CALIFORNIA CONSUMER PRIVACY ACT OF 2018

effective 01/01/2026 – AB 137, AB 566 update
posted to cppa.ca.gov December 2025

Contents

1798.100. General Duties of Businesses that Collect Personal Information 3

1798.105. Consumers' Right to Delete Personal Information 4

1798.106. Consumers' Right to Correct Inaccurate Personal Information 6

1798.110. Consumers' Right to Know What Personal Information is Being Collected. Right to Access Personal Information 6

1798.115. Consumers' Right to Know What Personal Information is Sold or Shared and to Whom... 7

1798.120. Consumers' Right to Opt Out of Sale or Sharing of Personal Information 8

1798.121. Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information 9

1798.125. Consumers' Right of No Retaliation Following Opt Out or Exercise of Other Rights..... 10

1798.130. Notice, Disclosure, Correction, and Deletion Requirements 11

1798.135. Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information 15

1798.136. 19

1798.140. Definitions 19

1798.145. Exemptions 32

1798.146. 42

1798.148. 44

1798.150. Personal Information Security Breaches 46

1798.155. Administrative Enforcement 47

1798.160. Consumer Privacy Fund 47

1798.175. Conflicting Provisions 49

1798.180. Preemption 50

1798.185. Regulations 50

1798.190. Anti-Avoidance 57

1798.192. Waiver 57

1798.194. 57

1798.196. 57

1798.198. 58
1798.199. 58
1798.199.10. 58
1798.199.15. 58
1798.199.20. 59
1798.199.25. 59
1798.199.30. 59
1798.199.35. 59
1798.199.40. 59
1798.199.45. 61
1798.199.50. 61
1798.199.55. 61
1798.199.60. 62
1798.199.65. 62
1798.199.70. 62
1798.199.75. 63
1798.199.80. 63
1798.199.85. 64
1798.199.90. 64
1798.199.95. 65
1798.199.100. 66

1798.100. General Duties of Businesses that Collect Personal Information

(a) A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers of the following:

(1) The categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice consistent with this section.

(2) If the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section.

(3) The length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.

(b) A business that, acting as a third party, controls the collection of personal information about a consumer may satisfy its obligation under subdivision (a) by providing the required information prominently and conspicuously on the homepage of its internet website. In addition, if a business acting as a third party controls the collection of personal information about a consumer on its premises, including in a vehicle, then the business shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information are used, and whether that personal information is sold, in a clear and conspicuous manner at the location.

(c) A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.

(d) A business that collects a consumer's personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose shall enter into an agreement with the third party, service provider, or contractor, that:

(1) Specifies that the personal information is sold or disclosed by the business only for limited and specified purposes.

(2) Obligates the third party, service provider, or contractor to comply with applicable obligations under this title and obligate those persons to provide the same level of privacy protection as is required by this title.

(3) Grants the business rights to take reasonable and appropriate steps to help ensure that the third party, service provider, or contractor uses the personal information transferred in a manner consistent with the business' obligations under this title.

(4) Requires the third party, service provider, or contractor to notify the business if it makes a determination that it can no longer meet its obligations under this title.

(5) Grants the business the right, upon notice, including under paragraph (4), to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

(e) A business that collects a consumer's personal information shall 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 Section 1798.81.5.

(f) Nothing in this section shall require a business to disclose trade secrets, as specified in regulations adopted pursuant to paragraph (3) of subdivision (a) of Section 1798.185.

1798.105. Consumers' Right to Delete Personal Information

(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

(c) (1) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records, notify any service providers or contractors to delete the consumer's personal information from their records, and notify all third parties to whom the business has sold or shared the

personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.

(2) The business may maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws or for other purposes, solely to the extent permissible under this title.

(3) A service provider or contractor shall cooperate with the business in responding to a verifiable consumer request, and at the direction of the business, shall delete, or enable the business to delete and shall notify any of its own service providers or contractors to delete personal information about the consumer collected, used, processed, or retained by the service provider or the contractor. The service provider or contractor shall notify any service providers, contractors, or third parties who may have accessed personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, to delete the consumer's personal information unless this proves impossible or involves disproportionate effort. A service provider or contractor shall not be required to comply with a deletion request submitted by the consumer directly to the service provider or contractor to the extent that the service provider or contractor has collected, used, processed, or retained the consumer's personal information in its role as a service provider or contractor to the business.

(d) A business, or a service provider or contractor acting pursuant to its contract with the business, another service provider, or another contractor, shall not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for the business, service provider, or contractor to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated by the consumer within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Help to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law.

(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

(6) Engage in public or peer-reviewed scientific, historical, or statistical research that conforms or adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the ability to complete such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business and compatible with the context in which the consumer provided the information.

(8) Comply with a legal obligation.

1798.106. Consumers' Right to Correct Inaccurate Personal Information

(a) A consumer shall have the right to request a business that maintains inaccurate personal information about the consumer to correct that inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's right to request correction of inaccurate personal information.

(c) A business that receives a verifiable consumer request to correct inaccurate personal information shall use commercially reasonable efforts to correct the inaccurate personal information as directed by the consumer, pursuant to Section 1798.130 and regulations adopted pursuant to paragraph (7) of subdivision (a) of Section 1798.185.

1798.110. Consumers' Right to Know What Personal Information is Being Collected. Right to Access Personal Information

(a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

(1) The categories of personal information it has collected about that consumer.

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

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

(4) The categories of third parties to whom the business discloses personal information.

(5) The specific pieces of personal information it has collected about that consumer.

(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to subparagraph (B) of paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer, provided that a business shall be deemed to be in compliance with paragraphs (1) to (4), inclusive, of subdivision (a) to the extent that the categories of information and the business or commercial purpose for collecting, selling, or sharing personal information it would be required to disclose to the consumer pursuant to paragraphs (1) to (4), inclusive, of subdivision (a) is the same as the information it has disclosed pursuant to paragraphs (1) to (4), inclusive, of subdivision (c).

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The categories of personal information it has collected about consumers.

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

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

(4) The categories of third parties to whom the business discloses personal information.

(5) That a consumer has the right to request the specific pieces of personal information the business has collected about that consumer.

1798.115. Consumers' Right to Know What Personal Information is Sold or Shared and to Whom

(a) A consumer shall have the right to request that a business that sells or shares the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

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

(2) The categories of personal information that the business sold or shared about the consumer and the categories of third parties to whom the personal information was sold or shared, by category or categories of personal information for each category of third parties to whom the personal information was sold or shared.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose and the categories of persons to whom it was disclosed for a business purpose.

(b) A business that sells or shares personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to paragraph (4) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

(c) A business that sells or shares consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The category or categories of consumers' personal information it has sold or shared, or if the business has not sold or shared consumers' personal information, it shall disclose that fact.

(2) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell or share personal information about a consumer that has been sold to, or shared with, the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.

1798.120. Consumers' Right to Opt Out of Sale or Sharing of Personal Information

(a) (1) A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. This right may be referred to as the right to opt out of sale or sharing.

(2) A business to which another business transfers the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the transferee assumes control of all of, or part of, the transferor shall comply with a consumer's direction to the transferor made pursuant to this subdivision.

(b) A business that sells consumers' personal information to, or shares it with, third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold or shared and that consumers have the "right to opt out" of the sale or sharing of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell or share the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of

consumers who are less than 13 years of age, has affirmatively authorized the sale or sharing of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.

(d) A business that has received direction from a consumer not to sell or share the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell or share the minor consumer's personal information, shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from selling or sharing the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides consent, for the sale or sharing of the consumer's personal information.

1798.121. Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information

(a) A consumer shall have the right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, to perform the services set forth in paragraphs (2), (4), (5), and (8) of subdivision (e) of Section 1798.140, and as authorized by regulations adopted pursuant to subparagraph (C) of paragraph (18) of subdivision (a) of Section 1798.185. A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in this subdivision shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be used, or disclosed to a service provider or contractor, for additional, specified purposes and that consumers have the right to limit the use or disclosure of their sensitive personal information.

(b) A business that has received direction from a consumer not to use or disclose the consumer's sensitive personal information, except as authorized by subdivision (a), shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from using or disclosing the consumer's sensitive personal information for any other purpose after its receipt of the consumer's direction unless the consumer subsequently provides consent for the use or disclosure of the consumer's sensitive personal information for additional purposes.

(c) A service provider or contractor that assists a business in performing the purposes authorized by subdivision (a) may not use the sensitive personal information after it has received instructions from the business and to the extent it has actual knowledge that the personal information is sensitive personal information for any other purpose. A service provider or contractor is only required to limit its use of sensitive personal information received pursuant to a written contract with the business in response to instructions from the business and only with respect to its relationship with that business.

(d) Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to this section, as further defined

in regulations adopted pursuant to subparagraph (C) of paragraph (18) of subdivision (a) of Section 1798.185, and shall be treated as personal information for purposes of all other sections of this act, including Section 1798.100.

1798.125. Consumers' Right of No Retaliation Following Opt Out or Exercise of Other Rights

(a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(E) Retaliating against an employee, applicant for employment, or independent contractor, as defined in subparagraph (A) of paragraph (2) of subdivision (m) of Section 1798.145, for exercising their rights under this title.

(2) Nothing in this subdivision prohibits a business, pursuant to subdivision (b), from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.

