NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document : Secure Controls Framework (SCF) version 2025.4
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **California Consumer Privacy Act (CCPA) January 2026 (amended California Privacy Rights Act (CPRA))**
Focal Document URL: https://cppa.ca.gov/regulations/pdf/ccpa_statute_eff_20260101.pdf
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-us-state-ca-ccpa-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7000	Title and Scope	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7000(a)	N/A	This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as “these regulations.” These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7000(b)	N/A	A violation of these regulations shall constitute a violation of the CCPA and be subject to the remedies provided for therein.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7001	Definitions	See Focal Document for details	Functional	Subset Of	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	10	
7002	Restrictions on the Collection and Use of Personal Information	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7002(a)	N/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:	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
7002(a)(1)	N/A	The purpose(s) for which the personal information was collected or processed, which shall comply with the requirements set forth in subsection (b); or	Functional	Intersects With	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	8	
7002(a)(2)	N/A	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).	Functional	Intersects With	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	5	
7002(b)	N/A	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:	Functional	Subset Of	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
7002(b)(1)	N/A	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.	Functional	Subset Of	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
7002(b)(2)	N/A	The type, nature, and amount of personal information that the business plans 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.	Functional	Subset Of	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
7002(b)(3)	N/A	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.	Functional	Subset Of	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
7002(b)(4)	N/A	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.	Functional	Intersects With	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	8	
7002(b)(5)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7002(c)	N/A	Whether another disclosed purpose is compatible with the context in which the personal information was collected shall be based on the following:	Functional	Subset Of	Purpose Compatibility	PRI-02.8	Mechanisms exist to periodically assess disclosed purposes for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared to ensure compatibility with reasonable consumer expectations.	10	
7002(c)(1)	N/A	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).	Functional	Subset Of	Purpose Compatibility	PRI-02.8	Mechanisms exist to periodically assess disclosed purposes for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared to ensure compatibility with reasonable consumer expectations.	10	
7002(c)(2)	N/A	The other disclosed purpose for which the business plans 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) – (e)(8).	Functional	Subset Of	Purpose Compatibility	PRI-02.8	Mechanisms exist to periodically assess disclosed purposes for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared to ensure compatibility with reasonable consumer expectations.	10	
7002(c)(3)	N/A	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.	Functional	Subset Of	Purpose Compatibility	PRI-02.8	Mechanisms exist to periodically assess disclosed purposes for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared to ensure compatibility with reasonable consumer expectations.	10	
7002(d)	N/A	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:	Functional	Subset Of	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
7002(d)(1)	N/A	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.	Functional	Subset Of	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
7002(d)(2)	N/A	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.	Functional	Subset Of	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
7002(d)(3)	N/A	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.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
7002(e)	N/A	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.	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
7002(f)	N/A	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).	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7002(f)	N/A	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).	Functional	Intersects With	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	8	
7003	Requirements for Disclosures and Communications to Consumers.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7003(a)	N/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.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	8	
7003(a)	N/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.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	8	
7003(b)	N/A	Disclosures required under Article 2 shall also:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7003(b)(1)	N/A	Use a format that makes the disclosure readable, including on smaller screens, if applicable.	Functional	Subset Of	Privacy Notice Formatting	PRI-02.9	Mechanisms exist to reasonably accommodate data privacy notice formatting for consumers requiring alternative formatting due to accessibility needs through: (1) Screen resolution / screen sizes; (2) Multilingual support; and/or (3) Disability-specific concessions.	10	
7003(b)(2)	N/A	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.	Functional	Subset Of	Privacy Notice Formatting	PRI-02.9	Mechanisms exist to reasonably accommodate data privacy notice formatting for consumers requiring alternative formatting due to accessibility needs through: (1) Screen resolution / screen sizes; (2) Multilingual support; and/or (3) Disability-specific concessions.	10	
7003(b)(3)	N/A	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.	Functional	Subset Of	Privacy Notice Formatting	PRI-02.9	Mechanisms exist to reasonably accommodate data privacy notice formatting for consumers requiring alternative formatting due to accessibility needs through: (1) Screen resolution / screen sizes; (2) Multilingual support; and/or (3) Disability-specific concessions.	10	
7003(c)	N/A	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 any internet webpage where personal information is collected.	Functional	Intersects With	Conspicuous Link To Data Privacy Notice	PRI-17.1	Mechanisms exist to include a conspicuous link to the organization's data privacy notice on all consumer-facing websites and mobile applications.	5	
7003(d)	N/A	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 must also be accessible through a link within the application, such as through the application's settings menu.	Functional	Intersects With	Conspicuous Link To Data Privacy Notice	PRI-17.1	Mechanisms exist to include a conspicuous link to the organization's data privacy notice on all consumer-facing websites and mobile applications.	5	
7004	Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)	N/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:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)(1)	N/A	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.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	8	
7004(a)(2)	N/A	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.	Functional	Equal	Symmetry In Choice	PRI-02.10	Mechanisms exist to ensure symmetry in choice, where options presented to consumers for more protective options are not longer, more difficult, nor more time-consuming than less protective options.	10	
7004(a)(2)(A)	N/A	It is not symmetrical when a business's process for submitting a request to optout of sale/sharing requires more steps than that business's process for optingin to the sale of personal information. For example, the number of steps for submitting a request to opt-out of sale/sharing as 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 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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)(2)(B)	N/A	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."	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)(2)(C)	N/A	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."	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)(2)(D)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)(2)(E)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)(3)	N/A	Do not use language or interactive elements that are confusing to the consumer. The methods 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.	Functional	Subset Of	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	10	
7004(a)(3)(A)	N/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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)(3)(B)	N/A	Toggles or buttons that state "on" or "off" are confusing to a consumer if they do not include further clarifying language.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)(3)(C)	N/A	The unintuitive placement of buttons to confirm a consumer's choice 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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)(3)(D)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)(3)(E)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)(4)	N/A	Do not use choice architecture that impairs or interferes with the consumer's ability to make a choice. Businesses 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.	Functional	Subset Of	Choice Architecture	PRI-02.11	Mechanisms exist to avoid choice architecture that impairs, interferes with or subverts a consumer's ability to make well-informed choices.	10	
7004(a)(4)(A)	N/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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7004(a)(4)(B)	N/A	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 locationbased 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 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).	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)(4)(C)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)(5)	N/A	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 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.	Functional	Subset Of	Choice Architecture Testing	PRI-02.12	Mechanisms exist to perform testing of choice architecture to ensure it does not undermine a consumer's ability to submit choice selections.	10	
7004(a)(5)(A)	N/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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)(5)(B)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)(5)(C)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(a)(5)(D)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7004(b)	N/A	A method that does not comply with subsection (a) may be 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.	Functional	Subset Of	Choice Architecture	PRI-02.11	Mechanisms exist to avoid choice architecture that impairs, interferes with or subverts a consumer's ability to make well-informed choices.	10	
7004(c)	N/A	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 still a dark pattern.	Functional	Subset Of	Choice Architecture	PRI-02.11	Mechanisms exist to avoid choice architecture that impairs, interferes with or subverts a consumer's ability to make well-informed choices.	10	
7010	Overview of Required Disclosures.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7010(a)	N/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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7010(b)	N/A	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.	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	8	
7010(c)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7010(d)	N/A	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).	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7010(e)	N/A	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.	Functional	Intersects With	Active Participation By Data Subjects	PRI-03.7	Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.).	5	
7010(f)	N/A	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.	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent.	5	
7010(f)	N/A	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.	Functional	Intersects With	Active Participation By Data Subjects	PRI-03.7	Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.).	5	
7010(g)	N/A	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.	Functional	Subset Of	Notice of Financial Incentive	PRI-17.2	Mechanisms exist to provide data subjects with a Notice of Financial Incentive that explains the material terms of a financial incentive, price or service difference so the data subject can make an informed decision about whether to participate.	10	
7011	Privacy Policy.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7011(a)	N/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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7011(b)	N/A	The privacy policy shall comply with section 7003, subsections (a) and (b).	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7011(c)	N/A	The privacy policy shall be available in a format that allows a consumer to print it out as a document.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7011(d)	N/A	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 must also include a link to the privacy policy in the application’s settings menu.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7011(e)	N/A	The privacy policy shall include the following information:	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7011(e)(1)	N/A	A comprehensive description of the business’s online and offline information practices, which includes the following:	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(1)(A)	N/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) – (K) and (ae)(1) – (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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(1)(B)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(1)(C)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(1)(D)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7011(e)(1)(E)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(1)(F)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(1)(G)	N/A	A statement regarding whether the business has actual knowledge that it sells or shares the personal information of consumers under 16 years of age.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(1)(H)	N/A	Identification of the categories of personal information, if any, that the business has disclosed to a service provider or contractor for a business purpose 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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(1)(I)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(1)(J)	N/A	A statement regarding whether the business uses or discloses sensitive personal information for purposes other than those specified in section 7027, subsection (m).	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(2)	N/A	An explanation of the rights that the CCPA confers on consumers regarding their personal information, which includes all of the following:	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(2)(A)	N/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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7011(e)(2)(B)	N/A	The right to delete personal information that the business has collected from the consumer, subject to certain exceptions.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(2)(C)	N/A	The right to correct inaccurate personal information that a business maintains about a consumer.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(2)(D)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(2)(E)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(2)(F)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(2)(G)	N/A	If the business uses ADMT as set forth in section 7200, subsection (a), the right to access ADMT.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(2)(H)	N/A	The right not to be retaliated against 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, or an independent contractor.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(3)	N/A	An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes all of the following:	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7011(e)(3)(A)	N/A	An explanation of the methods by which the consumer can exercise their CCPA rights.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(3)(B)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(3)(C)	N/A	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).	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(3)(D)	N/A	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).	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(3)(E)	N/A	A general description of the process the business uses to verify a consumer request to know, request to delete, request to correct, and request to access ADMT, when applicable, including any information the consumer must provide.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(3)(F)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(3)(G)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(3)(H)	N/A	Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7011(e)(3)(I)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(3)(J)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7011(e)(4)	N/A	Date the privacy policy was last updated.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7011(e)(5)	N/A	If subject to the data reporting requirements set forth in section 7102, the information required under section 7102, or a link to that information.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7012	Notice at Collection of Personal Information.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7012(a)	N/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.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
7012(b)	N/A	The Notice at Collection shall comply with section 7003, subsections (a) and (b).	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
7012(c)	N/A	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.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
7012(c)(1)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7012(c)(2)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7012(c)(3)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7012(c)(4)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7012(d)	N/A	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.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
7012(e)	N/A	A business shall include the following in its Notice at Collection:	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7012(e)(1)	N/A	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.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
7012(e)(2)	N/A	The purpose(s) for which the categories of personal information, including categories of sensitive personal information, are collected and used.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
7012(e)(3)	N/A	Whether each category of personal information identified in subsection (e)(1) is sold or shared.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
7012(e)(4)	N/A	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.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
7012(e)(5)	N/A	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.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
7012(e)(6)	N/A	A link to the business's privacy policy, or in the case of offline notices, where the privacy policy can be found online.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7012(f)	N/A	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) – (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 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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7012(g)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7012(g)(1)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7012(g)(2)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7012(g)(2)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	8	
7012(g)(2)	N/A	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.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
7012(g)(3)	N/A	Illustrative examples follow.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7012(g)(3)(A)	N/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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7012(g)(3)(B)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7012(g)(3)(C)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7012(h)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7012(i)	N/A	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.	Functional	Intersects With	Data Brokers	PRI-20	Mechanisms exist to ensure data brokers that collect Personal Data (PD) from a source other than directly from the data subject adhere to all applicable statutory, regulatory and/or contractual obligations.	8	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7013	Notice of Right to Opt-out of Sale/Sharing and the "Do Not Sell or Share My Personal Information" Link.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7013(a)	N/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.	Functional	Equal	Notice of Right To Opt-Out	PRI-21	Mechanisms exist to include within the data privacy notice a notification to data subjects of: (1) Their right to direct an organization that sells or shares their Personal Data (PD) to stop selling or sharing their PD; and (2) The methods available to exercise that right.	10	
7013(b)	N/A	The Notice of Right to Opt-out of Sale/Sharing shall comply with section 7003, subsections (a) and (b).	Functional	Subset Of	Notice of Right To Opt-Out	PRI-21	Mechanisms exist to include within the data privacy notice a notification to data subjects of: (1) Their right to direct an organization that sells or shares their Personal Data (PD) to stop selling or sharing their PD; and (2) The methods available to exercise that right.	10	
7013(c)	N/A	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).	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7013(d)	N/A	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.	Functional	Intersects With	Notice of Right To Opt-Out	PRI-21	Mechanisms exist to include within the data privacy notice a notification to data subjects of: (1) Their right to direct an organization that sells or shares their Personal Data (PD) to stop selling or sharing their PD; and (2) The methods available to exercise that right.	5	
7013(e)	N/A	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:	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7013(e)(1)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7013(e)(2)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7013(e)(3)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7013(e)(3)(A)	N/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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7013(e)(3)(B)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7013(e)(3)(C)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7013(e)(3)(D)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7013(f)	N/A	A business shall include the following in its Notice of Right to Opt-out of Sale/Sharing:	Functional	Subset Of	Notice of Right To Opt-Out	PRI-21	Mechanisms exist to include within the data privacy notice a notification to data subjects of: (1) Their right to direct an organization that sells or shares their Personal Data (PD) to stop selling or sharing their PD; and (2) The methods available to exercise that right.	10	
