer's personal information using that ADMT.

(n) If the consumer did not opt-out in response to the Pre-use Notice, and submitted a request to opt-out of ADMT after the business initiated the processing, the business must comply with the consumer's opt-out request by:

(1) Ceasing to process the consumer's personal information using that ADMT as soon as feasibly possible, but no later than 15 business days from the date the business receives the request; and

(2) Notifying all the business's service providers, contractors, or other persons to whom the business has disclosed or made personal information available to process the consumer's personal information using that ADMT, that the consumer has made a request to opt-out of that ADMT and instructing them to comply with the consumer's request to opt-out of that ADMT within the same time frame.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.185, Civil Code.

§ 7222. Requests to Access ADMT.

(a) A business that uses ADMT to make a significant decision must provide a consumer with information about this use when responding to a consumer's request to access ADMT.

(b) When responding to a consumer's request to access ADMT, a business must provide plain language explanations of the following information to the consumer:

(1) The specific purpose for which the business used ADMT with respect to the consumer. The business must not describe the purpose in generic terms, such as "to improve our services."

(2) Information about the logic of the ADMT. Such information must enable a consumer to understand how the ADMT processed their personal information to generate an output with respect to them, which may include the parameters that generated the output as well as the specific output with respect to the consumer.

(3) The outcome of the decisionmaking process for the consumer, including how the business used the output of the ADMT to make a significant decision with respect to the consumer. For example, this may include information about whether the output was the sole factor to make the decision; and if it was not the sole factor, which other factors played a role in making the decision; and to the extent that a human was part of the decisionmaking process in a manner that does not meet the requirements of "human involvement" in section 7001, subsection (e)(1), what that human's role was in the decisionmaking process.

(A) If the business also plans to use the output to make an additional significant decision concerning the consumer in the future, the business's explanation must include how the business plans to use that output to make a significant decision about the consumer in the future. For example, this may include whether the output will be the sole factor in the decisionmaking process or what the other factors will be in that decisionmaking process; and to the extent that a human will be part of the decisionmaking process in a manner that does not meet the requirements of "human involvement" in section 7001, subsection (e)(1), what that human's role will be in the decisionmaking process.

(4) That the business is prohibited from retaliating against consumers for exercising their CCPA rights, and instructions for how the consumer can exercise their other CCPA rights. These instructions must include any links to an online request form or portal for making such a request, if offered by the business.

(A) The business may comply with the instructions requirement by providing a link that takes the consumer directly to the specific section of the business's privacy policy that contains these instructions. Directing the consumer to the beginning of the privacy

policy, or to another section of the privacy policy that does not contain these instructions, so that the consumer is required to scroll through other information in order to find the instructions, does not satisfy the instructions requirement.

(c) In providing the information required by subsections (b)(2)–(3), a business's response to a consumer's request to access ADMT is not required to include:

(1) Trade secrets, as defined in Civil Code section 3426.1, subdivision (d); or

(2) Information that would compromise the business's ability to:

(A) Prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information;

(B) Resist malicious, deceptive, fraudulent, or illegal actions directed at the business or at consumers, or to prosecute those responsible for those actions; or

(C) Ensure the physical safety of natural persons.

(d) A business's methods for consumers to submit requests to access ADMT must be easy to use and must not use dark patterns. A business may use its existing methods to submit requests to know, delete, or correct as set forth in section 7020 for requests to access ADMT.

(e) A business must comply with the verification requirements set forth in Article 5 for requests to access ADMT. If a business cannot verify the identity of the person making the request to access ADMT, the business must inform the requestor that it cannot verify their identity.

(f) If a business denies a consumer's verified request to exercise their right to access ADMT, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business must inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business must disclose the other information sought by the consumer.

(g) A business must use reasonable security measures when transmitting the requested information to the consumer.

(h) If a business maintains a password-protected account with the consumer, it may comply with a request to access ADMT by using a secure self-service portal for consumers to access, view, and receive a portable copy of their requested information if the portal fully discloses the requested information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 5.

(i) A service provider or contractor must provide assistance to the business in responding to a verifiable consumer request to access ADMT, including by providing the business with the consumer's personal information it has in its possession that it collected pursuant to their written contract with the business, or by enabling the business to access that personal information.

(j) A business that used an ADMT with respect to a consumer more than four times within a 12-month period may provide an aggregate-level response to the consumer's request to access ADMT. Specifically, for the information required by subsection (b)(2), the business may provide a summary of the outputs with respect to the consumer over the preceding 12 months; the parameters that, on average over the preceding 12 months, affected the outputs with respect to the consumer; and a summary of how those parameters applied to the consumer.

(k) A business must not retaliate against a consumer because the consumer exercised their right to access ADMT as set forth in Civil Code section 1798.125 and Article 7.