(3) This subdivision does not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs consistent with this title.

(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale or sharing of personal information, or the retention of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is reasonably related to the value provided to the business by the consumer's data.

(2) A business that offers any financial incentives pursuant to this subdivision, shall notify consumers of the financial incentives pursuant to Section 1798.130.

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.130 that clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time. If a consumer refuses to provide opt-

in consent, then the business shall wait for at least 12 months before next requesting that the consumer provide opt-in consent, or as prescribed by regulations adopted pursuant to Section 1798.185.

(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

1798.130. Notice, Disclosure, Correction, and Deletion Requirements

(a) In order to comply with Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1) (A) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively, including, at a minimum, a toll-free telephone number. 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 for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or for requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively.

(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively.

(2) (A) Disclose and deliver the required information to a consumer free of charge, correct inaccurate personal information, or delete a consumer's personal information, based on the consumer's request, within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business' duty to disclose and deliver the information, to correct inaccurate personal information, or to delete personal information within 45 days of receipt of the consumer's request. The time period to provide the required information, to correct inaccurate personal information, or to delete personal information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure of the required information shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity

to another entity without hindrance. The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request provided that if the consumer, has an account with the business, the business may require the consumer to use that account to submit a verifiable consumer request.

(B) The disclosure of the required information shall cover the 12-month period preceding the business' receipt of the verifiable consumer request provided that, upon the adoption of a regulation pursuant to paragraph (8) of subdivision (a) of Section 1798.185, a consumer may request that the business disclose the required information beyond the 12-month period, and the business shall be required to provide that information unless doing so proves impossible or would involve a disproportionate effort. A consumer's right to request required information beyond the 12-month period, and a business' obligation to provide that information, shall only apply to personal information collected on or after January 1, 2022. Nothing in this subparagraph shall require a business to keep personal information for any length of time.

(3) (A) A business that receives a verifiable consumer request pursuant to Section 1798.110 or 1798.115 shall disclose any personal information it has collected about a consumer, directly or indirectly, including through or by a service provider or contractor, to the consumer. A service provider or contractor shall not be required to comply with a verifiable consumer request received directly from a consumer or a consumer's authorized agent, pursuant to Section 1798.110 or 1798.115, to the extent that the service provider or contractor has collected personal information about the consumer in its role as a service provider or contractor. A service provider or contractor shall provide assistance to a business with which it has a contractual relationship with respect to the business' response to a verifiable consumer request, including, but not limited to, by providing to the business the consumer's personal information in the service provider or contractor's possession, which the service provider or contractor obtained as a result of providing services to the business, and by correcting inaccurate information or by enabling the business to do the same. A service provider or contractor that collects personal information pursuant to a written contract with a business shall be required to assist the business through appropriate technical and organizational measures in complying with the requirements of subdivisions (d) to (f), inclusive, of Section 1798.100, taking into account the nature of the processing.

(B) For purposes of subdivision (b) of Section 1798.110:

(i) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(ii) Identify by category or categories the personal information collected about the consumer for the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected; the categories of sources from which the consumer's personal information was collected; the business or commercial purpose for collecting, selling, or sharing the consumer's personal information; and the categories of third parties to whom the business discloses the consumer's personal information.

(iii) Provide the specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance. "Specific pieces of information" do not include data generated to help ensure security and integrity or as prescribed by regulation. Personal information is not considered to have been disclosed by a business when a consumer instructs a business to transfer the consumer's personal information from one business to another in the context of switching services.

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold or shared during the applicable period of time by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold or shared during the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold or shared. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose during the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of persons to whom the consumer's personal information was

disclosed for a business purpose during the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its internet website, and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, and 1798.125 and two or more designated methods for submitting requests, except as provided in subparagraph (A) of paragraph (1) of subdivision (a).

(B) For purposes of subdivision (c) of Section 1798.110:

(i) A list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

(ii) The categories of sources from which consumers' personal information is collected.

(iii) The business or commercial purpose for collecting, selling, or sharing consumers' personal information.

(iv) The categories of third parties to whom the business discloses consumers' personal information.

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold or shared about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold or shared, or if the business has not sold or shared consumers' personal information in the preceding 12 months, the business shall prominently disclose that fact in its privacy policy.

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by

reference to the enumerated category in subdivision (c) that most closely describes the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business' privacy practices or the business' compliance with this title are informed of all requirements in Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business' verification of the consumer's request solely for the purposes of verification and shall not further disclose the personal information, retain it longer than necessary for purposes of verification, or use it for unrelated purposes.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.100, 1798.110, and 1798.115 shall follow the definitions of personal information and sensitive personal information in Section 1798.140 by describing the categories of personal information using the specific terms set forth in subparagraphs (A) to (K), inclusive, of paragraph (1) of subdivision (v) of Section 1798.140 and by describing the categories of sensitive personal information using the specific terms set forth in paragraphs (1) to (9), inclusive, of subdivision (ae) of Section 1798.140.

1798.135. Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information

(a) A business that sells or shares consumers' personal information or uses or discloses consumers' sensitive personal information for purposes other than those authorized by subdivision (a) of Section 1798.121 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business' internet homepages, titled "Do Not Sell or Share My Personal Information," to an internet web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale or sharing of the consumer's personal information.

(2) Provide a clear and conspicuous link on the business' internet homepages, titled "Limit the Use of My Sensitive Personal Information," that enables a consumer, or a person authorized by the consumer, to limit the use or disclosure of the consumer's

sensitive personal information to those uses authorized by subdivision (a) of Section 1798.121.

(3) At the business' discretion, utilize a single, clearly labeled link on the business' internet homepages, in lieu of complying with paragraphs (1) and (2), if that link easily allows a consumer to opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information.

(4) In the event that a business responds to opt-out requests received pursuant to paragraph (1), (2), or (3) by informing the consumer of a charge for the use of any product or service, present the terms of any financial incentive offered pursuant to subdivision (b) of Section 1798.125 for the retention, use, sale, or sharing of the consumer's personal information.

(b) (1) A business shall not be required to comply with subdivision (a) if the business allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications set forth in regulations adopted pursuant to paragraph(19) of subdivision (a) of Section 1798.185, to the business indicating the consumer's intent to opt out of the business' sale or sharing of the consumer's personal information or to limit the use or disclosure of the consumer's sensitive personal information, or both.

(2) A business that allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information pursuant to paragraph (1) may provide a link to a web page that enables the consumer to consent to the business ignoring the opt-out preference signal with respect to that business' sale or sharing of the consumer's personal information or the use of the consumer's sensitive personal information for additional purposes provided that:

(A) The consent web page also allows the consumer or a person authorized by the consumer to revoke the consent as easily as it is affirmatively provided.

(B) The link to the web page does not degrade the consumer's experience on the web page the consumer intends to visit and has a similar look, feel, and size relative to other links on the same web page.

(C) The consent web page complies with technical specifications set forth in regulations adopted pursuant to paragraph (19) of subdivision (a) of Section 1798.185.

(3) A business that complies with subdivision (a) is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b).

(c) A business that is subject to this section shall:

(1) Not require a consumer to create an account or provide additional information beyond what is necessary in order to direct the business not to sell or share the consumer's personal information or to limit use or disclosure of the consumer's sensitive personal information.

(2) Include a description of a consumer's rights pursuant to Sections 1798.120 and 1798.121, along with a separate link to the "Do Not Sell or Share My Personal Information" internet web page and a separate link to the "Limit the Use of My Sensitive Personal Information" internet web page, if applicable, or a single link to both choices, or a statement that the business responds to and abides by opt-out preference signals sent by a platform, technology, or mechanism in accordance with subdivision (b), in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers' privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business' privacy practices or the business' compliance with this title are informed of all requirements in Sections 1798.120, 1798.121, and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt out of the sale or sharing of their personal information or limit the use or disclosure of their sensitive personal information, refrain from selling or sharing the consumer's personal information or using or disclosing the consumer's sensitive personal information and wait for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's personal information or the use and disclosure of the consumer's sensitive personal information for additional purposes, or as authorized by regulations.

(5) For consumers under 16 years of age who do not consent to the sale or sharing of their personal information, refrain from selling or sharing the personal information of the consumer under 16 years of age and wait for at least 12 months before requesting the consumer's consent again, or as authorized by regulations or until the consumer attains 16 years of age.

(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(d) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

(e) A consumer may authorize another person to opt out of the sale or sharing of the consumer's personal information and to limit the use of the consumer's sensitive personal information on the consumer's behalf, including through an opt-out preference signal, as defined in paragraph (1) of subdivision (b), indicating the consumer's intent to opt out, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General regardless of whether the business has elected to comply with subdivision (a) or (b). For purposes of clarity, a business that elects to comply with subdivision (a) may respond to the consumer's opt-out request consistently with Section 1798.125.

(f) If a business communicates a consumer's opt-out request to any person authorized by the business to collect personal information, the person shall thereafter only use that consumer's personal information for a business purpose specified by the business, or as otherwise permitted by this title, and shall be prohibited from:

(1) Selling or sharing the personal information.

(2) Retaining, using, or disclosing that consumer's personal information.

(A) For any purpose other than for the specific purpose of performing the services offered to the business.

(B) Outside of the direct business relationship between the person and the business.

(C) For a commercial purpose other than providing the services to the business.