7013(f)(1)	N/A	A description of the consumer’s right to opt-out of the sale or sharing of their personal information by the business; and	Functional	Subset Of	Notice of Right To Opt-Out	PRI-21	Mechanisms exist to include within the data privacy notice a notification to data subjects of: (1) Their right to direct an organization that sells or shares their Personal Data (PD) to stop selling or sharing their PD; and (2) The methods available to exercise that right.	10	
7013(f)(2)	N/A	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.	Functional	Subset Of	Notice of Right To Opt-Out	PRI-21	Mechanisms exist to include within the data privacy notice a notification to data subjects of: (1) Their right to direct an organization that sells or shares their Personal Data (PD) to stop selling or sharing their PD; and (2) The methods available to exercise that right.	10	
7013(g)	N/A	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:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7013(g)(1)	N/A	It does not sell or share personal information; and	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7013(g)(2)	N/A	It states in its privacy policy that it does not sell or share personal information.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7013(h)	N/A	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.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
7014	Notice of Right to Limit and the "Limit the Use of My Sensitive Personal Information" Link.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7014(a)	N/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.	Functional	Subset Of	Notice of Right To Limit	PRI-02.13	Mechanisms exist to include within the data privacy notice a notification to data subjects of: (1) Their right to limit the use and disclosure of their sensitive Personal Data (sPD); and (2) The methods available to exercise that right.	10	
7014(b)	N/A	The Notice of Right to Limit shall comply with section 7003, subsections (a) and (b).	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7014(c)	N/A	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).	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7014(d)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7014(e)	N/A	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:	Functional	Subset Of	Notice of Right To Limit	PRI-02.13	Mechanisms exist to include within the data privacy notice a notification to data subjects of: (1) Their right to limit the use and disclosure of their sensitive Personal Data (sPD); and (2) The methods available to exercise that right.	10	
7014(e)(1)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7014(e)(2)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7014(e)(3)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7014(e)(3)(A)	N/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).	Functional	Subset Of	Alternative Means To Deliver Privacy Notice	PRI-02.14	Mechanisms exist to provide data subjects with a data privacy notice through alternative means for interactions that do not utilize an interface on a website or application.	10	
7014(e)(3)(B)	N/A	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.	Functional	Subset Of	Alternative Means To Deliver Privacy Notice	PRI-02.14	Mechanisms exist to provide data subjects with a data privacy notice through alternative means for interactions that do not utilize an interface on a website or application.	10	
7014(e)(3)(C)	N/A	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.	Functional	Subset Of	Alternative Means To Deliver Privacy Notice	PRI-02.14	Mechanisms exist to provide data subjects with a data privacy notice through alternative means for interactions that do not utilize an interface on a website or application.	10	
7014(e)(3)(D)	N/A	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.	Functional	Subset Of	Alternative Means To Deliver Privacy Notice	PRI-02.14	Mechanisms exist to provide data subjects with a data privacy notice through alternative means for interactions that do not utilize an interface on a website or application.	10	
7014(f)	N/A	A business shall include the following in its Notice of Right to Limit:	Functional	Subset Of	Notice of Right To Limit	PRI-02.13	Mechanisms exist to include within the data privacy notice a notification to data subjects of: (1) Their right to limit the use and disclosure of their sensitive Personal Data (sPD); and (2) The methods available to exercise that right.	10	
7014(f)(1)	N/A	A description of the consumer's right to limit; and	Functional	Subset Of	Notice of Right To Limit	PRI-02.13	Mechanisms exist to include within the data privacy notice a notification to data subjects of: (1) Their right to limit the use and disclosure of their sensitive Personal Data (sPD); and (2) The methods available to exercise that right.	10	
7014(f)(2)	N/A	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.	Functional	Subset Of	Notice of Right To Limit	PRI-02.13	Mechanisms exist to include within the data privacy notice a notification to data subjects of: (1) Their right to limit the use and disclosure of their sensitive Personal Data (sPD); and (2) The methods available to exercise that right.	10	
7014(g)	N/A	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:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7014(g)(1)	N/A	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	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7014(g)(2)	N/A	It only collects or processes sensitive personal information without the purpose of inferring characteristics about a consumer, and states so in its privacy policy.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7014(h)	N/A	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.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7014(h)	N/A	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.	Functional	Intersects With	Opt-Out Links	PRI-21.1	Mechanisms exist to publish conspicuous links for data subjects to exercise their rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	8	
7015	Alternative Opt-out Link.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7015(a)	N/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.	Functional	Equal	Alternative Out-Out Link	PRI-21.2	Mechanisms exist to publish a single, clearly-labeled link that allows data subjects to efficiently exercise their opt-out rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	10	
7015(b)	N/A	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.	Functional	Subset Of	Alternative Out-Out Link	PRI-21.2	Mechanisms exist to publish a single, clearly-labeled link that allows data subjects to efficiently exercise their opt-out rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	10	
7015(b)(1)	N/A	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).	Functional	Subset Of	Alternative Out-Out Link	PRI-21.2	Mechanisms exist to publish a single, clearly-labeled link that allows data subjects to efficiently exercise their opt-out rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	10	
7015(b)(2)	N/A	The icon shall be approximately the same size as other icons used by the business in the header or footer of its webpage.	Functional	Subset Of	Alternative Out-Out Link	PRI-21.2	Mechanisms exist to publish a single, clearly-labeled link that allows data subjects to efficiently exercise their opt-out rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	10	
7015(b)(3)	N/A	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.	Functional	Subset Of	Alternative Out-Out Link	PRI-21.2	Mechanisms exist to publish a single, clearly-labeled link that allows data subjects to efficiently exercise their opt-out rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	10	✓✕
7015(c)	N/A	The Alternative Opt-out Link shall direct the consumer to a webpage that includes the following information:	Functional	Subset Of	Alternative Out-Out Link	PRI-21.2	Mechanisms exist to publish a single, clearly-labeled link that allows data subjects to efficiently exercise their opt-out rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	10	
7015(c)(1)	N/A	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	Functional	Subset Of	Alternative Out-Out Link	PRI-21.2	Mechanisms exist to publish a single, clearly-labeled link that allows data subjects to efficiently exercise their opt-out rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	10	
7015(c)(2)	N/A	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.	Functional	Subset Of	Alternative Out-Out Link	PRI-21.2	Mechanisms exist to publish a single, clearly-labeled link that allows data subjects to efficiently exercise their opt-out rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	10	
7016	Notice of Financial Incentive.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7016(a)	N/A	The purpose of the Notice of Financial Incentive is to explain to the consumer the material terms of a financial incentive or price or service difference the business is offering so that the consumer may make an informed decision about whether to participate. A business that does not offer a financial incentive or price or service difference is not required to provide a Notice of Financial Incentive.	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7016(b)	N/A	The Notice of Financial Incentive shall comply with section 7003, subsections (a) and (b).	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7016(c)	N/A	The Notice of Financial Incentive shall be readily available where consumers will encounter it before opting-in to the financial incentive or price or service difference. If the business offers the financial incentive or price or service difference online, the notice may be given by providing a link that takes the consumer directly to the specific section of a business's privacy policy that contains the information required in subsection (d).	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7016(d)	N/A	A business shall include the following in its Notice of Financial Incentive:	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7016(d)(1)	N/A	A succinct summary of the financial incentive or price or service difference offered;	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7016(d)(2)	N/A	A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data;	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7016(d)(3)	N/A	How the consumer can opt-in to the financial incentive or price or service difference;	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7016(d)(4)	N/A	A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7016(d)(5)	N/A	An explanation of how the price or service difference is reasonably related to the value of the consumer's data, including:	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7016(d)(5)(A)	N/A	A good-faith estimate of the value of the consumer's data that forms the basis for offering the price or service difference; and	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7016(d)(5)(B)	N/A	A description of the method(s) the business used to calculate the value of the consumer's data.	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7020	Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7020(a)	N/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.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
7020(b)	N/A	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.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
7020(c)	N/A	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.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
7020(d)	N/A	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.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
7020(e)	N/A	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).	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
7020(f)	N/A	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:	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7020(f)(1)	N/A	Treat the request as if it had been submitted in accordance with the business's designated manner, or	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
7020(f)(2)	N/A	Provide the consumer with information on how to submit the request or remedy any deficiencies with the request, if applicable.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
7021	Timelines for Responding to Requests to Delete, Requests to Correct, Requests to Know, Requests to Access ADMT, and Requests to Appeal ADMT.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7021(a)	N/A	No later than 10 business days after receiving a request to delete, request to correct, 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.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
7021(b)	N/A	Businesses shall respond to a request to delete, request to correct, 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.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
7022	Requests to Delete.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7022(a)	N/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.	Functional	Subset Of	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	10	
7022(b)	N/A	A business shall comply with a consumer's request to delete their personal information by doing all of the following:	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
7022(b)(1)	N/A	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.	Functional	Intersects With	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	8	
7022(b)(2)	N/A	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.	Functional	Intersects With	Obligation To Inform Third-Parties	PRI-07.3	Mechanisms exist to inform applicable third-parties of any modification, deletion or other change that affects shared Personal Data (PD).	8	
7022(b)(3)	N/A	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.	Functional	Intersects With	Obligation To Inform Third-Parties	PRI-07.3	Mechanisms exist to inform applicable third-parties of any modification, deletion or other change that affects shared Personal Data (PD).	8	
7022(c)	N/A	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:	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
7022(c)(1)	N/A	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.	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
7022(c)(2)	N/A	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.	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
7022(c)(3)	N/A	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.	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
7022(c)(4)	N/A	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.	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
7022(d)	N/A	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.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
7022(d)	N/A	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.	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
7022(e)	N/A	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.	Functional	Intersects With	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected, amended or deleted.	5	
7022(e)	N/A	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.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7022(f)	N/A	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:	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7022(f)(1)	N/A	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.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7022(f)(2)	N/A	Delete the consumer’s personal information that is not subject to the exception.	Functional	Intersects With	Right to Erasure	PRI-06.5	Mechanisms exist to maintain a process to erase a data subject's Personal Data (PD), in accordance with applicable laws, regulations and contractual obligations pertaining to the retention of their PD.	5	
7022(f)(3)	N/A	Not use the consumer’s personal information retained for any other purpose than provided for by that exception; and	Functional	Intersects With	Continued Use of Personal Data (PD)	PRI-03.9	Mechanisms exist to govern the continued use of Personal Data (PD) as it is collected, received, processed, stored, transmitted and/or shared until: (1) Disposal of PD occurs when there is no longer a legitimate business purpose; (2) Disposal of PD occurs when the data retention timeline for the use case is met; and/or (3) Continued use of PD is prohibited upon withdrawal of data subject consent.	5	
7022(f)(4)	N/A	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.	Functional	Intersects With	Obligation To Inform Third-Parties	PRI-07.3	Mechanisms exist to inform applicable third-parties of any modification, deletion or other change that affects shared Personal Data (PD).	5	
7022(g)	N/A	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.	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent.	5	
7022(h)	N/A	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.	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent.	5	
7023	Requests to Correct.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7023(a)	N/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.	Functional	Intersects With	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for: (1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or amendments of PD to other authorized users of the PD.	5	
7023(a)	N/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.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7023(a)	N/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.	Functional	Intersects With	Enabling Data Subjects To Update Personal Data (PD)	PRI-12.1	Mechanisms exist to enable data subjects to update their Personal Data (PD).	5	
7023(b)	N/A	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.	Functional	Intersects With	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for: (1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or amendments of PD to other authorized users of the PD.	5	
7023(b)	N/A	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.	Functional	Intersects With	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	5	
7023(b)	N/A	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.	Functional	Subset Of	Updating Personal Data (PD)	PRI-12	Mechanisms exist to develop processes to identify and record the method under which Personal Data (PD) is updated and the frequency that such updates occur.	10	
7023(b)	N/A	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.	Functional	Intersects With	Enabling Data Subjects To Update Personal Data (PD)	PRI-12.1	Mechanisms exist to enable data subjects to update their Personal Data (PD).	5	
7023(b)(1)	N/A	Considering the totality of the circumstances includes, but is not limited to, considering:	Functional	Subset Of	Updating Personal Data (PD)	PRI-12	Mechanisms exist to develop processes to identify and record the method under which Personal Data (PD) is updated and the frequency that such updates occur.	10	
7023(b)(1)(A)	N/A	The nature of the personal information (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).	Functional	Subset Of	Updating Personal Data (PD)	PRI-12	Mechanisms exist to develop processes to identify and record the method under which Personal Data (PD) is updated and the frequency that such updates occur.	10	
7023(b)(1)(B)	N/A	How the business obtained the contested information.	Functional	Subset Of	Updating Personal Data (PD)	PRI-12	Mechanisms exist to develop processes to identify and record the method under which Personal Data (PD) is updated and the frequency that such updates occur.	10	
7023(b)(1)(C)	N/A	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).	Functional	Subset Of	Updating Personal Data (PD)	PRI-12	Mechanisms exist to develop processes to identify and record the method under which Personal Data (PD) is updated and the frequency that such updates occur.	10	
7023(b)(2)	N/A	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.	Functional	Subset Of	Updating Personal Data (PD)	PRI-12	Mechanisms exist to develop processes to identify and record the method under which Personal Data (PD) is updated and the frequency that such updates occur.	10	
7023(c)	N/A	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:	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
7023(c)	N/A	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:	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7023(c)	N/A	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:	Functional	Intersects With	Obligation To Inform Third-Parties	PRI-07.3	Mechanisms exist to inform applicable third-parties of any modification, deletion or other change that affects shared Personal Data (PD).	5	
7023(c)	N/A	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:	Functional	Intersects With	Data Quality Operations	DCH-22	Mechanisms exist to check for Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data to ensure the accuracy, relevance, timeliness, impact, completeness and de-identification of information throughout the information lifecycle.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7023(c)	N/A	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:	Functional	Intersects With	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	5	
7023(c)	N/A	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:	Functional	Intersects With	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	5	
7023(c)(1)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7023(c)(2)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7023(d)	N/A	Documentation.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7023(d)(1)	N/A	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.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
7023(d)(1)	N/A	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.	Functional	Intersects With	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for: (1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or amendments of PD to other authorized users of the PD.	5	
7023(d)(1)	N/A	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.	Functional	Intersects With	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	5	
7023(d)(2)	N/A	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:	Functional	Intersects With	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for: (1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or amendments of PD to other authorized users of the PD.	5	
7023(d)(2)(A)	N/A	The nature of the personal information at issue (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7023(d)(2)(B)	N/A	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.)	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7023(d)(2)(C)	N/A	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.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7023(d)(2)(D)	N/A	The impact on the consumer. For example, if the personal information has a negative impact on the consumer, the business may require less documentation.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7023(d)(3)	N/A	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.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	8	
7023(d)(4)	N/A	The business shall implement and maintain reasonable security procedures and practices in maintaining any documentation relating to the consumer's request to correct.	Functional	Subset Of	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	10	
7023(e)	N/A	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.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
7023(f)	N/A	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:	Functional	Intersects With	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected, amended or deleted.	5	