(*l*) Nothing in this section prohibits a business from providing additional information to enable a consumer to understand how the ADMT was used to make a significant decision with respect to them. For example, a business may provide the range of possible outputs or aggregate output statistics to help a consumer understand how they compare to other consumers, such as the five most common outputs of the ADMT and the percentage of consumers that received each of those outputs during the preceding calendar year.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.185, Civil Code.

ARTICLE 12. INSURANCE COMPANIES

§ 7270. Definition of Insurance Company.

(a) For the purposes of these regulations, insurance company shall mean any person that is subject to the California Insurance Code and its regulations. Insurance company shall include insurance institutions, agents, and insurance-support organizations, as those terms are defined in Insurance Code, section 791.02.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7271. General Application of the CCPA to Insurance Companies.

(a) Insurance companies that meet the definition of "business" under the CCPA shall comply with the CCPA with regard to any personal information not subject to the Insurance Code and its regulations. For example, those insurance companies shall comply with the CCPA for personal information that is collected for purposes not in connection with an insurance transaction, as that term is defined in Insurance Code, section 791.02.

(b) Illustrative examples follow.

(1) Insurance company A collects personal information from visitors of its website who have not applied for any insurance product or other financial product or service from Company A. This information is used to tailor personalized advertisements across different business websites. Insurance company A must comply with the CCPA, including by providing consumers the right to opt-out of the sale/sharing of their personal information and honoring opt-out preference signals, because the personal information collected from the website browsing is not related to an application for or provision of an insurance transaction or other financial product or service.

(2) Insurance company B collects personal information from its employees and job applicants for employment purposes. Insurance company B must comply with the CCPA with regard to employee information, including by providing a Notice at Collection to the employees and job applicants at or

before the time their personal information is collected. This is because the personal information collected in this situation is not subject to the Insurance Code or its regulations.

(3) Sloane submits personal information to her insurance company as part of a claim for losses incurred by a fire at her home. This information is used to service the insurance policy, and thus subject to the Insurance Code and its regulations. This information is not subject to the CCPA.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135, 1798.145, 1798.150, 1798.155, 1798.185, Civil Code.

ARTICLE ~~9~~ 13. INVESTIGATIONS AND ENFORCEMENT

§ 7300. Sworn Complaints Filed with the Agency.

(a) Requirements for filing a sworn complaint. Sworn complaints ~~may~~ must be filed with the Enforcement Division via the electronic complaint system available on the Agency's website at https://cppa.ca.gov/ or submitted in person or by mail to the headquarters office of the Agency.

A complaint must:

(1) Identify the business, service provider, contractor, or person who allegedly violated the CCPA;

(2) State the facts that support each alleged violation and include any documents or other evidence supporting this conclusion;

(3) Authorize the alleged violator and the Agency to communicate regarding the complaint, including disclosing the complaint and any information relating to the complaint;

(4) Include the name and current contact information of the complainant; and

(5) Be signed and submitted under penalty of perjury.

(b) The Enforcement Division will notify the complainant in writing of the action, if any, the Agency has taken or plans to take on the complaint, together with the reasons for that action or nonaction. Duplicate complaints submitted by the same complainant may be rejected without notice.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.199.45, Civil Code.

§ 7302. Probable Cause Proceedings.

(a) Probable Cause. Under Civil Code section 1798.199.50, probable cause exists when the evidence supports a reasonable belief that the CCPA has been violated.

(b) Probable Cause Notice. The ~~Enforcement Division~~ Agency will provide the alleged violator with notice of the probable cause proceeding as required by Civil Code section 1798.199.50.

(c) Probable Cause Proceeding.

(1) The proceeding shall be closed to the public and conducted in whole or in part by telephone or videoconference unless the alleged violator files, at least 10 business days before the proceeding, a written request for an in-person or public proceeding. ~~If the proceeding is not open to the public, then the proceeding may be conducted in whole or in part by telephone or videoconference.~~

(2) The Agency shall conduct the proceeding informally. Only the alleged violator(s), their legal counsel, and the Enforcement Division shall have the right to participate at the proceeding. The Agency 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.

(3) If the alleged violator(s) fails to ~~participate or appear at~~ attend the probable cause proceeding, the alleged violator(s) waives the right to further probable cause proceedings under Civil Code section 1798.199.50, and the Agency shall determine whether there is probable cause based on the notice and any information or arguments provided by the Enforcement Division.

(d) Probable Cause Determination. The Agency shall issue a written decision with its probable cause determination and serve it on the alleged violator electronically or by mail. The Agency's probable cause determination is final and not subject to appeal.

~~(e) Notices of probable cause and probable cause determinations shall not be open to the public nor admissible in evidence in any action or special proceeding other than one enforcing the CCPA.~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.199.50, Civil Code.