(g) A business that communicates a consumer's opt-out request to a person pursuant to subdivision (f) shall not be liable under this title if the person receiving the opt-out request violates the restrictions set forth in the title provided that, at the time of communicating the opt-out request, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation. Any provision of a

contract or agreement of any kind that purports to waive or limit in any way this subdivision shall be void and unenforceable.

1798.136.

(a) (1) A business shall not develop or maintain a browser that does not include functionality configurable by a consumer that enables the browser to send an opt-out preference signal to businesses with which the consumer interacts through the browser.

(2) The functionality required by paragraph (1) shall be easy for a reasonable person to locate and configure.

(b) A business that develops or maintains a browser shall make clear to a consumer in its public disclosures how the opt-out preference signal works and the intended effect of the opt-out preference signal.

(c) The California Privacy Protection Agency may adopt regulations as necessary to implement and administer this section.

(d) A business that develops or maintains a browser that includes a functionality that enables the browser to send an opt-out preference signal pursuant to this section shall not be liable for a violation of this title by a business that receives the opt-out preference signal.

(e) As used in this section:

(1) "Browser" means an interactive software application that is used by consumers to locate, access, and navigate internet websites.

(2) "Opt-out preference signal" means a signal that complies with this title and that communicates the consumer's choice to opt out of the sale and sharing of the consumer's personal information.

(f) This section shall become operative on January 1, 2027.

1798.140. Definitions

For purposes of this title:

(a) "Advertising and marketing" means a communication by a business or a person acting on the business' behalf in any medium intended to induce a consumer to obtain goods, services, or employment.

(b) "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device.

"Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

(c) "Biometric information" means an individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(d) "Business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000)* in the preceding calendar year, as adjusted pursuant to subdivision (d) of Section 1798.199.95.

(B) Alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households.

(C) Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business and with whom the business shares consumers' personal information. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark that the average consumer would understand that two or more entities are commonly owned.

* Pursuant to Civil Code § 1798.199.95(d), this monetary amount has been updated. Please see updated amount.

(3) A joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.

(4) A person that does business in California, that is not covered by paragraph (1), (2), or (3), and that voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, this title.

(e) "Business purpose" means the use of personal information for the business' operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, as defined by regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) 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 consumer's 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.

(5) Performing services on behalf of the business, including 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.

(6) Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers 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 persons or collects from its own interaction with consumers.

(7) Undertaking internal research for technological development and demonstration.

(8) Undertaking activities to verify or maintain the quality or safety of a 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, manufactured for, or controlled by the business.

(f) "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

(g) "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.

(h) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.

(i) "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

(j) (1) "Contractor" means a person to whom the business makes available a consumer's personal information for a business purpose, pursuant to a written contract with the business, provided that the contract:

(A) Prohibits the contractor from:

(i) Selling or sharing the personal information.

(ii) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract, including retaining, using, or disclosing the personal information for a commercial

purpose other than the business purposes specified in the contract, or as otherwise permitted by this title.

(iii) Retaining, using, or disclosing the information outside of the direct business relationship between the contractor and the business.

(iv) Combining the personal information that the contractor receives pursuant to a written contract with the business with personal information that it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that the contractor may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (9) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) and in regulations adopted by the California Privacy Protection Agency.

(B) Includes a certification made by the contractor that the contractor understands the restrictions in subparagraph (A) and will comply with them.

(C) Permits, subject to agreement with the contractor, the business to monitor the contractor's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

(2) If a contractor engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the contractor engages another person to assist in processing personal information for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

(k) "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly branded internet websites, applications, or services, other than the business, distinctly branded internet website, application, or service with which the consumer intentionally interacts.

(l) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation.

(m) "Deidentified" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information:

(1) Takes reasonable measures to ensure that the information cannot be associated with a consumer or household.

(2) Publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision.

(3) Contractually obligates any recipients of the information to comply with all provisions of this subdivision.

(n) "Designated methods for submitting requests" means a mailing address, email address, internet web page, internet web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

(o) "Device" means any physical object that is capable of connecting to the internet, directly or indirectly, or to another device.

(p) "Homepage" means the introductory page of an internet website and any internet web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information,'' or settings page, and any other location that allows consumers to review the notices required by this title, including, but not limited to, before downloading the application.

(q) "Household" means a group, however identified, of consumers who cohabitate with one another at the same residential address and share use of common devices or services.

(r) "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(s) "Intentionally interacts" means when the consumer intends to interact with a person, or disclose personal information to a person, via one or more deliberate interactions, including visiting the person's internet website or purchasing a good or service from the person. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a person.

(t) "Nonpersonalized advertising" means advertising and marketing that is based solely on a consumer's personal information derived from the consumer's current interaction with the business with the exception of the consumer's precise geolocation.

(u) "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(v) (1) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(B) Any personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(L) Sensitive personal information.

(2) (A) "Personal information" does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern.

(B) (i) For purposes of this paragraph, "publicly available" means any of the following:

(I) Information that is lawfully made available from federal, state, or local government records.

(II) Information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media.

(III) Information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.

(ii) "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

(3) "Personal information" does not include consumer information that is deidentified or aggregate consumer information.

(4) "Personal information" can exist in various formats, including, but not limited to, all of the following:

(A) Physical formats, including paper documents, printed images, vinyl records, or video tapes.

(B) Digital formats, including text, image, audio, or video files.

(C) Abstract digital formats, including compressed or encrypted files, metadata, or artificial intelligence systems that are capable of outputting personal information.

(w) "Precise geolocation" means any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by regulations.

(x) "Probabilistic identifier" means the identification of a consumer or a consumer's device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(y) “Processing” means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.

(z) “Profiling” means any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (15) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(aa) “Pseudonymize” or “Pseudonymization” means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(ab) “Research” means scientific analysis, systematic study, and observation, including basic research or applied research that is designed to develop or contribute to public or scientific knowledge and that adheres or otherwise conforms to all other applicable ethics and privacy laws, including, but not limited to, studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer’s interactions with a business’ service or device for other purposes shall be:

(1) Compatible with the business purpose for which the personal information was collected.

(2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, by a business.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain, other than as needed to support the research.

(4) Subject to business processes that specifically prohibit reidentification of the information, other than as needed to support the research.

(5) Made subject to business processes to prevent inadvertent release of deidentified information.

(6) Protected from any reidentification attempts.

(7) Used solely for research purposes that are compatible with the context in which the personal information was collected.

(8) Subjected by the business conducting the research to additional security controls that limit access to the research data to only those individuals as are necessary to carry out the research purpose.

(ac) "Security and integrity" means the ability of:

(1) Networks or information systems to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.

(2) Businesses to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions and to help prosecute those responsible for those actions.

(3) Businesses to ensure the physical safety of natural persons.

(ad) (1) "Sell," "selling," "sale," or "sold,'' means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration.

(2) For purposes of this title, a business does not sell personal information when:

(A) A consumer uses or directs the business to intentionally:

(i) Disclose personal information.

(ii) Interact with one or more third parties.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information.

(C) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently

prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this title. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(ae) "Sensitive personal information" means:

(1) Personal information that reveals:

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

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

(C) A consumer's precise geolocation.

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

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

(F) A consumer's genetic data.

(G) (i) A consumer's neural data.

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

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

(B) Personal information collected and analyzed concerning a consumer's health.

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

(3) Sensitive personal information that is "publicly available" pursuant to paragraph (2) of subdivision (v) shall not be considered sensitive personal information or personal information.

(af) "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.

(ag) (1) "Service provider" means a person that processes personal information on behalf of a business and that receives from or on behalf of the business consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the person from:

(A) Selling or sharing the personal information.

(B) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business, or as otherwise permitted by this title.

(C) Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business.

(D) Combining the personal information that the service provider receives from, or on behalf of, the business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that the service provider may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (9) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this section and in regulations adopted by the California Privacy Protection Agency. The contract may, subject to agreement with the service provider, permit the business to monitor the service provider's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

(2) If a service provider engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the service provider engages another person to assist in processing personal information for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

(ah) (1) "Share," "shared," or "sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a

business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

(2) For purposes of this title, a business does not share personal information when:

(A) A consumer uses or directs the business to intentionally disclose personal information or intentionally interact with one or more third parties.

(B) The business uses or shares an identifier for a consumer who has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information.

(C) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this title. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(ai) "Third party" means a person who is not any of the following:

(1) The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the business under this title.

(2) A service provider to the business.

(3) A contractor.

(aj) "Unique identifier" or "unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protoc ol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone

numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device that is linked to a consumer or family. For purposes of this subdivision, "family" means a custodial parent or guardian and any children under 18 years of age over which the parent or guardian has custody.

(ak) "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, or by a person who has power of attorney or is acting as a conservator for the consumer, and that the business can verify, using commercially reasonable methods, pursuant to regulations adopted by the Attorney General pursuant to paragraph 6) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115, to delete personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106, if the business cannot verify, pursuant to this subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

1798.145. Exemptions

(a) (1) The obligations imposed on businesses by this title shall not restrict a business's ability to:

(A) Comply with federal, state, or local laws or comply with a court order or subpoena to provide information.