7023(f)(1)	N/A	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.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7023(f)(2)	N/A	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.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7023(f)(3)	N/A	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)(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.	Functional	Intersects With	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	5	
7023(f)(3)	N/A	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)(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.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7023(f)(4)	N/A	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.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7023(g)	N/A	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.	Functional	Intersects With	Justification To Reject Disclosure Requests	PRI-07.5	Mechanisms exist to reject data subject access requests that are categorized as: (1) Harassing; (2) Repetitive; or (3) Fraudulent.	5	
7023(h)	N/A	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.	Functional	Subset Of	Justification To Reject Disclosure Requests	PRI-07.5	Mechanisms exist to reject data subject access requests that are categorized as: (1) Harassing; (2) Repetitive; or (3) Fraudulent.	10	
7023(i)	N/A	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 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.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7023(j)	N/A	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 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.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7023(k)	N/A	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 supplements personal information it maintains about consumers with information obtained from a data broker, failing to consider and address the possibility that corrected information may be overridden by inaccurate information subsequently received from a data broker factors into whether that business, service provider, or contractor has adequately complied with a consumer's request to correct.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7024	Requests to Know.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7024(a)	N/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).	Functional	Intersects With	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	8	
7024(b)	N/A	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.	Functional	Intersects With	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	8	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7024(c)	N/A	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:	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7024(c)(1)	N/A	The business does not maintain the personal information in a searchable or reasonably accessible format.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7024(c)(2)	N/A	The business maintains the personal information solely for legal or compliance purposes.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7024(c)(3)	N/A	The business does not sell the personal information and does not use it for any commercial purpose.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7024(c)(4)	N/A	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.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7024(d)	N/A	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 business shall:	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7024(d)(1)	N/A	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	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7024(d)(2)	N/A	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.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7024(e)	N/A	If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, the business shall do all of the following:	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
7024(e)(1)	N/A	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	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
7024(e)(2)	N/A	Disclose the consumer's personal information that is not subject to the exception.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
7024(f)	N/A	A business shall use reasonable security measures when transmitting personal information to the consumer.	Functional	Subset Of	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	10	
7024(g)	N/A	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.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	8	
7024(g)	N/A	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.	Functional	Intersects With	Data Portability	PRI-06.6	Mechanisms exist to format exports of Personal Data (PD) in a structured, machine-readable format that allows data subjects to transfer their PD to another controller without hindrance.	3	
7024(g)	N/A	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.	Functional	Intersects With	Personal Data (PD) Exports	PRI-06.7	Mechanisms exist to export a data subject's available Personal Data (PD) in a readily usable format, upon an authenticated request.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7024(g)	N/A	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.	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-06	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	8	
7024(h)	N/A	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.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
7024(i)	N/A	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.	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
7024(j)	N/A	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.	Functional	Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	5	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7024(j)	N/A	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.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7024(k)	N/A	In responding to a verified request to know categories of personal information, the business shall provide all of the following:	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
7024(k)(1)	N/A	The categories of personal information the business has collected about the consumer.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
7024(k)(2)	N/A	The categories of sources from which the personal information was collected.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
7024(k)(3)	N/A	The business or commercial purpose for which it collected, sold, or shared the personal information.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
7024(k)(4)	N/A	The categories of third parties with whom the business discloses personal information.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
7024(k)(5)	N/A	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.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
7024(k)(6)	N/A	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 to whom it disclosed that particular category of personal information.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
7024(l)	N/A	A business shall identify the categories of personal information, categories of sources of personal information, categories of third parties to whom a business sold or shared 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.	Functional	Intersects With	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).	8	
7024(l)	N/A	A business shall identify the categories of personal information, categories of sources of personal information, categories of third parties to whom a business sold or shared 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.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	8	
7024(l)	N/A	A business shall identify the categories of personal information, categories of sources of personal information, categories of third parties to whom a business sold or shared 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.	Functional	Intersects With	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
7025	Opt-out Preference Signals.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7025(a)	N/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.	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
7025(b)	N/A	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:	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
7025(b)(1)	N/A	The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field or JavaScript object.	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
7025(b)(2)	N/A	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.	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
7025(c)	N/A	When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b):	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
7025(c)(1)	N/A	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.	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
7025(c)(2)	N/A	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.	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7025(c)(3)	N/A	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).	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
7025(c)(4)	N/A	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).	Functional	Intersects With	Active Participation By Data Subjects	PRI-03.7	Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.).	8	
7025(c)(5)	N/A	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.	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent	5	
7025(c)(5)	N/A	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.	Functional	Intersects With	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	5	
7025(c)(6)	N/A	A business 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 Honored" when a browser, device, or consumer using an opt-out preference signal visits the website, 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).	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
7025(c)(7)	N/A	Illustrative examples follow.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7025(c)(7)(A)	N/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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7025(c)(7)(B)	N/A	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).	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7025(c)(7)(C)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7025(c)(7)(D)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7025(c)(7)(E)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7025(d)	N/A	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.	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
7025(e)	N/A	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.	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
7025(f)	N/A	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:	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
7025(f)(1)	N/A	Charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal.	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
7025(f)(2)	N/A	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.	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
7025(f)(3)	N/A	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) – (3).	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
7025(g)	N/A	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:	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
7025(g)(1)	N/A	Processes the opt-out preference signal in a frictionless manner in accordance with the CCPA and these regulations.	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7025(g)(2)	N/A	Includes in its privacy policy the following information:	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7025(g)(2)(A)	N/A	A description of the consumer's right to opt-out of the sale or sharing of their personal information by the business;	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7025(g)(2)(B)	N/A	A statement that the business processes opt-out preference signals in a frictionless manner;	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7025(g)(2)(C)	N/A	Information on how consumers can implement opt-out preference signals for the business to process in frictionless manner; and	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7025(g)(2)(D)	N/A	Instructions for any other method by which the consumer may submit a request to opt-out of sale/sharing.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
7025(g)(3)	N/A	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.	Functional	Subset Of	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).	10	
7025(g)(3)(A)	N/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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7025(g)(3)(B)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7026	Requests to Opt-out of Sale/Sharing.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7026(a)	N/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.	Functional	Intersects With	Notice of Right To Opt-Out	PRI-21	Mechanisms exist to include within the data privacy notice a notification to data subjects of: (1) Their right to direct an organization that sells or shares their Personal Data (PD) to stop selling or sharing their PD; and (2) The methods available to exercise that right.	5	
7026(a)	N/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.	Functional	Intersects With	Opt-Out Links	PRI-21.1	Mechanisms exist to publish conspicuous links for data subjects to exercise their rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	5	
7026(a)(1)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7026(a)(2)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7026(a)(3)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7026(a)(4)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7026(b)	N/A	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.	Functional	Intersects With	Opt-Out Links	PRI-21.1	Mechanisms exist to publish conspicuous links for data subjects to exercise their rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7026(c)	N/A	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.	Functional	Intersects With	Opt-Out Links	PRI-21.1	Mechanisms exist to publish conspicuous links for data subjects to exercise their rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	5	
7026(d)	N/A	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.	Functional	Intersects With	Opt-Out Links	PRI-21.1	Mechanisms exist to publish conspicuous links for data subjects to exercise their rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	5	
7026(e)	N/A	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.	Functional	Intersects With	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	3	
7026(f)	N/A	A business shall comply with a request to opt-out of sale/sharing by:	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
7026(f)(1)	N/A	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.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
7026(f)(2)	N/A	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.	Functional	Intersects With	Obligation To Inform Third-Parties	PRI-07.3	Mechanisms exist to inform applicable third-parties of any modification, deletion or other change that affects shared Personal Data (PD).	5	
7026(f)(3)	N/A	Illustrative examples follow.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7026(f)(3)(A)	N/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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7026(f)(3)(B)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7026(g)	N/A	A business 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" in accordance with section 7025, subsection (b)(6), and 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.	Functional	Intersects With	Opt-Out Links	PRI-21.1	Mechanisms exist to publish conspicuous links for data subjects to exercise their rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	5	
7026(h)	N/A	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).	Functional	Intersects With	Opt-Out Links	PRI-21.1	Mechanisms exist to publish conspicuous links for data subjects to exercise their rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	5	
7026(i)	N/A	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).	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7026(j)	N/A	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.	Functional	Intersects With	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	5	
7026(k)	N/A	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.	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent.	5	
7027	Requests to Limit Use and Disclosure of Sensitive Personal Information.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7027(a)	N/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.	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
7027(b)	N/A	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.	Functional	Intersects With	Active Participation By Data Subjects	PRI-03.7	Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.).	3	
7027(b)	N/A	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.	Functional	Intersects With	Continued Use of Personal Data (PD)	PRI-03.9	Mechanisms exist to govern the continued use of Personal Data (PD) as it is collected, received, processed, stored, transmitted and/or shared until: (1) Disposal of PD occurs when there is no longer a legitimate business purpose; (2) Disposal of PD occurs when the data retention timeline for the use case is met; and/or (3) Continued use of PD is prohibited upon withdrawal of data subject consent.	3	
7027(b)(1)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7027(b)(2)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7027(b)(3)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7027(b)(4)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7027(c)	N/A	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.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7027(d)	N/A	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.	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
7027(d)	N/A	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.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
7027(e)	N/A	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 applies. However, to the extent that the business can comply with a request to limit without additional information, it shall do so.	Functional	Intersects With	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
7027(e)	N/A	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 applies. However, to the extent that the business can comply with a request to limit without additional information, it shall do so.	Functional	Intersects With	Strong Customer Authentication (SCA)	WEB-06	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.	3	
7027(f)	N/A	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.	Functional	Intersects With	Justification To Reject Disclosure Requests	PRI-07.5	Mechanisms exist to reject data subject access requests that are categorized as: (1) Harassing; (2) Repetitive; or (3) Fraudulent.	5	
7027(g)	N/A	A business shall comply with a request to limit by:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7027(g)(1)	N/A	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.	Functional	Intersects With	Continued Use of Personal Data (PD)	PRI-03.9	Mechanisms exist to govern the continued use of Personal Data (PD) as it is collected, received, processed, stored, transmitted and/or shared until: (1) Disposal of PD occurs when there is no longer a legitimate business purpose; (2) Disposal of PD occurs when the data retention timeline for the use case is met; and/or (3) Continued use of PD is prohibited upon withdrawal of data subject consent.	5	
7027(g)(1)	N/A	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.	Functional	Intersects With	Cease Processing, Storing and/or Sharing Personal Data (PD)	PRI-03.10	Mechanisms exist to ensure the organization ceases collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) upon receiving a data subject's consent revocation.	5	
7027(g)(2)	N/A	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.	Functional	Intersects With	Obligation To Inform Third-Parties	PRI-07.3	Mechanisms exist to inform applicable third-parties of any modification, deletion or other change that affects shared Personal Data (PD).	5	
7027(g)(3)	N/A	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 the sensitive personal information during that time period.	Functional	Intersects With	Obligation To Inform Third-Parties	PRI-07.3	Mechanisms exist to inform applicable third-parties of any modification, deletion or other change that affects shared Personal Data (PD).	5	
7027(h)	N/A	A business 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.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	5	
7027(i)	N/A	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.	Functional	Intersects With	Active Participation By Data Subjects	PRI-03.7	Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.).	5	
7027(j)	N/A	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.	Functional	Intersects With	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	5	
7027(j)	N/A	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.	Functional	Intersects With	Justification To Reject Disclosure Requests	PRI-07.5	Mechanisms exist to reject data subject access requests that are categorized as: (1) Harassing; (2) Repetitive; or (3) Fraudulent.	3	
7027(k)	N/A	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.	Functional	Intersects With	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	3	
7027(k)	N/A	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.	Functional	Intersects With	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	3	
7027(l)	N/A	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).	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent.	5	
7027(m)	N/A	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.	Functional	Intersects With	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	3	
7027(m)	N/A	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.	Functional	Intersects With	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	3	
7027(m)	N/A	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.	Functional	Subset Of	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	
7027(m)(1)	N/A	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.	Functional	Subset Of	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7027(m)(2)	N/A	To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information. Illustrative examples follow.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery	5	
7027(m)(2)	N/A	To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information. Illustrative examples follow.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
7027(m)(2)(A)	N/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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7027(m)(2)(B)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7027(m)(3)	N/A	To resist malicious, deceptive, fraudulent, or illegal actions directed at the business or at consumers, or to prosecute those responsible for those actions. Illustrative examples follow.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
7027(m)(3)(A)	N/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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7027(m)(3)(B)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7027(m)(4)	N/A	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.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
7027(m)(5)	N/A	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.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
7027(m)(6)	N/A	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.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
7027(m)(7)	N/A	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.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
7027(m)(8)	N/A	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.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	5	
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.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.

7028(a)	N/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.	Functional	Intersects With	Data Subject Opt-In Consent	PRI-03.12	Mechanisms exist to obtain consent from data subjects to opt-in for the following Personal Data (PD) actions:
							(1) Collecting;
							(2) Receiving;
							(3) Processing;
							(4) Storing;
							(5) Transmitting:
							(6) Sharing; and/or
							(7) Updating
								5	

7028(b)	N/A	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.	Functional	Intersects With	Data Subject Opt-In Consent	PRI-03.12	Mechanisms exist to obtain consent from data subjects to opt-in for the following Personal Data (PD) actions:
							(1) Collecting;
							(2) Receiving;
							(3) Processing;
							(4) Storing;
							(5) Transmitting:
							(6) Sharing; and/or
							(7) Updating
								5	

7028(c)	N/A	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.	Functional	Intersects With	Data Subject Opt-In Consent	PRI-03.12	Mechanisms exist to obtain consent from data subjects to opt-in for the following Personal Data (PD) actions:
							(1) Collecting;
							(2) Receiving;
							(3) Processing;
							(4) Storing;
							(5) Transmitting:
							(6) Sharing; and/or
							(7) Updating
								5	

7050	Service Providers and Contractors.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7050(a)	N/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.	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
7050(a)(1)	N/A	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.	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
7050(a)(2)	N/A	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.	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
7050(a)(3)	N/A	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.	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
7050(a)(3)(A)	N/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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7050(a)(3)(B)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7050(a)(4)	N/A	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.	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
7050(a)(5)	N/A	For the purposes enumerated in Civil Code section 1798.145, subdivisions (a)(1).	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7050(b)	N/A	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.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7050(b)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7050(b)(1)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7050(b)(2)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7050(c)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7050(d)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7050(e)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7050(f)	N/A	A service provider or a contractor shall comply with the terms of the contract required by the CCPA and these regulations.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7050(g)	N/A	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).	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7050(h)	N/A	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:	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7050(h)(1)	N/A	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	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7050(h)(2)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7051	Contract Requirements for Service Providers and Contractors.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7051(a)	N/A	The contract required by the CCPA for service providers and contractors shall:	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
7051(a)	N/A	The contract required by the CCPA for service providers and contractors shall:	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
7051(a)(1)	N/A	Prohibit the service provider or contractor from selling or sharing personal information it collects pursuant to the written contract with the business.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7051(a)(2)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7051(a)(3)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7051(a)(4)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7051(a)(5)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7051(a)(6)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7051(a)(7)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7051(a)(8)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7051(a)(9)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
7051(b)	N/A	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).	Functional	Subset Of	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	10	
7051(c)	N/A	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, 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.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	5	In the example, this is a case of "due care" and not "due diligence" practices. Once the contract is in place, it is a matter of due care to enforce the terms of the contract.
7052	Third Parties.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7052(a)	N/A	A third party that does not have a contract that complies with section 7053, subsection (a), shall not collect, use, process, retain, sell, or share the personal information that the business made available to it.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
7052(a)	N/A	A third party that does not have a contract that complies with section 7053, subsection (a), shall not collect, use, process, retain, sell, or share the personal information that the business made available to it.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7052(b)	N/A	A third party shall comply with the terms of the contract required by the CCPA and these regulations, which include treating the personal information that the business made available to it in a manner consistent with the business's obligations under the CCPA and these regulations.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
7052(b)	N/A	A third party shall comply with the terms of the contract required by the CCPA and these regulations, which include treating the personal information that the business made available to it in a manner consistent with the business's obligations under the CCPA and these regulations.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	8	
7053	Contract Requirements for Third Parties.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7053(a)	N/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:	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
7053(a)	N/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:	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	8	
7053(a)(1)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	8	
7053(a)(2)	N/A	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).	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	8	
7053(a)(3)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	8	
7053(a)(4)	N/A	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.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	8	
7053(a)(5)	N/A	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.	Functional	Intersects With	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data protection controls.	5	
7053(a)(5)	N/A	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.	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
7053(a)(6)	N/A	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.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
7053(b)	N/A	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, 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.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	5	In the example, this is a case of "due care" and not "due diligence" practices. Once the contract is in place, it is a matter of due care to enforce the terms of the contract.
7060	General Rules Regarding Verification.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7060(a)	N/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, request to know, or request to access ADMT is the consumer about whom the business has collected information.	Functional	Intersects With	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	8	
7060(b)	N/A	A business shall not require a consumer to verify their identity to make a request to opt-out of sale/sharing, 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.	Functional	Intersects With	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	5	
7060(b)	N/A	A business shall not require a consumer to verify their identity to make a request to opt-out of sale/sharing, 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.	Functional	Intersects With	Opt-Out Links	PRI-21.1	Mechanisms exist to publish conspicuous links for data subjects to exercise their rights to: (1) Limit the collection and/or use of Personal Data (PD); and (2) Not sell or share PD.	5	
7060(c)	N/A	In determining the method by which the business will verify the consumer's identity, the business shall:	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7060(c)(1)	N/A	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.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7060(c)(2)	N/A	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.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7060(c)(3)	N/A	Consider the following factors:	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7060(c)(3)(A)	N/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.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7060(c)(3)(B)	N/A	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.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7060(c)(3)(C)	N/A	The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7060(c)(3)(D)	N/A	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.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7060(c)(3)(E)	N/A	The manner in which the business interacts with the consumer.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7060(c)(3)(F)	N/A	Available technology for verification.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7060(d)	N/A	A business shall 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.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7060(e)	N/A	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 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.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7060(f)	N/A	A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized deletion, correction, or access to a consumer's personal information, or access to information about a business's use of ADMT with respect to a consumer.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7060(g)	N/A	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.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7060(h)	N/A	For requests to correct, the business must 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.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7061	Verification for Password-Protected Accounts.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7061(a)	N/A	If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 7060. The business shall also require a consumer to re-authenticate themselves before deleting, correcting, or disclosing the consumer's data.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7061(b)	N/A	If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to delete, request to correct, or request to know until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 7062 to further verify the identity of the consumer.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7062	N/A	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7062(a)	N/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.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7062(b)	N/A	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.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7062(c)	N/A	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.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7062(d)	N/A	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.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7062(e)	N/A	Illustrative examples follow:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7062(e)(1)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7062(e)(2)	N/A	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 (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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7062(f)	N/A	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.	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	
7062(g)	N/A	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).	Functional	Subset Of	Data Subject Authentication	PRI-06.8	Mechanisms exist to utilize reasonable consumer expectations to verify a data subject's identity, prior to taking action to disclose, share, correct, amend and/or delete Personal Data (PD).	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7063	Authorized Agents.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7063(a)	N/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: Bottom section: However, businesses shall not require the consumer to resubmit their request in their individual capacity.	Functional	Subset Of	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	10	
7063(a)(1)	N/A	Verify their own identity directly with the business.	Functional	Subset Of	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	10	
7063(a)(2)	N/A	Directly confirm with the business that they provided the authorized agent permission to submit the request.	Functional	Subset Of	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	10	
7063(b)	N/A	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.	Functional	Subset Of	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	10	
7063(c)	N/A	An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information.	Functional	Subset Of	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	10	
7063(d)	N/A	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.	Functional	Subset Of	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	10	
7070	Consumers Less Than 13 Years of Age.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7070(a)	N/A	Process for Opting-In to Sale or Sharing of Personal Information	Functional	Subset Of	Parent or Guardian Opt-In Consent For Minors	PRI-03.13	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	10	
7070(a)(1)	N/A	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.	Functional	Subset Of	Parent or Guardian Opt-In Consent For Minors	PRI-03.13	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	10	
7070(a)(2)	N/A	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:	Functional	Subset Of	Parent or Guardian Opt-In Consent For Minors	PRI-03.13	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	10	
7070(a)(2)(A)	N/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;	Functional	Subset Of	Parent or Guardian Opt-In Consent For Minors	PRI-03.13	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	10	
7070(a)(2)(B)	N/A	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;	Functional	Subset Of	Parent or Guardian Opt-In Consent For Minors	PRI-03.13	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	10	
7070(a)(2)(C)	N/A	Having a parent or guardian call a toll-free telephone number staffed by trained personnel;	Functional	Subset Of	Parent or Guardian Opt-In Consent For Minors	PRI-03.13	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	10	
7070(a)(2)(D)	N/A	Having a parent or guardian connect to trained personnel via video-conference;	Functional	Subset Of	Parent or Guardian Opt-In Consent For Minors	PRI-03.13	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	10	
7070(a)(2)(E)	N/A	Having a parent or guardian communicate in person with trained personnel; and	Functional	Subset Of	Parent or Guardian Opt-In Consent For Minors	PRI-03.13	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	10	
7070(a)(2)(F)	N/A	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.	Functional	Subset Of	Parent or Guardian Opt-In Consent For Minors	PRI-03.13	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	10	
7070(b)	N/A	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).	Functional	Subset Of	Parent or Guardian Opt-In Consent For Minors	PRI-03.13	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	10	
7070(c)	N/A	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.	Functional	Subset Of	Parent or Guardian Opt-In Consent For Minors	PRI-03.13	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	10	
7071	Consumers at Least 13 Years of Age and Less Than 16 Years of Age.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7071(a)	N/A	A business that has actual knowledge that it sells or shares the personal information of consumers at least 13 years of age and less than 16 years of age shall establish, document, and comply with a reasonable process for allowing such consumers to opt-in to the sale or sharing of their personal information, pursuant to section 7028.	Functional	Intersects With	Parent or Guardian Opt-In Consent For Minors	PRI-03.13	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	5	
7071(b)	N/A	When a business receives a request to opt-in to the sale or sharing of personal information from a consumer at least 13 years of age and less than 16 years of age, the business shall inform the consumer of their ongoing right to opt-out of sale/sharing at any point in the future and of the process for doing so pursuant to section 7026.	Functional	Intersects With	Parent or Guardian Opt-In Consent For Minors	PRI-03.13	Mechanisms exist to obtain parental or guardian consent for Personal Data (PD) processing actions through reasonable consumer expectations, when the data subject is a minor.	5	
7072	Notices to Consumers Less Than 16 Years of Age.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7072(a)	N/A	A business subject to sections 7070 and/or 7071 shall include a description of the processes set forth in those sections in its privacy policy.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7072(b)	N/A	A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell or share the personal information without the consent of consumers at least 13 years of age and less than 16 years of age, or the consent of their parent or guardian for consumers under 13 years of age, is not required to provide the Notice of Right to Opt-out of Sale/Sharing.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
7080	Discriminatory Practices.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7080(a)	N/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.	Functional	Subset Of	Product or Service Delivery Restrictions	PRI-03.5	Mechanisms exist to prevent discrimination against a data subject for exercising their legal rights pertaining to modifying or revoking consent, including prohibiting: (1) Refusing products and/or services; (2) Charging different rates for goods and/or services; and (3) Providing different levels of quality.	10	
7080(b)	N/A	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.	Functional	Subset Of	Product or Service Delivery Restrictions	PRI-03.5	Mechanisms exist to prevent discrimination against a data subject for exercising their legal rights pertaining to modifying or revoking consent, including prohibiting: (1) Refusing products and/or services; (2) Charging different rates for goods and/or services; and (3) Providing different levels of quality.	10	
7080(c)	N/A	A business's denial of a consumer's request to delete, request to correct, request to know, request to access ADMT, 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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7080(d)	N/A	Illustrative examples follow:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7080(d)(1)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7080(d)(2)	N/A	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).	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7080(d)(3)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7080(d)(4)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7080(e)	N/A	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.	Functional	Subset Of	Notice of Financial Incentive	PRI-17.2	Mechanisms exist to provide data subjects with a Notice of Financial Incentive that explains the material terms of a financial incentive, price or service difference so the data subject can make an informed decision about whether to participate.	10	