(B) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities. Law enforcement agencies, including police and sheriff's departments, may direct a business pursuant to a law enforcement agency-approved investigation with an active case number not to delete a consumer's personal information, and, upon receipt of that direction, a business shall not delete the personal information for 90 days in order to allow the law enforcement agency to obtain a court-issued subpoena, order, or warrant to obtain a consumer's personal information. For good cause and only to the extent necessary for investigatory purposes, a law enforcement agency may direct a business not to delete the consumer's personal information for additional 90-day periods. A business that has received direction from a law enforcement agency not to delete the personal information of a consumer who has requested deletion of the consumer's personal information shall not use the consumer's personal information for any purpose other than retaining it to produce to law enforcement in response to a court-issued subpoena, order, or warrant unless the

consumer's deletion request is subject to an exemption from deletion under this title.

(C) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(D) (i) Cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury provided that:

(I) The request is approved by a high-ranking agency officer for emergency access to a consumer's personal information.

(II) The request is based on the agency's good faith determination that it has a lawful basis to access the information on a nonemergency basis.

(III) The agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted.

(ii) For purposes of this subparagraph, a consumer accessing, procuring, or searching for services regarding contraception, pregnancy care, and perinatal care, including, but not limited to, abortion services, shall not constitute a natural person being at risk or danger of death or serious physical injury.

(E) Exercise or defend legal claims.

(F) Collect, use, retain, sell, share, or disclose consumers' personal information that is deidentified or aggregate consumer information.

(G) Collect, sell, or share a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not prohibit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

(2) (A) This subdivision shall not apply if the consumer's personal information contains information related to accessing, procuring, or searching for services

regarding contraception, pregnancy care, and perinatal care, including, but not limited to, abortion services.

(B) This paragraph does not alter the use of aggregated or deidentified personal information consistent with a business purpose as defined in paragraphs (1), (2), (3), (4), (5), (7), or (8) of subdivision (e) of Section 1798.140, provided that the personal information is only retained in aggregated and deidentified form and is not sold or shared.

(C) This paragraph does not alter the duty of a business to preserve or retain evidence pursuant to California or federal law in an ongoing civil proceeding.

(b) The obligations imposed on businesses by Sections 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, and 1798.135 shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c) (1) This title shall not apply to any of the following:

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Personal information collected as part of a clinical trial or other biomedical research study subject to, or conducted in accordance with, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of

the United States Food and Drug Administration, provided that the information is not sold or shared in a manner not permitted by this subparagraph, and, if it is inconsistent, that participants be informed of that use and provide consent.

(2) For purposes of this subdivision, the definitions of "medical information" and "provider of health care" in Section 56.05 shall apply and the definitions of "business associate," "covered entity," and "protected health information" in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) (1) This title shall not apply to an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code.

(2) Paragraph (1) shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, Section 1681 et seq., Title 15 of the United States Code and the information is not collected, maintained, used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting Act.

(3) This subdivision shall not apply to Section 1798.150.

(e) This title shall not apply to personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code), or the federal Farm Credit Act of 1971 (as amended in 12 U.S.C. 2001-2279cc and implementing regulations, 12 C.F.R. 600, et seq.). This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This subdivision shall not apply to Section 1798.150.

(g) (1) Section 1798.120 shall not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer, as defined in Section 426 of the Vehicle Code, and the vehicle's manufacturer, as defined in Section 672 of the Vehicle Code, if the vehicle information or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered

by a vehicle warranty or a recall conducted pursuant to Sections 30118 to 30120, inclusive, of Title 49 of the United States Code, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.

(2) Section 1798.120 shall not apply to vessel information or ownership information retained or shared between a vessel dealer and the vessel's manufacturer, as defined in Section 651 of the Harbors and Navigation Code, if the vessel information or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vessel repair covered by a vessel warranty or a recall conducted pursuant to Section 4310 of Title 46 of the United States Code, provided that the vessel dealer or vessel manufacturer with which that vessel information or ownership information is shared does not sell, share, or use that information for any other purpose.

(3) For purposes of this subdivision:

(A) "Ownership information" means the name or names of the registered owner or owners and the contact information for the owner or owners.

(B) "Vehicle information" means the vehicle information number, make, model, year, and odometer reading.

(C) "Vessel dealer" means a person who is engaged, wholly or in part, in the business of selling or offering for sale, buying or taking in trade for the purpose of resale, or exchanging, any vessel or vessels, as defined in Section 651 of the Harbors and Navigation Code, and receives or expects to receive money, profit, or any other thing of value.

(D) "Vessel information" means the hull identification number, model, year, month and year of production, and information describing any of the following equipment as shipped, transferred, or sold from the place of manufacture, including all attached parts and accessories:

(i) An inboard engine.

(ii) An outboard engine.

(iii) A stern drive unit.

(iv) An inflatable personal floatation device approved under Section 160.076 of Title 46 of the Code of Federal Regulations.

(h) Notwithstanding a business's obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to a consumer for any verifiable consumer request may be extended by up to a total of 90 days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verifiable consumer request is manifestly unfounded or excessive.

(i) (1) A business that discloses personal information to a service provider or contractor in compliance with this title shall not be liable under this title if the service provider or contractor receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider or contractor intends to commit such a violation. A service provider or contractor shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title provided that the service provider or contractor shall be liable for its own violations of this title.

(2) A business that discloses personal information of a consumer, with the exception of consumers who have exercised their right to opt out of the sale or sharing of their personal information, consumers who have limited the use or disclosure of their sensitive personal information, and minor consumers who have not opted in to the collection or sale of their personal information, to a third party pursuant to a written contract that requires the third party to provide the same level of protection of the consumer's rights under this title as provided by the business shall not be liable under this title if the third party receiving the personal information uses it in violation of the restrictions set forth in this title provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the third party intends to commit such a violation.

(j) This title shall not be construed to require a business, service provider, or contractor to:

(1) Reidentify or otherwise link information that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

(2) Retain any personal information about a consumer if, in the ordinary course of business, that information about the consumer would not be retained.

(3) Maintain information in identifiable, linkable, or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with personal information.

(k) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other natural persons. A verifiable consumer request for specific pieces of personal information pursuant to Section 1798.110, to delete a consumer's personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106, shall not extend to personal information about the consumer that belongs to, or the business maintains on behalf of, another natural person. A business may rely on representations made in a verifiable consumer request as to rights with respect to personal information and is under no legal requirement to seek out other persons that may have or claim to have rights to personal information, and a business is under no legal obligation under this title or any other provision of law to take any action under this title in the event of a dispute between or among persons claiming rights to personal information in the business's possession.

(l) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.

(m) (1) This title shall not apply to any of the following:

(A) Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or an independent contractor of, that business.

(B) Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.

(C) Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as a

job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of, that business to the extent that the personal information is collected and used solely within the context of administering those benefits.

(2) For purposes of this subdivision:

(A) "Independent contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as director, or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Medical staff member" means a licensed physician and surgeon, dentist, or podiatrist, licensed pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code and a clinical psychologist as defined in Section 1316.5 of the Health and Safety Code.

(D) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, including a chief executive officer, president, secretary, or treasurer.

(E) "Owner" means a natural person who meets one of the following criteria:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall not apply to subdivision (a) of Section 1798.100 or Section 1798.150.

(4) This subdivision shall become inoperative on January 1, 2023.

(n) (1) The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.121, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who acted or is acting as an employee, owner, director, officer, or independent contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and

whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency.

(2) For purposes of this subdivision:

(A) "Independent contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(D) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall become inoperative on January 1, 2023.

(o) (1) Sections 1798.105 and 1798.120 shall not apply to a commercial credit reporting agency's collection, processing, sale, or disclosure of business controller information to the extent the commercial credit reporting agency uses the business controller information solely to identify the relationship of a consumer to a business that the consumer owns or contact the consumer only in the consumer's role as the owner, director, officer, or management employee of the business.

(2) For the purposes of this subdivision:

(A) "Business controller information" means the name or names of the owner or owners, director, officer, or management employee of a business and the contact information, including a business title, for the owner or owners, director, officer, or management employee.

(B) "Commercial credit reporting agency" has the meaning set forth in subdivision (b) of Section 1785.42.

(C) "Owner" means a natural person that meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(D) "Director" means a natural person designated in the articles of incorporation of a business as director, or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(E) "Officer" means a natural person elected or appointed by the board of directors of a business to manage the daily operations of a corporation, including a chief executive officer, president, secretary, or treasurer.

(F) "Management employee" means a natural person whose name and contact information is reported to or collected by a commercial credit reporting agency as the primary manager of a business and used solely within the context of the natural person's role as the primary manager of the business.

(p) The obligations imposed on businesses in Sections 1798.105, 1798.106, 1798.110, and 1798.115 shall not apply to household data.

(q) (1) This title does not require a business to comply with a verifiable consumer request to delete a consumer's personal information under Section 1798.105 to the extent the verifiable consumer request applies to a student's grades, educational scores, or educational test results that the business holds on behalf of a local educational agency, as defined in subdivision (d) of Section 49073.1 of the Education Code, at which the student is currently enrolled. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception.

(2) This title does not require, in response to a request pursuant to Section 1798.110, that a business disclose on educational standardized assessment or educational assessment or a consumer's specific responses to the educational standardized assessment or educational assessment if consumer access, possession, or control would jeopardize the validity and reliability of that educational standardized assessment or educational assessment. If a business does not comply with a request

pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception.