7080(f)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7080(g)	N/A	A price or service difference that is the direct result of compliance with a state or federal law shall not be considered discriminatory.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7081	Calculating the Value of Consumer Data.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7081(a)	N/A	A business offering a price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good-faith method for calculating the value of the consumer's data. The business shall consider one or more of the following:	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7081(a)(1)	N/A	The marginal value to the business of the sale, collection, or deletion of a consumer's data.	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7081(a)(2)	N/A	The average value to the business of the sale, collection, or deletion of a consumer's data.	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7081(a)(3)	N/A	The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers.	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7081(a)(4)	N/A	Revenue generated by the business from sale, collection, or retention of consumers' personal information.	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7081(a)(5)	N/A	Expenses related to the sale, collection, or retention of consumers' personal information.	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7081(a)(6)	N/A	Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference.	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7081(a)(7)	N/A	Profit generated by the business from sale, collection, or retention of consumers' personal information.	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7081(a)(8)	N/A	Any other practical and reasonably reliable method of calculation used in good faith.	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7081(b)	N/A	For the purpose of calculating the value of consumer data, a business may consider the value to the business of the data of all natural persons in the United States and not just consumers.	Functional	Subset Of	Financial Incentives For Personal Data (PD)	PRI-01.10	Mechanisms exist to strictly govern financial incentives offered to data subjects for Personal Data (PD) to ensure compliance with applicable legal and regulatory requirements.	10	
7100	Training.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7100(a)	N/A	All individuals responsible for handling consumer inquiries about the business's information practices or the business's compliance with the CCPA shall be informed of all of the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.	Functional	Subset Of	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	
7100(a)	N/A	All individuals responsible for handling consumer inquiries about the business's information practices or the business's compliance with the CCPA shall be informed of all of the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.	Functional	Intersects With	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8	
7100(a)	N/A	All individuals responsible for handling consumer inquiries about the business's information practices or the business's compliance with the CCPA shall be informed of all of the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	8	
7100(b)	N/A	A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity and data protection-specific business plan and set of objectives to achieve that plan.	8	
7100(b)	N/A	A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.	Functional	Intersects With	Cybersecurity & Data Protection Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	8	
7101	Record-Keeping.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7101(a)	N/A	A business shall maintain records of consumer requests made pursuant to the CCPA and how it responded to the requests for at least 24 months. The business shall implement and maintain reasonable security procedures and practices in maintaining these records.	Functional	Subset Of	Data Subject Communications Documentation	PRI-17.3	Mechanisms exist to maintain records of data subject requests and responses in accordance with an established documentation retention schedule that adheres to applicable statutory, regulatory and/or contractual obligations.	10	
7101(b)	N/A	The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.	Functional	Subset Of	Data Subject Communications Documentation	PRI-17.3	Mechanisms exist to maintain records of data subject requests and responses in accordance with an established documentation retention schedule that adheres to applicable statutory, regulatory and/or contractual obligations.	10	
7101(c)	N/A	A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.	Functional	Subset Of	Data Subject Communications Documentation	PRI-17.3	Mechanisms exist to maintain records of data subject requests and responses in accordance with an established documentation retention schedule that adheres to applicable statutory, regulatory and/or contractual obligations.	10	
7101(d)	N/A	Information maintained for record-keeping purposes shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and these regulations. Information maintained for record-keeping purposes shall not be shared with any third party except as necessary to comply with a legal obligation.	Functional	Subset Of	Data Subject Communications Documentation	PRI-17.3	Mechanisms exist to maintain records of data subject requests and responses in accordance with an established documentation retention schedule that adheres to applicable statutory, regulatory and/or contractual obligations.	10	
7101(e)	N/A	Other than as required by subsection (b), a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.	Functional	Subset Of	Data Subject Communications Documentation	PRI-17.3	Mechanisms exist to maintain records of data subject requests and responses in accordance with an established documentation retention schedule that adheres to applicable statutory, regulatory and/or contractual obligations.	10	
7102	Requirements for Businesses Collecting Large Amounts of Personal Information.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7102(a)	N/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:	Functional	Intersects With	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity and data protection-specific business plan and set of objectives to achieve that plan.	8	
7102(a)(1)	N/A	Compile the following metrics for the previous calendar year:	Functional	Subset Of	Data Subject Communications Metrics	PRI-17.4	Mechanisms exist to collect metrics associated with data subject requests and responses.	10	
7102(a)(1)(A)	N/A	The number of requests to delete that the business received, complied with in whole or in part, and denied;	Functional	Subset Of	Data Subject Communications Metrics	PRI-17.4	Mechanisms exist to collect metrics associated with data subject requests and responses.	10	
7102(a)(1)(B)	N/A	The number of requests to correct that the business received, complied with in whole or in part, and denied;	Functional	Subset Of	Data Subject Communications Metrics	PRI-17.4	Mechanisms exist to collect metrics associated with data subject requests and responses.	10	
7102(a)(1)(C)	N/A	The number of requests to know that the business received, complied with in whole or in part, and denied;	Functional	Subset Of	Data Subject Communications Metrics	PRI-17.4	Mechanisms exist to collect metrics associated with data subject requests and responses.	10	
7102(a)(1)(D)	N/A	The number of requests to access ADMT that the business received, complied with in whole or in part, and denied;	Functional	Subset Of	Data Subject Communications Metrics	PRI-17.4	Mechanisms exist to collect metrics associated with data subject requests and responses.	10	
7102(a)(1)(E)	N/A	The number of requests to opt-out of sale/sharing that the business received, complied with in whole or in part, and denied;	Functional	Subset Of	Data Subject Communications Metrics	PRI-17.4	Mechanisms exist to collect metrics associated with data subject requests and responses.	10	
7102(a)(1)(F)	N/A	The number of requests to limit that the business received, complied with in whole or in part, and denied;	Functional	Subset Of	Data Subject Communications Metrics	PRI-17.4	Mechanisms exist to collect metrics associated with data subject requests and responses.	10	
7102(a)(1)(G)	N/A	The number of requests to opt-out of ADMT that the business received, complied with in whole or in part, and denied; and	Functional	Subset Of	Data Subject Communications Metrics	PRI-17.4	Mechanisms exist to collect metrics associated with data subject requests and responses.	10	
7102(a)(1)(H)	N/A	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.	Functional	Subset Of	Data Subject Communications Metrics	PRI-17.4	Mechanisms exist to collect metrics associated with data subject requests and responses.	10	
7102(a)(2)	N/A	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.	Functional	Subset Of	Data Subject Communications Disclosure	PRI-17.5	Mechanisms exist to publicly disclose applicable data subject communications metrics, as required by statutory and/or regulatory obligations.	10	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7102(b)	N/A	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.	Functional	Subset Of	Data Subject Communications Disclosure	PRI-17.5	Mechanisms exist to publicly disclose applicable data subject communications metrics, as required by statutory and/or regulatory obligations.	10	
7120	Requirement to Complete a Cybersecurity Audit.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7120(a)	N/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.	Functional	Subset Of	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements.	10	
7120(b)	N/A	A business's processing of consumers' personal information presents significant risk to consumers' security if any of the following is true:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7120(b)(1)	N/A	The business meets the threshold set forth in Civil Code section 1798.140, subdivision (d)(1)(C), in the preceding calendar year; or	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7120(b)(2)	N/A	The business meets the threshold set forth in Civil Code section 1798.140, subdivision (d)(1)(A); and	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7120(b)(2)(A)	N/A	Processed the personal information of 250,000 or more consumers or households in the preceding calendar year; or	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7120(b)(2)(B)	N/A	Processed the sensitive personal information of 50,000 or more consumers in the preceding calendar year.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7121	Timing Requirements for Cybersecurity Audits and Audit Reports.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7121(a)	N/A	A business must complete its first cybersecurity audit report no later than:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7121(a)(1)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7121(a)(2)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7121(a)(3)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7121(b)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7122	Thoroughness and Independence of Cybersecurity Audits.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7122(a)	N/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.	Functional	Subset Of	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	10	
7122(a)(1)	N/A	To be qualified, an auditor must have knowledge of cybersecurity and how to audit a business's cybersecurity program.	Functional	Subset Of	Assessment Team Subject Matter Expertise	CPL-01.6	Mechanisms exist to ensure individuals performing audits and/or assessments have reasonable: (1) Professional qualifications to perform the audit and/or assessment; and (2) Subject matter expertise to perform review, interview and test activities for in-scope People, Processes, Technologies, Data and/or Facilities (PPTDF).	10	
7122(a)(2)	N/A	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.	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate cybersecurity and data protection controls at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	8	
7122(a)(3)	N/A	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.	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	8	
7122(a)(3)	N/A	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.	Functional	Subset Of	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7122(b)	N/A	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.	Functional	Subset Of	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	10	
7122(b)	N/A	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.	Functional	Intersects With	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersecurity and data protection policies, standards and other applicable requirements.	8	
7122(c)	N/A	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.	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-01.3	Mechanisms exist to ensure the organization is able to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	8	
7122(c)	N/A	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.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	8	
7122(d)	N/A	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.	Functional	Subset Of	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	10	
7122(d)	N/A	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.	Functional	Intersects With	Assessment Team Subject Matter Expertise	CPL-01.6	Mechanisms exist to ensure individuals performing audits and/or assessments have reasonable: (1) Professional qualifications to perform the audit and/or assessment; and (2) Subject matter expertise to perform review, interview and test activities for in-scope People, Processes, Technologies, Data and/or Facilities (PPTDF).	8	
7122(e)	N/A	The cybersecurity audit report must include the information set forth in section 7123, subsection (e).	Functional	Subset Of	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	10	
7122(f)	N/A	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.	Functional	Subset Of	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	10	
7122(f)	N/A	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.	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	8	
7122(g)	N/A	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.	Functional	Subset Of	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	10	
7123	Scope of Cybersecurity Audit and Audit Report.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7123(a)	N/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.	Functional	Subset Of	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	10	
7123(b)	N/A	The cybersecurity audit must assess:	Functional	Subset Of	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	10	
7123(b)(1)	N/A	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	Functional	Intersects With	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	5	
7123(b)(1)	N/A	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	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	
7123(b)(2)	N/A	Each of the components of a cybersecurity program listed in subsection (c) that the auditor deems applicable to the business's information system.	Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	8	
7123(b)(2)	N/A	Each of the components of a cybersecurity program listed in subsection (c) that the auditor deems applicable to the business's information system.	Functional	Subset Of	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	10	
7123(b)(3)	N/A	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).	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program.	5	
7123(b)(3)	N/A	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).	Functional	Intersects With	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
7123(b)(3)	N/A	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).	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
7123(b)(3)	N/A	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).	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
7123(b)(3)	N/A	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).	Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
7123(b)(3)	N/A	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).	Functional	Intersects With	Ability To Demonstrate Conformity	CPL-01.3	Mechanisms exist to ensure the organization is able to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	5	
7123(c)	N/A	The cybersecurity audit must assess the following components, if applicable:	Functional	Subset Of	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	10	
7123(c)(1)	N/A	Authentication, including:	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
7123(c)(1)(A)	N/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	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	8	
7123(c)(1)(B)	N/A	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).	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
7123(c)(1)(B)	N/A	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).	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	8	
7123(c)(1)(B)	N/A	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).	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	8	
7123(c)(1)(B)	N/A	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).	Functional	Intersects With	Passkeys	IAC-10.14	Mechanisms exist to utilize passkeys, or equivalent cryptographic key pairing technologies, to authenticate users to Technology Assets, Applications and/or Services (TAAS).	3	
7123(c)(2)	N/A	Encryption of personal information, at rest and in transit.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
7123(c)(2)	N/A	Encryption of personal information, at rest and in transit.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
7123(c)(2)	N/A	Encryption of personal information, at rest and in transit.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
7123(c)(3)	N/A	Account management and access controls, including:	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
7123(c)(3)	N/A	Account management and access controls, including:	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
7123(c)(3)(A)	N/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:	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
7123(c)(3)(A)	N/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:	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	8	
7123(c)(3)(A)(i)	N/A	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;	Functional	Intersects With	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	8	
7123(c)(3)(A)(i)	N/A	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;	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	8	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7123(c)(3)(A)(i)	N/A	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;	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	8	
7123(c)(3)(A)(ii)	N/A	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	Functional	Intersects With	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	5	
7123(c)(3)(A)(ii)	N/A	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	Functional	Intersects With	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	5	
7123(c)(3)(A)(ii)	N/A	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	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
7123(c)(3)(A)(ii)	N/A	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	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
7123(c)(3)(A)(ii)	N/A	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	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	
7123(c)(3)(A)(iii)	N/A	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.	Functional	Intersects With	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	5	