(3) For purposes of this subdivision:

(A) "Educational standardized assessment or educational assessment" means a standardized or nonstandardized quiz, test, or other assessment used to evaluate students in or for entry to kindergarten and grades 1 to 12, inclusive, schools, postsecondary institutions, vocational programs, and postgraduate programs that are accredited by an accrediting agency or organization recognized by the State of California or the United States Department of Education, as well as certification and licensure examinations used to determine competency and eligibility to receive certification or licensure from a government agency or government certification body.

(B) "Jeopardize the validity and reliability of that educational standardized assessment or educational assessment" means releasing information that would provide an advantage to the consumer who has submitted a verifiable consumer request or to another natural person.

(r) Sections 1798.105 and 1798.120 shall not apply to a business's use, disclosure, or sale of particular pieces of a consumer's personal information if the consumer has consented to the business's use, disclosure, or sale of that information to produce a physical item, including a school yearbook containing the consumer's photograph if:

(1) The business has incurred significant expense in reliance on the consumer's consent.

(2) Compliance with the consumer's request to opt out of the sale of the consumer's personal information or to delete the consumer's personal information would not be commercially reasonable.

(3) The business complies with the consumer's request as soon as it is commercially reasonable to do so.

1798.146.

(a) This title shall not apply to any of the following:

(1) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the federal

Health Information Technology for Economic and Clinical Health Act, Title XIII of the federal American Recovery and Reinvestment Act of 2009 (Public Law 111-5).

(2) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains, uses, and discloses patient information in the same manner as medical information or protected health information as described in paragraph (1).

(3) A business associate of a covered entity governed by the privacy, security, and data breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the federal Health Information Technology for Economic and Clinical Health Act, Title XIII of the federal American Recovery and Reinvestment Act of 2009 (Public Law 111-5), to the extent that the business associate maintains, uses, and discloses patient information in the same manner as medical information or protected health information as described in paragraph (1).

(4) (A) Information that meets both of the following conditions:

(i) It is deidentified in accordance with the requirements for deidentification set forth in Section 164.514 of Part 164 of Title 45 of the Code of Federal Regulations.

(ii) It is derived from patient information that was originally collected, created, transmitted, or maintained by an entity regulated by the Health Insurance Portability and Accountability Act, the Confidentiality Of Medical Information Act, or the Federal Policy for the Protection of Human Subjects, also known as the Common Rule.

(B) Information that met the requirements of subparagraph (A) but is subsequently reidentified shall no longer be eligible for the exemption in this paragraph, and shall be subject to applicable federal and state data privacy and security laws, including, but not limited to, the Health Insurance Portability and Accountability Act, the Confidentiality Of Medical Information Act, and this title.

(5) Information that is collected, used, or disclosed in research, as defined in Section 164.501 of Title 45 of the Code of Federal Regulations, including, but not limited to, a clinical trial, and that is conducted in accordance with applicable ethics,

confidentiality, privacy, and security rules of Part 164 of Title 45 of the Code of Federal Regulations, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, good clinical practice guidelines issued by the International Council for Harmonisation, or human subject protection requirements of the United States Food and Drug Administration.

(b) For purposes of this section, all of the following shall apply:

(1) "Business associate" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(2) "Covered entity" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(3) "Identifiable private information" has the same meaning as defined in Section 46.102 of Title 45 of the Code of Federal Regulations.

(4) "Individually identifiable health information" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(5) "Medical information" has the same meaning as defined in Section 56.05.

(6) "Patient information" shall mean identifiable private information, protected health information, individually identifiable health information, or medical information.

(7) "Protected health information" has the same meaning as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(8) "Provider of health care" has the same meaning as defined in Section 56.05.

1798.148.

(a) A business or other person shall not reidentify, or attempt to reidentify, information that has met the requirements of paragraph (4) of subdivision (a) of Section 1798.146, except for one or more of the following purposes:

(1) Treatment, payment, or health care operations conducted by a covered entity or business associate acting on behalf of, and at the written direction of, the covered entity. For purposes of this paragraph, "treatment," "payment," "health care operations," "covered entity," and "business associate" have the same meaning as defined in Section 164.501 of Title 45 of the Code of Federal Regulations.

(2) Public health activities or purposes as described in Section 164.512 of Title 45 of the Code of Federal Regulations.

(3) Research, as defined in Section 164.501 of Title 45 of the Code of Federal Regulations, that is conducted in accordance with Part 46 of Title 45 of the Code of Federal Regulations, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule.

(4) Pursuant to a contract where the lawful holder of the deidentified information that met the requirements of paragraph (4) of subdivision (a) of Section 1798.146 expressly engages a person or entity to attempt to reidentify the deidentified information in order to conduct testing, analysis, or validation of deidentification, or related statistical techniques, if the contract bans any other use or disclosure of the reidentified information and requires the return or destruction of the information that was reidentified upon completion of the contract.

(5) If otherwise required by law.

(b) In accordance with paragraph (4) of subdivision (a) of Section 1798.146, information reidentified pursuant this section shall be subject to applicable federal and state data privacy and security laws including, but not limited to, the Health Insurance Portability and Accountability Act, the Confidentiality of Medical Information Act, and this title.

(c) Beginning January 1, 2021, any contract for the sale or license of deidentified information that has met the requirements of paragraph (4) of subdivision (a) of Section 1798.146, where one of the parties is a person residing or doing business in the state, shall include the following, or substantially similar, provisions:

(1) A statement that the deidentified information being sold or licensed includes deidentified patient information.

(2) A statement that reidentification, and attempted reidentification, of the deidentified information by the purchaser or licensee of the information is prohibited pursuant to this section.

(3) A requirement that, unless otherwise required by law, the purchaser or licensee of the deidentified information may not further disclose the deidentified information to any third party unless the third party is contractually bound by the same or stricter restrictions and conditions.

(d) For purposes of this section, “reidentify” means the process of reversal of deidentification techniques, including, but not limited to, the addition of specific pieces of information or data elements that can, individually or in combination, be used to uniquely identify an individual or usage of any statistical method, contrivance, computer software, or other means that have the effect of associating deidentified information with a specific identifiable individual.

1798.150. Personal Information Security Breaches

(a) (1) Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, or whose email address in combination with a password or security question and answer that would permit access to the account is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars ($100)* and not greater than seven hundred and fifty ($750)* per consumer per incident or actual damages, whichever is greater. The amounts in this subdivision shall be adjusted pursuant to subdivision (d) of Section 1798.199.95.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

* Pursuant to Civil Code § 1798.199.95(d), this monetary amount has been updated. Please see updated amount.

(b) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. The implementation and maintenance of reasonable security procedures and practices pursuant to Section 1798.81.5 following a breach does not constitute a cure with respect to that breach. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement

provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

(c) The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

1798.155. Administrative Enforcement

(a) Any business, service provider, contractor, or other person that violates this title shall be liable for an administrative fine of not more than two thousand five hundred dollars ($2,500)* for each violation or seven thousand five hundred dollars ($7,500)* for each intentional violation or violations involving the personal information of consumers whom the business, service provider, contractor, or other person has actual knowledge are under 16 years of age, as adjusted pursuant to subdivision (d) of Section 1798.199.95, in an administrative enforcement action brought by the California Privacy Protection Agency.

(b) (1) Ninety-five percent of any administrative fine assessed for a violation of this title, and of the proceeds of any settlement of an action brought pursuant to subdivision (a), shall be deposited into the Consumer Privacy Subfund created within the Consumer Privacy Fund pursuant to subdivision (b) of Section 1798.160, and shall be

* Pursuant to Civil Code § 1798.199.95(d), this monetary amount has been updated. Please see updated amount.

used exclusively by the California Privacy Protection Agency in carrying out its duties under this title.

(2) Five percent of any administrative fine assessed for a violation of this title, and of the proceeds of any settlement of an action brought pursuant to subdivision (a), shall be deposited into the Consumer Privacy Grant Subfund created within the Consumer Privacy Fund pursuant to subdivision (d) of Section 1798.160.

1798.160. Consumer Privacy Fund

(a) (1) A special fund to be known as the "Consumer Privacy Fund" is hereby created within the General Fund in the State Treasury, and is available upon appropriation by the Legislature.

(2) Funds in the Consumer Privacy Fund and all subfunds within the fund shall be used exclusively for the purposes described in this section and shall not be subject to

appropriation or transfer by the Legislature for any other purpose. Any interest and

earnings from the fund and all subfunds within the fund shall be transferred on an annual basis to the State Treasury to be available in the General Fund for appropriation by the Legislature.

(b) (1) The Consumer Privacy Subfund is hereby created within the Consumer Privacy Fund and is available upon appropriation by the Legislature. Funds in the Consumer Privacy Subfund shall be used exclusively for the purposes described in this subdivision.

(2) Ninety-five percent of any administrative fine recovered in an action brought by the California Privacy Protection Agency for a violation of this title shall be deposited into the Consumer Privacy Subfund and shall be used exclusively by the California Privacy Protection Agency in carrying out its duties under this title.

(c) (1) The Attorney General Consumer Privacy Enforcement Subfund is hereby created within the Consumer Privacy Fund and is available upon appropriation by the Legislature. Funds in the Attorney General Consumer Privacy Enforcement Subfund shall be used exclusively for the purposes described in this subdivision.