7123(c)(3)(A)(iii)	N/A	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.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
7123(c)(3)(A)(iii)	N/A	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.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
7123(c)(3)(A)(iii)	N/A	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.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
7123(c)(3)(B)	N/A	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).	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
7123(c)(3)(B)	N/A	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).	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
7123(c)(3)(B)	N/A	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).	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
7123(c)(3)(B)	N/A	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).	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	8	
7123(c)(3)(B)	N/A	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).	Functional	Intersects With	Management Approval For Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.	5	
7123(c)(3)(C)	N/A	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).	Functional	Intersects With	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	8	
7123(c)(3)(C)	N/A	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).	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
7123(c)(3)(C)	N/A	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).	Functional	Intersects With	Management Approval For Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.	5	
7123(c)(3)(C)	N/A	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).	Functional	Intersects With	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5	
7123(c)(3)(D)	N/A	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).	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
7123(c)(3)(D)	N/A	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).	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
7123(c)(3)(D)	N/A	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).	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	8	
7123(c)(3)(D)	N/A	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).	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	8	
7123(c)(3)(D)	N/A	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).	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	3	
7123(c)(3)(D)	N/A	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).	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	3	
7123(c)(3)(D)	N/A	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).	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	8	
7123(c)(3)(D)	N/A	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).	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	3	
7123(c)(4)	N/A	Inventory and management of personal information and the business's information system, including:	Functional	Subset Of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	10	
7123(c)(4)(A)	N/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);	Functional	Intersects With	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive/regulated data is stored, transmitted or processed.	5	
7123(c)(4)(A)	N/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);	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	8	
7123(c)(4)(A)	N/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);	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity and data protection control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	3	
7123(c)(4)(A)	N/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);	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	8	
7123(c)(4)(A)	N/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);	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
7123(c)(4)(A)	N/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);	Functional	Intersects With	Automated Marking	DCH-04.1	Automated mechanisms exist to mark physical media and digital files to indicate the distribution limitations, handling requirements and applicable security markings (if any) of the information to aid Data Loss Prevention (DLP) technologies.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7123(c)(4)(A)	N/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);	Functional	Intersects With	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	5	
7123(c)(4)(A)	N/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);	Functional	Intersects With	Data Tags	DCH-22.2	Mechanisms exist to utilize data tags to automate tracking of sensitive/regulated data across the information lifecycle.	8	
7123(c)(4)(A)	N/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);	Functional	Intersects With	Inventory of Personal Data (PD)	PRI-05.5	Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store, transmit, update and/or share Personal Data (PD).	8	
7123(c)(4)(A)	N/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);	Functional	Intersects With	Metadata	NET-04.5	Mechanisms exist to enforce information flow controls based on metadata.	5	
7123(c)(4)(B)	N/A	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	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	
7123(c)(4)(B)	N/A	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	Functional	Intersects With	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	8	
7123(c)(4)(B)	N/A	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	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
7123(c)(4)(B)	N/A	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	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	8	
7123(c)(4)(C)	N/A	Hardware and software approval processes, and preventing the connection of unauthorized hardware and devices to the business's information system.	Functional	Intersects With	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	8	
7123(c)(4)(C)	N/A	Hardware and software approval processes, and preventing the connection of unauthorized hardware and devices to the business's information system.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	8	
7123(c)(4)(C)	N/A	Hardware and software approval processes, and preventing the connection of unauthorized hardware and devices to the business's information system.	Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	8	
7123(c)(4)(C)	N/A	Hardware and software approval processes, and preventing the connection of unauthorized hardware and devices to the business's information system.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.	10	
7123(c)(4)(C)	N/A	Hardware and software approval processes, and preventing the connection of unauthorized hardware and devices to the business's information system.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical cybersecurity and data protection controls.	5	
7123(c)(4)(C)	N/A	Hardware and software approval processes, and preventing the connection of unauthorized hardware and devices to the business's information system.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	8	
7123(c)(5)	N/A	Secure configuration of hardware and software, including:	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
7123(c)(5)	N/A	Secure configuration of hardware and software, including:	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
7123(c)(5)(A)	N/A	Software updates and upgrades;	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
7123(c)(5)(A)	N/A	Software updates and upgrades;	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5	
7123(c)(5)(A)	N/A	Software updates and upgrades;	Functional	Intersects With	Stable Versions	VPM-04.1	Mechanisms exist to install the latest stable version of any software and/or security-related updates on all applicable systems.	5	
7123(c)(5)(A)	N/A	Software updates and upgrades;	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	8	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Development & Test Environment Configurations	CFG-02.4	Mechanisms exist to manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the risk of unintentional changes.	5	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	3	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	3	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	8	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	8	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Cloud Infrastructure Security Subnet	CLD-03	Mechanisms exist to host security-specific technologies in a dedicated subnet.	5	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	5	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	5	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	5	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Centralized Management of Cybersecurity & Data Protection Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity and data protection controls and related processes.	5	
7123(c)(5)(B)	N/A	Securing on-premises and cloud-based environments;	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity and data protection principles that addresses risk to organizational operations, assets, individuals and other organizations.	3	
7123(c)(5)(C)	N/A	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;	Functional	Intersects With	Masking Displayed Data	DCH-03.2	Mechanisms exist to apply data masking to sensitive/regulated information that is displayed or printed.	3	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7123(c)(5)(C)	N/A	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;	Functional	Intersects With	Removal, Masking, Encryption, Hashing or Replacement of Direct Identifiers	DCH-23.4	Mechanisms exist to remove, mask, encrypt, hash or replace direct identifiers in a dataset.	5	
7123(c)(5)(C)	N/A	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;	Functional	Subset Of	Data Masking	PRI-05.3	Mechanisms exist to mask sensitive/regulated data through data anonymization, pseudonymization, redaction or de-identification.	10	
7123(c)(5)(D)	N/A	Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and	Functional	Intersects With	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	3	
7123(c)(5)(D)	N/A	Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	3	
7123(c)(5)(D)	N/A	Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and	Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	3	
7123(c)(5)(D)	N/A	Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	3	
7123(c)(5)(D)	N/A	Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and	Functional	Intersects With	Cybersecurity & Data Protection Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process.	3	
7123(c)(5)(D)	N/A	Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and	Functional	Intersects With	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	3	
7123(c)(5)(D)	N/A	Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	3	
7123(c)(5)(D)	N/A	Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of cybersecurity and data protection controls following implemented changes to ensure applicable controls operate as designed.	3	
7123(c)(5)(D)	N/A	Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
7123(c)(5)(D)	N/A	Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	8	
7123(c)(5)(D)	N/A	Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8	
7123(c)(5)(D)	N/A	Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	3	
7123(c)(5)(D)	N/A	Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	8	
7123(c)(5)(D)	N/A	Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	8	
7123(c)(5)(D)	N/A	Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	8	
7123(c)(5)(D)	N/A	Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	
7123(c)(5)(E)	N/A	Change management (i.e., processes and procedures to ensure that changes to information system(s) do not undermine existing safeguards).	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
7123(c)(5)(E)	N/A	Change management (i.e., processes and procedures to ensure that changes to information system(s) do not undermine existing safeguards).	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	8	
7123(c)(5)(E)	N/A	Change management (i.e., processes and procedures to ensure that changes to information system(s) do not undermine existing safeguards).	Functional	Intersects With	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	8	
7123(c)(5)(E)	N/A	Change management (i.e., processes and procedures to ensure that changes to information system(s) do not undermine existing safeguards).	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	8	
7123(c)(5)(E)	N/A	Change management (i.e., processes and procedures to ensure that changes to information system(s) do not undermine existing safeguards).	Functional	Intersects With	Cybersecurity & Data Protection Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process.	8	
7123(c)(5)(E)	N/A	Change management (i.e., processes and procedures to ensure that changes to information system(s) do not undermine existing safeguards).	Functional	Intersects With	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	8	
7123(c)(5)(E)	N/A	Change management (i.e., processes and procedures to ensure that changes to information system(s) do not undermine existing safeguards).	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of cybersecurity and data protection controls following implemented changes to ensure applicable controls operate as designed.	8	
7123(c)(6)	N/A	Internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting (e.g., bug bounty and ethical hacking programs).	Functional	Intersects With	Disclosure of Vulnerabilities	TDA-02.11	Mechanisms exist to disclose information about vulnerabilities to relevant stakeholders, including: (1) A description of the vulnerability(ies); (2) Affected product(s) and/or service(s); (3) Potential impact of the vulnerability(ies); (4) Severity of the vulnerability(ies); and (5) Guidance to remediate the vulnerability(ies).	5	
7123(c)(6)	N/A	Internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting (e.g., bug bounty and ethical hacking programs).	Functional	Intersects With	Reporting Exploitable Vulnerabilities	TDA-02.13	Mechanisms exist to notify applicable stakeholders about potentially exploitable vulnerabilities in organization-developed Technology Assets, Applications and/or Services (TAAS), as required by statutory, regulatory and/or contractual obligations.	5	
7123(c)(6)	N/A	Internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting (e.g., bug bounty and ethical hacking programs).	Functional	Intersects With	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made Technology Assets, Applications and/or Services (TAAS).	5	
7123(c)(6)	N/A	Internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting (e.g., bug bounty and ethical hacking programs).	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	8	
7123(c)(6)	N/A	Internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting (e.g., bug bounty and ethical hacking programs).	Functional	Intersects With	Security Disclosure Contact Information	THR-06.1	Mechanisms exist to enable public submissions of discovered or potential security vulnerabilities.	5	
7123(c)(6)	N/A	Internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting (e.g., bug bounty and ethical hacking programs).	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
7123(c)(6)	N/A	Internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting (e.g., bug bounty and ethical hacking programs).	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	
7123(c)(6)	N/A	Internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting (e.g., bug bounty and ethical hacking programs).	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
7123(c)(7)	N/A	Audit-log management, including the centralized storage, retention, and monitoring of logs.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
7123(c)(7)	N/A	Audit-log management, including the centralized storage, retention, and monitoring of logs.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	8	
7123(c)(7)	N/A	Audit-log management, including the centralized storage, retention, and monitoring of logs.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	8	
7123(c)(7)	N/A	Audit-log management, including the centralized storage, retention, and monitoring of logs.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	8	
7123(c)(7)	N/A	Audit-log management, including the centralized storage, retention, and monitoring of logs.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	8	
7123(c)(7)	N/A	Audit-log management, including the centralized storage, retention, and monitoring of logs.	Functional	Intersects With	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	8	
7123(c)(7)	N/A	Audit-log management, including the centralized storage, retention, and monitoring of logs.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	8	
7123(c)(7)	N/A	Audit-log management, including the centralized storage, retention, and monitoring of logs.	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	8	
7123(c)(7)	N/A	Audit-log management, including the centralized storage, retention, and monitoring of logs.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	8	
7123(c)(8)	N/A	Network monitoring and defenses, including the deployment of:	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
7123(c)(8)(A)	N/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	Functional	Intersects With	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
7123(c)(8)(A)	N/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	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
7123(c)(8)(A)	N/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	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7123(c)(8)(A)	N/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	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5	
7123(c)(8)(A)	N/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	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
7123(c)(8)(A)	N/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	Functional	Intersects With	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	5	
7123(c)(8)(A)	N/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	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
7123(c)(8)(A)	N/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	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	
7123(c)(8)(B)	N/A	Data-loss-prevention systems (e.g., software to detect and prevent unauthorized access, use, or disclosure of personal information).	Functional	Equal	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	10	
7123(c)(9)	N/A	Antivirus and antimalware protections.	Functional	Equal	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	
7123(c)(10)	N/A	Segmentation of an information system (e.g., via properly configured firewalls, routers, switches).	Functional	Intersects With	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	3	Incorrect use of "information system" that is defining a network of systems, based on the example provided.
7123(c)(10)	N/A	Segmentation of an information system (e.g., via properly configured firewalls, routers, switches).	Functional	Intersects With	Cloud Infrastructure Security Subnet	CLD-03	Mechanisms exist to host security-specific technologies in a dedicated subnet.	3	Incorrect use of "information system" that is defining a network of systems, based on the example provided.
7123(c)(10)	N/A	Segmentation of an information system (e.g., via properly configured firewalls, routers, switches).	Functional	Intersects With	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	3	Incorrect use of "information system" that is defining a network of systems, based on the example provided.
7123(c)(10)	N/A	Segmentation of an information system (e.g., via properly configured firewalls, routers, switches).	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	8	Incorrect use of "information system" that is defining a network of systems, based on the example provided.
7123(c)(10)	N/A	Segmentation of an information system (e.g., via properly configured firewalls, routers, switches).	Functional	Intersects With	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	3	Incorrect use of "information system" that is defining a network of systems, based on the example provided.
7123(c)(11)	N/A	Limitation and control of ports, services, and protocols.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
7123(c)(11)	N/A	Limitation and control of ports, services, and protocols.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
7123(c)(11)	N/A	Limitation and control of ports, services, and protocols.	Functional	Intersects With	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
7123(c)(11)	N/A	Limitation and control of ports, services, and protocols.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	8	
7123(c)(12)	N/A	Cybersecurity awareness, including how the business maintains current knowledge of changing cybersecurity threats and countermeasures.	Functional	Subset Of	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
7123(c)(12)	N/A	Cybersecurity awareness, including how the business maintains current knowledge of changing cybersecurity threats and countermeasures.	Functional	Intersects With	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
7123(c)(12)	N/A	Cybersecurity awareness, including how the business maintains current knowledge of changing cybersecurity threats and countermeasures.	Functional	Intersects With	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8	
7123(c)(12)	N/A	Cybersecurity awareness, including how the business maintains current knowledge of changing cybersecurity threats and countermeasures.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	5	
7123(c)(12)	N/A	Cybersecurity awareness, including how the business maintains current knowledge of changing cybersecurity threats and countermeasures.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity and data protection awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	8	
7123(c)(12)	N/A	Cybersecurity awareness, including how the business maintains current knowledge of changing cybersecurity threats and countermeasures.	Functional	Intersects With	Cybersecurity & Data Protection Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including basic cybersecurity and data protection awareness training, ongoing awareness training and specific-system training.	3	
7123(c)(13)	N/A	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).	Functional	Intersects With	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
7123(c)(13)	N/A	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).	Functional	Intersects With	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
7123(c)(13)	N/A	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).	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	5	
7123(c)(13)	N/A	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).	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity and data protection awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
7123(c)(13)	N/A	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).	Functional	Intersects With	Cybersecurity & Data Protection Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including basic cybersecurity and data protection awareness training, ongoing awareness training and specific-system training.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Malware Testing Prior to Release	TDA-01.3	Mechanisms exist to utilize at least one(1) malware detection tool to identify if any known malware exists in the final binaries of the product or security update.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	DevSecOps	TDA-01.4	Mechanisms exist to integrate cybersecurity and data protection into Development, Security and Operations (DevSecOps) to prioritize secure practices throughout the Software Development Lifecycle (SDLC).	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Pre-Established Secure Configurations	TDA-02.4	Mechanisms exist to ensure vendors / manufacturers: (1) Deliver the Technology Asset, Application and/or Service (TAAS) with a pre-established, secure configuration implemented; and (2) Use the pre-established, secure configuration as the default for any subsequent TAAS reinstallation or upgrade.	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Insecure Ports, Protocols & Services	TDA-02.6	Mechanisms exist to mitigate the risk associated with the use of insecure ports, protocols and services necessary to operate technology solutions.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Cybersecurity & Data Privacy Representatives For Product Changes	TDA-02.7	Mechanisms exist to include appropriate cybersecurity and data privacy representatives in the product feature and/or functionality change control review process.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Minimizing Attack Surfaces	TDA-02.8	Mechanisms exist to minimize the attack surface of Technology Assets, Applications and/or Services (TAAS) by reasonably mitigating known exploitable vulnerabilities.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Ongoing Product Security Support	TDA-02.9	Mechanisms exist to deliver security updates to Technology Assets, Applications and/or Services (TAAS), where applicable, through: (1) Automatic updates; and (2) Notification of available updates to affected users.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Product Testing & Reviews	TDA-02.10	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for an appropriate level of security and resiliency based on applicable risks and threats.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Disclosure of Vulnerabilities	TDA-02.11	Mechanisms exist to disclose information about vulnerabilities to relevant stakeholders, including: (1) A description of the vulnerability(ies); (2) Affected product(s) and/or service(s); (3) Potential impact of the vulnerability(ies); (4) Severity of the vulnerability(ies); and (5) Guidance to remediate the vulnerability(ies).	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Reporting Exploitable Vulnerabilities	TDA-02.13	Mechanisms exist to notify applicable stakeholders about potentially exploitable vulnerabilities in organization-developed Technology Assets, Applications and/or Services (TAAS), as required by statutory, regulatory and/or contractual obligations.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Developer Architecture & Design	TDA-05	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that: (1) Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; (2) Accurately and completely describes the required security functionality and the allocation of security controls among physical and logical components; and (3) Expresses how individual security functions, mechanisms and services work together to provide required security capabilities and a unified approach to protection.	3	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Criticality Analysis	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Software Assurance Maturity Model (SAMM)	TDA-06.3	Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets, Applications and/or Services (TAAS).	3	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Supporting Toolchain	TDA-06.4	Automated mechanisms exist to improve the accuracy, consistency and comprehensiveness of secure practices throughout the asset's lifecycle.	3	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Software Design Review	TDA-06.5	Mechanisms exist to have an independent review of the software design to confirm that all cybersecurity and data protection requirements are met and that any identified risks are satisfactorily addressed.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Software Design Root Cause Analysis	TDA-06.6	Mechanisms exist to assess software design processes that includes: (1) Conducting Root Cause Analysis (RCA) to identify the underlying causes of issues or failures; (2) Developing actions to address the root cause of the issue or failure; and (3) Implementing the actions and monitoring the implementation for effectiveness.	3	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	3	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Secure Migration Practices	TDA-08.1	Mechanisms exist to ensure secure migration practices purge Technology Assets, Applications and/or Services (TAAS) of test/development/staging data and accounts before it is migrated into a production environment.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Cybersecurity & Data Protection Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity and data protection personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	8	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Secure Settings By Default	TDA-09.6	Mechanisms exist to implement secure configuration settings by default to reduce the likelihood of Technology Assets, Applications and/or Services (TAAS) being deployed with weak security settings that would put the TAAS at a greater risk of compromise.	3	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Use of Live Data	TDA-10	Mechanisms exist to approve, document and control the use of live data in development and test environments.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Developer Configuration Management	TDA-14	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Approved Code	TDA-20.4	Mechanisms exist to govern the approval of binaries and code for production use.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Product Conformity Governance	TDA-21	Mechanisms exist to ensure developed Technology Assets, Applications and/or Services (TAAS) conform to applicable statutory and regulatory requirements, based on the product's and/or service's: (1) Use case(s); and (2) Geographic markets.	5	
7123(c)(14)	N/A	Secure development and coding best practices, including code-reviews and testing.	Functional	Intersects With	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Technology Assets, Applications and/or Services (TAAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	5	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	8	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	5	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	5	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity and data protection control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	3	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration(1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including any flow-down requirements to subcontractors.	3	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data protection controls.	3	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Monitoring for Third-Party Information Disclosure	TPM-07	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of organizational information.	5	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	8	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	8	
7123(c)(15)	N/A	Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053.	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	8	
7123(c)(16)	N/A	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.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	8	
7123(c)(16)	N/A	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.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	8	
7123(c)(16)	N/A	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.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	8	
7123(c)(16)	N/A	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.	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	8	
7123(c)(17)	N/A	How the business manages its responses to security incidents (i.e., its incident response management).	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
7123(c)(17)(A)	N/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.	Functional	Subset Of	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	10	
7123(c)(17)(B)	N/A	The business's incident response management includes:	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
7123(c)(17)(B)(i)	N/A	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	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8	
7123(c)(17)(B)(i)	N/A	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	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
7123(c)(17)(B)(ii)	N/A	How the business tests its incident-response capabilities; and	Functional	Subset Of	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	10	
7123(c)(18)	N/A	Business-continuity and disaster-recovery plans, including data-recovery capabilities and backups.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
7123(d)	N/A	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).	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7123(e)	N/A	The cybersecurity audit report must:	Functional	Subset Of	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	10	
7123(e)(1)	N/A	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.	Functional	Subset Of	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	10	
7123(e)(2)	N/A	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.	Functional	Subset Of	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	10	
7123(e)(3)	N/A	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.	Functional	Subset Of	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	10	
7123(e)(4)	N/A	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.	Functional	Subset Of	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	10	
7123(e)(5)	N/A	Identify any corrections or amendments to any prior cybersecurity audit reports.	Functional	Subset Of	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	10	
7123(e)(6)	N/A	Include the title of up to three qualified individuals responsible for the business's cybersecurity program.	Functional	Subset Of	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7123(e)(7)	N/A	Include the auditor’s name, affiliation, and relevant qualifications.	Functional	Subset Of	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	10	
7123(e)(8)	N/A	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.	Functional	Subset Of	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	10	
7123(e)(9)	N/A	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).	Functional	Subset Of	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	10	
7123(e)(10)	N/A	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.	Functional	Subset Of	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	10	
7123(f)	N/A	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.	Functional	Subset Of	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	10	With a lack of granular controls, NIST CSF 2.0 does not meet all the requirements of this Article.
7124	Certification of Completion.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7124(a)	N/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.	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7124(b)	N/A	The business must submit the certification no later than April 1 following any year that the business is required to complete a cybersecurity audit.	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7124(c)	N/A	The written certification must be completed by a member of the business’s executive management team who:	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7124(c)(1)	N/A	Is directly responsible for the business’s cybersecurity-audit compliance;	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7124(c)(2)	N/A	Has sufficient knowledge of the business’s cybersecurity audit to provide accurate information; and	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7124(c)(3)	N/A	Has the authority to submit the business’s certification to the Agency.	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7124(d)	N/A	The written certification must be completed and submitted to the Agency via its website at https://cppa.ca.gov/. The certification must include:	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7124(d)(1)	N/A	The business’s name and point of contact for the business, including the contact’s name, phone number, and email address.	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7124(d)(2)	N/A	A statement that the business has completed the cybersecurity audit.	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7124(d)(3)	N/A	The time period covered by the cybersecurity audit, by month and year.	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7124(d)(4)	N/A	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.”	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7124(d)(5)	N/A	The name and business title of the person submitting the certification, and the date of the certification.	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7150	When a Business Must Conduct a Risk Assessment.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7150(a)	N/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.	Functional	Subset Of	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7150(b)	N/A	Each of the following processing activities presents significant risk to consumers’ privacy:	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7150(b)(1)	N/A	Selling or sharing personal information.	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7150(b)(2)	N/A	Processing sensitive personal information.	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7150(b)(2)(A)	N/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.	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7150(b)(3)	N/A	Using ADMT for a significant decision concerning a consumer.	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7150(b)(4)	N/A	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.	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7150(b)(5)	N/A	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.	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7150(b)(6)	N/A	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.	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7150(c)	N/A	Illustrative examples of when a business must conduct a risk assessment follow:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7150(c)(1)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7150(c)(2)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7150(c)(3)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7150(c)(4)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7151	Stakeholder Involvement for Risk Assessments.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7151(a)	N/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.	Functional	Intersects With	Risk Assessment Stakeholder Involvement	RSK-04.4	Mechanisms exist to: (1) Define applicable stakeholders for each risk assessment; (2) Involve identified stakeholders in the risk assessment process; and (3) Provide identified stakeholders with results of the risk assessment, upon completion.	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7151(b)	N/A	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.	Functional	Intersects With	Risk Assessment Stakeholder Involvement	RSK-04.4	Mechanisms exist to: (1) Define applicable stakeholders for each risk assessment; (2) Involve identified stakeholders in the risk assessment process; and (3) Provide identified stakeholders with results of the risk assessment, upon completion.	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152	Risk Assessment Requirements.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7152(a)	N/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:	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)	N/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:	Functional	Intersects With	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)	N/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:	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)	N/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:	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(1)	N/A	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.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(2)	N/A	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.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(3)	N/A	Identify and document in a risk assessment report the following operational elements of the processing:	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(3)(A)	N/A	The business's planned method for collecting, using, disclosing, retaining, or otherwise processing personal information, and the sources of the personal information.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(3)(B)	N/A	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.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(3)(C)	N/A	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).	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(3)(D)	N/A	The approximate number of consumers whose personal information the business plans to process.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(3)(E)	N/A	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).	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(3)(F)	N/A	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.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(3)(G)	N/A	For the uses of ADMT set forth in section 7150, subsections (b)(3), the businessmust identify:	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(3)(G)(i)	N/A	The logic of the ADMT, including any assumptions or limitations of thelogic; and	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(3)(G)(ii)	N/A	The output of the ADMT, and how the business will use the output tomake a significant decision.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(4)	N/A	Identify the benefits to the business, the consumer, other stakeholders, and thepublic from the processing of the personal information, as applicable. The benefitsmust 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'sright to know request, a business may identify the relevant benefit as enablingconsumers to receive the personal information they requested on a quickertimeline.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(5)	N/A	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 considerinclude the following:	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(5)(A)	N/A	Unauthorized access, destruction, use, modification, or disclosure of personalinformation; and unauthorized activity resulting in the loss of availability ofpersonal information.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(5)(B)	N/A	Discrimination upon the basis of protected characteristics that would violatefederal or state law.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(5)(C)	N/A	Impairing consumers' control over their personal information, such as byproviding insufficient information for consumers to make an informed decisionregarding the processing of their personal information, or by interfering withconsumers' ability to make choices consistent with their reasonableexpectations.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(5)(D)	N/A	Coercing or compelling consumers into allowing the processing of theirpersonal information, such as by conditioning consumers' acquisition or use ofan online service upon their disclosure of personal information that isunnecessary to the expected functionality of the service, or requiringconsumers to consent to processing when such consent cannot be freely given(e.g., because it was obtained through the use of a dark pattern).	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(5)(E)	N/A	Economic harms, including limiting or depriving consumers of economicopportunities, charging consumers higher prices, or compensating consumersat lower rates based upon profiling; or imposing additional costs upon consumers, including costs associated with the unauthorized access to consumers' personal information.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(5)(F)	N/A	Physical harms to consumers or to property, including processing that createsthe opportunity for physical or sexual violence.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(5)(G)	N/A	Reputational harms, including stigmatization, that could negatively impact anaverage consumer, such as stigmatization of a consumer as a result of a mobiledating application's disclosure of the consumer's sexual or other preferences ina partner outside of the dating application.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(5)(H)	N/A	Psychological harms, including emotional distress, stress, anxiety,embarrassment, fear, frustration, shame, and feelings of violation, that couldnegatively impact an average consumer. Examples of such harms includeemotional distress resulting from disclosure of nonconsensual intimateimagery or disclosure of a consumer's purchase of pregnancy tests oremergency contraception for non-medical purposes.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(6)	N/A	Identify and document in a risk assessment report any safeguards that the businessplans to implement for the processing, such as safeguards to address the negativeimpacts identified in subsection (a)(5).	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(6)(A)	N/A	For example, safeguards that a business may consider include the following:	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(6)(A)(i)	N/A	Encryption, segmentation of information systems, physical and logicalaccess controls, change management, network monitoring and defenses,and data and integrity monitoring;	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(6)(A)(ii)	N/A	Use of privacy-enhancing technologies, such as trusted executionenvironments, federated learning, homomorphic encryption, anddifferential privacy;	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(6)(A)(iii)	N/A	Consulting external parties, such as those described in section 7151,subsection (b), to ensure that the business maintains current knowledgeof emergent privacy risks and countermeasures; and using thatknowledge to identify, assess, and mitigate risks to consumers' privacy;and	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(6)(A)(iv)	N/A	Implementing policies, procedures, and training to ensure that thebusiness's ADMT works for the business's purpose and does notunlawfully discriminate based upon protected characteristics.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7152(a)(7)	N/A	Identify and document in a risk assessment report whether it will initiate theprocessing subject to the risk assessment.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(8)	N/A	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.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7152(a)(9)	N/A	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.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7153	Additional Requirements for Businesses that Process Personal Information to Train Automated Decisionmaking Technology.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7153(a)	N/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.	Functional	Intersects With	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	8	