(2) Ninety-five percent of any civil penalty recovered in an action brought by the Attorney General for a violation of this title shall be deposited into the Attorney General Consumer Privacy Enforcement Subfund and shall be used exclusively by the Attorney General in carrying out its duties under this title.

(d) The Consumer Privacy Grant Subfund is hereby created within the Consumer Privacy Fund and is available upon appropriation by the Legislature. Funds in the Consumer Privacy Subfund shall be used exclusively for the purposes described in this subdivision.

(1) (A) Five percent of any administrative fine recovered in an action brought by the California Privacy Protection Agency for a violation of this title shall be deposited into the Consumer Privacy Grant Subfund.

(B) Five percent of any civil penalty recovered in an action brought by the Attorney General for a violation of this title shall be deposited into the Consumer Privacy Grant Subfund.

(2) (A) Funds deposited into the Consumer Privacy Grant Subfund shall be used exclusively by the California Privacy Protection Agency to administer and distribute grants to promote and protect consumer privacy, educate children in the area of online privacy, and fund cooperative programs with international law enforcement organizations to combat fraudulent activities with respect to consumer data breaches.

(B) Subject to subparagraph (A), the California Privacy Protection Agency shall make grants from the Consumer Privacy Grant Subfund by distributing one-

third of the amount allocated for grant funding in the subfund to each of the following grant recipients:

(i) Nonprofit organizations to promote and protect consumer privacy.

(ii) Nonprofit organizations and public agencies, including school districts, to educate children in the area of online privacy.

(iii) State and local law enforcement agencies to fund cooperative programs with international law enforcement organizations to combat fraudulent activities with respect to consumer data breaches.

(3) (A) The California Privacy Protection Agency shall begin administering the grant program described in paragraph (2) when the amount of funds in the Consumer Privacy Grant Subfund exceeds three hundred thousand dollars ($300,000).

(B) In a fiscal year in which the amount of funds in the Consumer Privacy Grant Subfund is equal to or less than three hundred thousand dollars ($300,000), the funds shall remain in the Consumer Privacy Grant Subfund until the total funds exceed three hundred thousand dollars ($300,000).

(e) Any remaining funds in the Consumer Privacy Fund and subfunds within the fund that were not appropriated as part of the 2025 Budget Act shall be transferred on a one-time basis in the 2025–26 fiscal year as follows:

(1) Forty-five percent of the remaining funds shall be transferred to the Consumer Privacy Subfund created within the Consumer Privacy Fund pursuant to subdivision (b).

(2) Forty-five percent of the remaining funds shall be transferred to the Attorney General Consumer Privacy Enforcement Subfund created within the Consumer Privacy Fund pursuant to subdivision (c).

(3) Ten percent of the remaining funds shall be transferred to the Consumer Privacy Grant Subfund created within the Consumer Privacy Fund pursuant to subdivision (d) of Section 1798.160.

1798.175. Conflicting Provisions

This title is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80). The provisions of this title are not limited to information collected electronically or over the Internet, but apply to the collection and sale of all personal information collected by a business from consumers. Wherever possible, law

relating to consumers' personal information should be construed to harmonize with the provisions of this title, but in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

1798.180. Preemption

This title is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers' personal information by a business.

1798.185. Regulations

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

(1) Updating or adding categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (v) of Section 1798.140, and updating or adding categories of sensitive personal information to those enumerated in subdivision (ae) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Updating as needed the definitions of "deidentified" and "unique identifier" to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and adding, modifying, or deleting categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to Section 1798.130. The authority to update the definition of "deidentified" shall not apply to deidentification standards set forth in Section 164.514 of Title 45 of the Code of Federal Regulations, where such information previously was "protected health information" as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter, with the intention that trade secrets should not be disclosed in response to a verifiable consumer request.

(4) Establishing rules and procedures for the following:

(A) To facilitate and govern the submission of a request by a consumer to opt out of the sale or sharing of personal information pursuant to Section 1798.120 and to limit the use of a consumer's sensitive personal information pursuant to

Section 1798.121 to ensure that consumers have the ability to exercise their choices without undue burden and to prevent business from engaging in deceptive or harassing conduct, including in retaliation against consumers for exercising their rights, while allowing businesses to inform consumers of the consequences of their decision to opt out of the sale or sharing of their personal information or to limit the use of their sensitive personal information.

(B) To govern business compliance with a consumer's opt-out request.

(C) For the development and use of a recognizable and uniform opt out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

(5) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentives within one year of passage of this title and as needed thereafter.

(6) Establishing rules and procedures to further the purposes of Sections 1798.105, 1798.106, 1798.110, and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to delete personal information, correct inaccurate personal information pursuant to Section 1798.106, or obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business' determination that a request for information received from a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business' authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

(7) Establishing how often, and under what circumstances, a consumer may request a correction pursuant to Section 1798.106, including standards governing the following:

(A) How a business responds to a request for correction, including exceptions for requests to which a response is impossible or would involve disproportionate effort, and requests for correction of accurate information.

(B) How concerns regarding the accuracy of the information may be resolved.

(C) The steps a business may take to prevent fraud.

(D) If a business rejects a request to correct personal information collected and analyzed concerning a consumer's health, the right of a consumer to provide a written addendum to the business with respect to any item or statement regarding any such personal information that the consumer believes to be incomplete or incorrect. The addendum shall be limited to 250 words per alleged incomplete or incorrect item and shall clearly indicate in writing that the consumer requests the addendum to be made a part of the consumer's record.

(8) Establishing the standard to govern a business' determination, pursuant to subparagraph (B) of paragraph (2) of subdivision (a) of Section 1798.130, that providing information beyond the 12-month period in a response to a verifiable consumer request is impossible or would involve a disproportionate effort.

(9) Issuing regulations further defining and adding to the business purposes, including other notified purposes, for which businesses, service providers, and contractors may use consumers' personal information consistent with consumers' expectations, and further defining the business purposes for which service providers and contractors may combine consumers' personal information obtained from different sources, except as provided for in paragraph (6) of subdivision (e) of Section 1798.140.

(10) Issuing regulations identifying those business purposes, including other notified purposes, for which service providers and contractors may use consumers' personal information received pursuant to a written contract with a business, for the service provider or contractor's own business purposes, with the goal of maximizing consumer privacy.

(11) Issuing regulations to further define "intentionally interacts," with the goal of maximizing consumer privacy.

(12) Issuing regulations to further define "precise geolocation," including if the size defined is not sufficient to protect consumer privacy in sparsely populated areas or when the personal information is used for normal operational purposes, including billing.

(13) Issuing regulations to define the term "specific pieces of information obtained from the consumer" with the goal of maximizing a consumer's right to access relevant personal information while minimizing the delivery of information to a consumer that would not be useful to the consumer, including system log information and other technical data. For delivery of the most sensitive personal information, the regulations may require a higher standard of authentication provided that the agency shall monitor the impact of the higher standard on the right of consumers to

obtain their personal information to ensure that the requirements of verification do not result in the unreasonable denial of verifiable consumer requests.

(14) Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to:

(A) Perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities.

(B) Submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public. Nothing in this section shall require a business to divulge trade secrets.

(15) Issuing regulations governing access and opt-out rights with respect to a business' use of automated decisionmaking technology, including profiling and requiring a business' response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.

(16) Issuing regulations to further define a "law enforcement agency-approved investigation" for purposes of the exception in subparagraph (B) of paragraph (1) of subdivision (a) of Section 1798.145.

(17) Issuing regulations to define the scope and process for the exercise of the agency's audit authority, to establish criteria for selection of persons to audit, and to protect consumers' personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena.

(18) (A) Issuing regulations to define the requirements and technical specifications for an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer's intent to opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information. The requirements and specifications for the

opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should:

(i) Ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business.

(ii) Ensure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer and does not require that the consumer provide additional information beyond what is necessary.

(iii) Clearly represent a consumer's intent and be free of defaults constraining or presupposing that intent.

(iv) Ensure that the opt-out preference signal does not conflict with other commonly used privacy settings or tools that consumers may employ.

(v) Provide a mechanism for the consumer to selectively consent to a business' sale of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, without affecting the consumer's preferences with respect to other businesses or disabling the opt-out preference signal globally.

(vi) State that in the case of a page or setting view that the consumer accesses to set the opt-out preference signal, the consumer should see up to three choices, including:

(I) Global opt out from sale and sharing of personal information, including a direction to limit the use of sensitive personal information.

(II) Choice to "Limit the Use of My Sensitive Personal Information."

(III) Choice titled "Do Not Sell/Do Not Share My Personal Information for Cross-Context Behavioral Advertising."

(B) Issuing regulations to establish technical specifications for an opt-out preference signal that allows the consumer, or the consumer's parent or guardian, to specify that the consumer is less than 13 years of age or at least 13 years of age and less than 16 years of age.

(C) Issuing regulations, with the goal of strengthening consumer privacy while considering the legitimate operational interests of businesses, to govern the use or disclosure of a consumer's sensitive personal information,

notwithstanding the consumer's direction to limit the use or disclosure of the consumer's sensitive personal information, including:

(i) Determining any additional purposes for which a business may use or disclose a consumer's sensitive personal information.

(ii) Determining the scope of activities permitted under paragraph (8) of subdivision (e) of Section 1798.140, as authorized by subdivision (a) of Section 1798.121, to ensure that the activities do not involve health-related research.