7153(a)	N/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.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
7153(b)	N/A	The requirements of this section apply only to ADMT trained using personal information.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7154	Goal of a Risk Assessment.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7154(a)	N/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.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7155	Timing and Retention Requirements for Risk Assessments.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7155(a)	N/A	A business must comply with the following timing requirements for conducting and updating its risk assessments:	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7155(a)	N/A	A business must comply with the following timing requirements for conducting and updating its risk assessments:	Functional	Intersects With	Risk Assessment Update	RSK-07	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7155(a)	N/A	A business must comply with the following timing requirements for conducting and updating its risk assessments:	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7155(a)(1)	N/A	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).	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7155(a)(2)	N/A	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.	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7155(a)(3)	N/A	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).	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7155(b)	N/A	For any processing activity identified in section 7150, subsection (b), that the business initiated prior to January 1, 2026 and that continues after January 1, 2026, 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).	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-04.3	Mechanisms exist to define instances that require a risk assessment to be performed.	8	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7155(c)	N/A	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.	Functional	Subset	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7156	Conducting Risk Assessments for a Comparable Set of Processing Activities or inCompliance with Other Laws or Regulations.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7156(a)	N/A	A business may conduct a single risk assessment for a comparable set of processingactivities. A "comparable set of processing activities" that can be addressed by a singlerisk assessment is a set of similar processing activities that present similar risks toconsumers' privacy.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7156(a)(1)	N/A	For example, Business E sells toys to children and is considering using in-store paperforms to collect names, mailing addresses, and birthdays from children that visittheir stores, and to use that information to mail a coupon and list of age-appropriatetoys to each child during the child's birth month and every November. Business Euses the same service providers and technology for each category of mailings acrossall stores. Business E must conduct a risk assessment, including documentingrequired information in its risk assessment report, because it is processing sensitivepersonal information. Business E may use a single risk assessment for processing thepersonal information for the birthday mailing and November mailing across allstores because in each case it is collecting the same personal information in thesame way for the purpose of sending coupons and age-appropriate toy lists tochildren, and this processing presents similar risks to consumers' privacy.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7156(b)	N/A	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.	Functional	Subset Of	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	CCPA refers to "risk assessment" when it is commonly referred to as a Data Protection Impact Assessment (DPIA)
7156(b)(1)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7157	Submission of Risk Assessments to the Agency.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7157(a)	N/A	Timing of Risk Assessment Submissions.	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7157(a)(1)	N/A	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.	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7157(a)(2)	N/A	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.	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7157(b)	N/A	A business must submit to the Agency the following risk assessment information:	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7157(b)(1)	N/A	The business's name and a point of contact for the business, including the contact's name, phone number, and email address.	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7157(b)(2)	N/A	The time period covered by the submission, by month and year.	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7157(b)(3)	N/A	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).	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7157(b)(4)	N/A	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).	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7157(b)(5)	N/A	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."	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7157(b)(6)	N/A	The name and business title of the person submitting the risk assessment information, and the date of the certification.	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7157(c)	N/A	The individual submitting the information set forth in subsection (b) must be a member of the business's executive management team who:	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7157(c)(1)	N/A	Is directly responsible for the business's risk-assessment compliance;	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7157(c)(2)	N/A	Has sufficient knowledge of the business's risk assessment to provide accurate information; and	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7157(c)(3)	N/A	Has the authority to submit the risk assessment information to the Agency.	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7157(d)	N/A	The risk assessment information must be submitted to the Agency via the Agency's website at https://cppa.ca.gov/.	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7157(e)	N/A	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.	Functional	Subset Of	Cybersecurity & Data Protection Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	10	
7200	When a Business's Use of Automated Decisionmaking Technology is Subject to the Requirements of This Article.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7200(a)	N/A	A business that uses ADMT to make a significant decision concerning a consumer must comply with the requirements of this Article.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
7200(b)	N/A	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.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
7220	Pre-use Notice Requirements.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7220(a)	N/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).	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(b)	N/A	The Pre-use Notice must:	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(b)(1)	N/A	Comply with section 7003, subsections (a)–(b).	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(b)(2)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(b)(3)	N/A	Be presented in the manner in which the business primarily interacts with the consumer.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(c)	N/A	The Pre-use Notice must include the following:	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(c)(1)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(c)(2)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(c)(2)(A)	N/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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(c)(2)(B)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(c)(3)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(c)(4)	N/A	That the business is prohibited from retaliating against consumers for exercising their CCPA rights.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(c)(5)	N/A	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:	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(c)(5)(A)	N/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).	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(c)(5)(B)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(c)(5)(C)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(d)	N/A	In providing the information required by subsection (c)(5), a business's Pre-use Notice is not required to include:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7220(d)(1)	N/A	Trade secrets, as defined in Civil Code section 3426.1, subdivision (d); or	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7220(d)(2)	N/A	Information that would compromise the business's ability to:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7220(d)(2)(A)	N/A	Prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information;	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7220(d)(2)(B)	N/A	Resist malicious, deceptive, fraudulent, or illegal actions directed at the business or at consumers, or to prosecute those responsible for those actions; or	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7220(d)(2)(C)	N/A	Ensure the physical safety of natural persons.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7220(e)	N/A	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:	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(e)(1)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(e)(2)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7220(e)(3)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7220(e)(4)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Use Notification	PRI-19.1	Mechanisms exist to notify data subjects of their rights through a pre-use notice when their Personal Data (PD) will be processed by an Automated Decision-Making Technology (ADMT).	10	
7221	Requests to Opt-Out of ADMT.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7221(a)	N/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).	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(b)	N/A	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:	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(b)(1)	N/A	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:	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(b)(1)(A)	N/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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(b)(1)(B)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(b)(2)	N/A	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:	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(b)(2)(A)	N/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	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(b)(2)(B)	N/A	The ADMT works for the business's purpose and does not unlawfully discriminate based upon protected characteristics.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(b)(3)	N/A	For allocation/assignment of work and compensation decisions as set forth in section 7001, subsection (ddd)(4)(B), if the following are true:	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(b)(3)(A)	N/A	The business uses the ADMT solely for the business's allocation/assignment of work or compensation; and	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(b)(3)(B)	N/A	The ADMT works for the business's purpose and does not unlawfully discriminate based upon protected characteristics.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(c)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(c)(1)	N/A	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."	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7221(c)(2)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7221(c)(3)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7221(c)(4)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7221(d)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(e)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(f)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(g)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(h)	N/A	A business must provide a means by which the consumer can confirm that the business has processed their request to opt-out of ADMT.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(i)	N/A	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).	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent	8	
7221(j)	N/A	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.	Functional	Intersects With	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	8	
7221(k)	N/A	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.	Functional	Intersects With	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent	5	
7221(l)	N/A	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.	Functional	Intersects With	Product or Service Delivery Restrictions	PRI-03.5	Mechanisms exist to prevent discrimination against a data subject for exercising their legal rights pertaining to modifying or revoking consent, including prohibiting: (1) Refusing products and/or services; (2) Charging different rates for goods and/or services; and (3) Providing different levels of quality	5	
7221(m)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(n)	N/A	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:	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(n)(1)	N/A	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	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	
7221(n)(2)	N/A	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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Opt-Out Consent	PRI-19.2	Mechanisms exist to provide concise, unambiguous and understandable instructions on how a data subjects can opt-out of Automated Decision-Making Technology (ADMT).	10	

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7222	Requests to Access ADMT.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7222(a)	N/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.	Functional	Subset Of	Automated Decision-Making Technology (ADMT) Transparency	PRI-19.3	Mechanisms exist to provide data subjects with sufficient details of the logic and parameters used by Automated Decision-Making Technology (ADMT) to process the Personal Data (PD) to generate an output with respect to the data subject.	10	
7222(b)	N/A	When responding to a consumer's request to access ADMT, a business must provide plain language explanations of the following information to the consumer:	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(b)(1)	N/A	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."	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(b)(2)	N/A	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.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(b)(3)	N/A	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.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(b)(3)(A)	N/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.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(b)(4)	N/A	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.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(b)(4)(A)	N/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.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	The proper terminology is a "privacy notice" for a publicly-facing document, not a "privacy policy" as stated in this law.
7222(c)	N/A	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:	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(c)(1)	N/A	Trade secrets, as defined in Civil Code section 3426.1, subdivision (d); or	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(c)(2)	N/A	Information that would compromise the business's ability to:	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(c)(2)(A)	N/A	Prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information;	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(c)(2)(B)	N/A	Resist malicious, deceptive, fraudulent, or illegal actions directed at the business or at consumers, or to prosecute those responsible for those actions; or	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(c)(2)(C)	N/A	Ensure the physical safety of natural persons.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(d)	N/A	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.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(e)	N/A	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.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(f)	N/A	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.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(g)	N/A	A business must use reasonable security measures when transmitting the requested information to the consumer.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(h)	N/A	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.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(i)	N/A	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.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(j)	N/A	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.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(k)	N/A	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.	Functional	Intersects With	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.	5	
7222(l)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7270	Definition of Insurance Company.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7270(a)	N/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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7271	General Application of the CCPA to Insurance Companies.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7271(a)	N/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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7271(b)	N/A	Illustrative examples follow.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7271(b)(1)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7271(b)(2)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7271(b)(3)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7300	Sworn Complaints Filed with the Agency.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7300(a)	N/A	Requirements for filing a sworn complaint. Sworn complaints 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:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7300(a)(1)	N/A	Identify the business, service provider, contractor, or person who allegedly violated the CCPA;	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7300(a)(2)	N/A	State the facts that support each alleged violation and include any documents or other evidence supporting this conclusion;	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7300(a)(3)	N/A	Authorize the alleged violator and the Agency to communicate regarding the complaint, including disclosing the complaint and any information relating to the complaint;	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
7300(a)(4)	N/A	Include the name and current contact information of the complainant; and	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7300(a)(5)	N/A	Be signed and submitted under penalty of perjury.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7300(b)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7301	Investigations.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7301(a)	N/A	The Agency may open investigations upon the sworn complaint of any person or on its own initiative. For example, the Agency may initiate investigations based upon referrals from government agencies or private organizations, and nonsworn or anonymous complaints.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7301(b)	N/A	As part of the Agency's decision to pursue investigations of possible or alleged violations of the CCPA, the Agency may consider all facts it determines to be relevant, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good-faith efforts to comply with those requirements.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7302	Probable Cause Proceedings.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7302(a)	N/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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7302(b)	N/A	Probable Cause Notice. The Agency will provide the alleged violator with notice of the probable cause proceeding as required by Civil Code section 1798.199.50.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7302(c)	N/A	Probable Cause Proceeding.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7302(c)(1)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7302(c)(2)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7302(c)(3)	N/A	If the alleged violator(s) fails to 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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7302(d)	N/A	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.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7303	Stipulated Orders.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7303(a)	N/A	At any time before or during an administrative hearing and in lieu of such a hearing, the Head of Enforcement and the alleged violator may stipulate to the entry of a final order. If a stipulation has been agreed upon and the scheduled date of the hearing is set to occur before the next Board meeting, the Enforcement Division will apply for a continuance of the hearing.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7303(b)	N/A	The final order must be approved by the Board, which may consider the matter in closed session.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7303(c)	N/A	The stipulated final order shall be public and have the force of an order of the Board.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7304	Agency Audits.	N/A	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7304(a)	N/A	Scope. The Agency may audit a business, service provider, contractor, or person to ensure compliance with any provision of the CCPA.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7304(b)	N/A	Criteria for Selection. The Agency may conduct an audit to investigate possible violations of the CCPA. Alternatively, the Agency may conduct an audit if the subject's collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7304(c)	N/A	Audits may be announced or unannounced as determined by the Agency.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7304(d)	N/A	Failure to Cooperate. A subject's failure to cooperate during the Agency's audit may result in the Agency issuing a subpoena, seeking a warrant, or otherwise exercising its powers to ensure compliance with the CCPA.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
7304(e)	N/A	Protection of Personal Information. Consumer personal information disclosed to the Agency during an audit shall be maintained in compliance with the Information Practices Act of 1977, Civil Code section 1798, et seq.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)