(iii) Ensuring the functionality of the business' operations.

(iv) Ensuring that the exemption in subdivision (d) of Section 1798.121 for sensitive personal information applies to information that is collected or processed incidentally, or without the purpose of inferring characteristics about a consumer, while ensuring that businesses do not use the exemption for the purpose of evading consumers' rights to limit the use and disclosure of their sensitive personal information under Section 1798.121.

(19) Issuing regulations to govern how a business that has elected to comply with subdivision (b) of Section 1798.135 responds to the opt-out preference signal and provides consumers with the opportunity subsequently to consent to the sale or sharing of their personal information or the use and disclosure of their sensitive personal information for purposes in addition to those authorized by subdivision (a) of Section 1798.121. The regulations should:

(A) Strive to promote competition and consumer choice and be technology neutral.

(B) Ensure that the business does not respond to an opt-out preference signal by:

(i) Intentionally degrading the functionality of the consumer experience.

(ii) Charging the consumer a fee in response to the consumer's opt-out preferences.

(iii) Making any products or services not function properly or fully for the consumer, as compared to consumers who do not use the opt-out preference signal.

(iv) Attempting to coerce the consumer to opt in to the sale or sharing of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, by stating or implying that the use of the opt-out preference signal will adversely affect the consumer as compared to consumers who do not use the opt-out preference signal,

including stating or implying that the consumer will not be able to use the business' products or services or that those products or services may not function properly or fully.

(v) Displaying any notification or pop-up in response to the consumer's opt-out preference signal.

(C) Ensure that any link to a web page or its supporting content that allows the consumer to consent to opt in:

(i) Is not part of a popup, notice, banner, or other intrusive design that obscures any part of the web page the consumer intended to visit from full view or that interferes with or impedes in any way the consumer's experience visiting or browsing the web page or internet website the consumer intended to visit.

(ii) Does not require or imply that the consumer must click the link to receive full functionality of any products or services, including the internet website.

(iii) Does not make use of any dark patterns.

(iv) Applies only to the business with which the consumer intends to interact.

(D) Strive to curb coercive or deceptive practices in response to an opt-out preference signal but should not unduly restrict businesses that are trying in good faith to comply with Section 1798.135.

(20) Review existing Insurance Code provisions and regulations relating to consumer privacy, except those relating to insurance rates or pricing, to determine whether any provisions of the Insurance Code provide greater protection to consumers than the provisions of this title. Upon completing its review, the agency shall adopt a regulation that applies only the more protective provisions of this title to insurance companies. For the purpose of clarity, the Insurance Commissioner shall have jurisdiction over insurance rates and pricing.

(21) Harmonizing the regulations governing opt-out mechanisms, notices to consumers, and other operational mechanisms in this title to promote clarity and the functionality of this title for consumers.

(b) The Attorney General may adopt additional regulations as necessary to further the purposes of this title.

(c) The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.

(d) Notwithstanding subdivision (a), the timeline for adopting final regulations required by the act adding this subdivision shall be July 1, 2022. Beginning the later of July 1, 2021, or six months after the agency provides notice to the Attorney General that it is prepared to begin rulemaking under this title, the authority assigned to the Attorney General to adopt regulations under this section shall be exercised by the California Privacy Protection Agency. Notwithstanding any other law, civil and administrative enforcement of the provisions of law added or amended by this act shall not commence until July 1, 2023, and shall only apply to violations occurring on or after that date. Enforcement of provisions of law contained in the California Consumer Privacy Act of 2018 amended by this act shall remain in effect and shall be enforceable until the same provisions of this act become enforceable.

1798.190. Anti-Avoidance

A court or the agency shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title:

(a) If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell or share.

(b) If steps or transactions were taken to purposely avoid the definition of sell or share by eliminating any monetary or other valuable consideration, including by entering into contracts that do not include an exchange for monetary or other valuable consideration, but where a party is obtaining something of value or use.

1798.192. Waiver

Any provision of a contract or agreement of any kind, including a representative action waiver, that purports to waive or limit in any way rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt out of a business's sale of the consumer's personal information, or authorizing a business to sell or share the consumer's personal information after previously opting out.

1798.194.

This title shall be liberally construed to effectuate its purposes.

1798.196.

This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.

1798.198.

(a) Subject to limitation provided in subdivision (b), and in Section 1798.199, this title shall be operative January 1, 2020.

(b) This title shall become operative only if initiative measure No. 17-0039, The Consumer Right to Privacy Act of 2018, is withdrawn from the ballot pursuant to Section 9604 of the Elections Code.

1798.199.

Notwithstanding Section 1798.198, Section 1798.180 shall be operative on the effective date of the act adding this section.

1798.199.10.

(a) There is hereby established in state government the California Privacy Protection Agency, which is vested with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018. The agency shall be governed by a five-member board, including the chairperson. The chairperson and one member of the board shall be appointed by the Governor. The Attorney General, Senate Rules Committee, and Speaker of the Assembly shall each appoint one member. These appointments should be made from among Californians with expertise in the areas of privacy, technology, and consumer rights.

(b) The initial appointments to the agency shall be made within 90 days of the effective date of the act adding this section.

1798.199.15.

Members of the agency board shall:

(a) Have qualifications, experience, and skills, in particular in the areas of privacy and technology, required to perform the duties of the agency and exercise its powers.

(b) Maintain the confidentiality of information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers, except to the extent that disclosure is required by the Public Records Act.

(c) Remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from another.

(d) Refrain from any action incompatible with their duties and engaging in any incompatible occupation, whether gainful or not, during their term.

(e) Have the right of access to all information made available by the agency to the chairperson.

(f) Be precluded, for a period of one year after leaving office, from accepting employment with a business that was subject to an enforcement action or civil action under this title during the member's tenure or during the five-year period preceding the member's appointment.

(g) Be precluded for a period of two years after leaving office from acting, for compensation, as an agent or attorney for, or otherwise representing, any other person in a matter pending before the agency if the purpose is to influence an action of the agency.

1798.199.20.

Members of the agency board, including the chairperson, shall serve at the pleasure of their appointing authority but shall serve for no longer than eight consecutive years.

1798.199.25.

For each day on which they engage in official duties, members of the agency board shall be compensated at the rate of one hundred dollars ($100)*, adjusted pursuant to subdivision (d) of Section 1798.199.95, and shall be reimbursed for expenses incurred in performance of their official duties.

* Pursuant to Civil Code § 1798.199.95(d), this monetary amount has been updated. Please see updated amount.

1798.199.30.

The agency board shall appoint an executive director who shall act in accordance with agency policies and regulations and with applicable law. The agency shall appoint and discharge officers, counsel, and employees, consistent with applicable civil service laws, and shall fix the compensation of employees and prescribe their duties. The agency may contract for services that cannot be provided by its employees.

1798.199.35.

The agency board may delegate authority to the chairperson or the executive director to act in the name of the agency between meetings of the agency, except with respect to resolution of enforcement actions and rulemaking authority.

1798.199.40.

The agency shall perform the following functions:

(a) Administer, implement, and enforce through administrative actions this title.

(b) On and after the later of July 1, 2021, or within six months of the agency providing the Attorney General with notice that it is prepared to assume rulemaking responsibilities under this title, adopt, amend, and rescind regulations pursuant to Section 1798.185 to carry out the purposes and provisions of the California Consumer Privacy Act of 2018, including regulations specifying recordkeeping requirements for businesses to ensure compliance with this title.

(c) Through the implementation of this title, protect the fundamental privacy rights of natural persons with respect to the use of their personal information.

(d) Promote public awareness and understanding of the risks, rules, responsibilities, safeguards, and rights in relation to the collection, use, sale, and disclosure of personal information, including the rights of minors with respect to their own information, and provide a public report summarizing the risk assessments filed with the agency pursuant to paragraph (14) of subdivision (a) of Section 1798.185 while ensuring that data security is not compromised.

(e) Provide guidance to consumers regarding their rights under this title.

(f) Provide guidance to businesses regarding their duties and responsibilities under this title and appoint a Chief Privacy Auditor to conduct audits of businesses to ensure compliance with this title pursuant to regulations adopted pursuant to paragraph (17) of subdivision (a) of Section 1798.185.

(g) Provide technical assistance and advice to the Legislature, upon request, with respect to privacy-related legislation.

(h) Monitor relevant developments relating to the protection of personal information and, in particular, the development of information and communication technologies and commercial practices.

(i) Cooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections.

(j) Establish a mechanism pursuant to which persons doing business in California that do not meet the definition of business set forth in paragraph (1), (2), or (3) of subdivision (d) of Section 1798.140 may voluntarily certify that they are in compliance with this title, as set forth in paragraph (4) of subdivision (d) of Section 1798.140, and make a list of those entities available to the public.

(k) Solicit, review, and approve applications for grants to the extent funds are available pursuant to paragraph (2) of subdivision (b) of Section 1798.160.

(l) Perform all other acts necessary or appropriate in the exercise of its power, authority, and jurisdiction and seek to balance the goals of strengthening consumer privacy while giving attention to the impact on businesses.

1798.199.45.

(a) Upon the sworn complaint of any person or on its own initiative, the agency may investigate possible violations of this title relating to any business, service provider, contractor, or person. The agency may decide not to investigate a complaint or decide to provide a business with a time period to cure the alleged violation. In making a decision not to investigate or provide more time to cure, the agency may consider the following:

(1) Lack of intent to violate this title.

(2) Voluntary efforts undertaken by the business, service provider, contractor, or person to cure the alleged violation prior to being notified by the agency of the complaint.

(b) (1) The agency shall notify in writing the person who made the complaint 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.

(2) The written notification required by this subdivision shall not include information that is subject to law enforcement exemptions and privileges, including, but not limited to, confidential information related to an investigation and information that is privileged under the Evidence Code and the Government Code.

1798.199.50.

No finding of probable cause to believe this title has been violated shall be made by the agency unless, at least 30 days prior to the agency's consideration of the alleged violation, the business, service provider, contractor, or person alleged to have violated this title is notified of the violation by service of process or registered mail with return receipt requested, provided with a summary of the evidence, and informed of their right to be present in person and represented by counsel at any proceeding of the agency held for the purpose of considering whether probable cause exists for believing the person violated this title. Notice to the alleged violator shall be deemed made on the date of service, the date the registered mail receipt is signed, or if the registered mail receipt is not signed, the date returned by the post office. A proceeding held for the purpose of considering probable cause shall be private unless the alleged violator files with the agency a written request that the proceeding be public.

1798.199.55.

(a) When the agency determines there is probable cause for believing this title has been violated, it shall hold a hearing to determine if a violation has or violations have occurred. Notice shall be given and the hearing conducted in accordance with the Administrative Procedure Act (Chapter 5 (commencing with Section 11500), of Part 1 of Division 3 of Title

2 of the Government Code). The agency shall have all the powers granted by that chapter. If the agency determines on the basis of the hearing conducted pursuant to this subdivision that a violation or violations have occurred, it shall issue an order that may require the violator to do all or any of the following:

(1) Cease and desist violation of this title.

(2) Subject to Section 1798.155, pay an administrative fine of up to two thousand five hundred dollars ($2,500) for each violation, or up to seven thousand five hundred dollars ($7,500) for each intentional violation and each violation involving the personal information of minor consumers. When the agency determines that no violation has occurred, it shall publish a declaration so stating.

(A) Ninety-five percent of any administrative fine assessed pursuant to this paragraph shall be deposited into the Consumer Privacy Subfund created within the Consumer Privacy Fund pursuant to subdivision (b) of Section 1798.160.

(B) Five percent of any administrative fine assessed pursuant to this paragraph shall be deposited into the Consumer Privacy Grant Subfund created within the Consumer Privacy Fund pursuant to subdivision (d) of Section 1798.160.

(b) If two or more persons are responsible for any violation or violations, they shall be jointly and severally liable.

1798.199.60.

Whenever the agency rejects the decision of an administrative law judge made pursuant to Section 11517 of the Government Code, the agency shall state the reasons in writing for rejecting the decision.

1798.199.65.

The agency may subpoena witnesses, compel their attendance and testimony, administer oaths and affirmations, take evidence and require by subpoena the production of any books, papers, records, or other items material to the performance of the agency's duties or exercise of its powers, including, but not limited to, its power to audit a business' compliance with this title.

1798.199.70.

No administrative action brought pursuant to this title alleging a violation of any of the provisions of this title shall be commenced more than five years after the date on which the violation occurred.

(a) The service of the probable cause hearing notice, as required by Section 1798.199.50, upon the person alleged to have violated this title shall constitute the commencement of the administrative action.

(b) If the person alleged to have violated this title engages in the fraudulent concealment of the person's acts or identity, the five-year period shall be tolled for the period of the concealment. For purposes of this subdivision, "fraudulent concealment" means the person knows of material facts related to the person's duties under this title and knowingly conceals them in performing or omitting to perform those duties for the purpose of defrauding the public of information to which it is entitled under this title.

(c) If, upon being ordered by a superior court to produce any documents sought by a subpoena in any administrative proceeding under this title, the person alleged to have violated this title fails to produce documents in response to the order by the date ordered to comply therewith, the five-year period shall be tolled for the period of the delay from the date of filing of the motion to compel until the date the documents are produced.

1798.199.75.

(a) In addition to any other available remedies, the agency may bring a civil action and obtain a judgment in superior court for the purpose of collecting any unpaid administrative fines imposed pursuant to this title after exhaustion of judicial review of the agency's action. The action may be filed as a small claims, limited civil, or unlimited civil case depending on the jurisdictional amount. The venue for this action shall be in the county where the administrative fines were imposed by the agency. In order to obtain a judgment in a proceeding under this section, the agency shall show, following the procedures and rules of evidence as applied in ordinary civil actions, all of the following:

    (1) That the administrative fines were imposed following the procedures set forth in this title and implementing regulations.

    (2) That the defendant or defendants in the action were notified, by actual or constructive notice, of the imposition of the administrative fines.

    (3) That a demand for payment has been made by the agency and full payment has not been received.

(b) A civil action brought pursuant to subdivision (a) shall be commenced within four years after the date on which the administrative fines were imposed.

1798.199.80.

(a) If the time for judicial review of a final agency order or decision has lapsed, or if all means of judicial review of the order or decision have been exhausted, the agency may apply to the clerk of the court for a judgment to collect the administrative fines imposed by the

order or decision, or the order as modified in accordance with a decision on judicial review.

(b) The application, which shall include a certified copy of the order or decision, or the order as modified in accordance with a decision on judicial review, and proof of service of the order or decision, constitutes a sufficient showing to warrant issuance of the judgment to collect the administrative fines. The clerk of the court shall enter the judgment immediately in conformity with the application.

(c) An application made pursuant to this section shall be made to the clerk of the superior court in the county where the administrative fines were imposed by the agency.

(d) A judgment entered in accordance with this section has the same force and effect as, and is subject to all the provisions of law relating to, a judgment in a civil action and may be enforced in the same manner as any other judgment of the court in which it is entered.

(e) The agency may bring an application pursuant to this section only within four years after the date on which all means of judicial review of the order or decision have been exhausted.

(f) The remedy available under this section is in addition to those available under any other law.

1798.199.85.

Any decision of the agency with respect to a complaint or administrative fine shall be subject to judicial review in an action brought by an interested party to the complaint or administrative fine and shall be subject to an abuse of discretion standard.

1798.199.90.

(a) Any business, service provider, contractor, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation and each violation involving the personal information of minor consumers, as adjusted pursuant to subdivision (d) of Section 1798.199.95, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The court may consider the good faith cooperation of the business, service provider, contractor, or other person in determining the amount of the civil penalty.

(b) (1) (A) Ninety-five percent of any civil penalty recovered by an action brought by the Attorney General for a violation of this title, and of the proceeds of any settlement of those actions, shall be deposited into the Attorney General Consumer Privacy Enforcement Subfund created within the Consumer Privacy

Fund pursuant to subdivision (c) of Section 1798.160 to support the Attorney General in the enforcement of this title.

(B) Notwithstanding any provision to the contrary, the Attorney General may, if an action or settlement is the result of a joint investigation with the agency, deposit a portion of the penalties and proceeds that would otherwise be subject to subparagraph (A) into the Consumer Privacy Subfund created within the Consumer Privacy Fund pursuant to subdivision (b) of Section 1798.160 in the amount necessary to provide reimbursement for investigative costs.

(2) Five percent of any civil penalty recovered by an action brought by the Attorney General for a violation of this title, and of the proceeds of any settlement of those actions, shall be deposited into the Consumer Privacy Grant Subfund created within the Consumer Privacy Fund pursuant to subdivision (d) of Section 1798.160.

(c) The agency shall, upon request by the Attorney General, stay an administrative action or investigation under this title to permit the Attorney General to proceed with an investigation or civil action and shall not pursue an administrative action or investigation, unless the Attorney General subsequently determines not to pursue an investigation or civil action. The agency may not limit the authority of the Attorney General to enforce this title.

(d) No civil action may be filed by the Attorney General under this section for any violation of this title after the agency has issued a decision pursuant to Section 1798.199.85 or an order pursuant to Section 1798.199.55 against that person for the same violation.

(e) This section shall not affect the private right of action provided for in Section 1798.150.

1798.199.95.

(a) There is hereby appropriated from the General Fund of the state to the agency the sum of five million dollars ($5,000,000) during the fiscal year 2020–21, and the sum of ten million dollars ($10,000,000) adjusted for cost-of-living changes, during each fiscal year thereafter, for expenditure to support the operations of the agency pursuant to this title. The expenditure of funds under this appropriation shall be subject to the normal administrative review given to other state appropriations. The Legislature shall appropriate those additional amounts to the commission and other agencies as may be necessary to carry out the provisions of this title.

(b) The Department of Finance, in preparing the state budget and the Budget Act bill submitted to the Legislature, shall include an item for the support of this title that shall indicate all of the following:

(1) The amounts to be appropriated to other agencies to carry out their duties under this title, which amounts shall be in augmentation of the support items of those agencies.

(2) The additional amounts required to be appropriated by the Legislature to the agency to carry out the purposes of this title, as provided for in this section.

(3) In parentheses, for informational purposes, the continuing appropriation during each fiscal year of ten million dollars ($10,000,000), adjusted for cost-of-living changes made pursuant to this section.

(c) The Attorney General shall provide staff support to the agency until the agency has hired its own staff. The Attorney General shall be reimbursed by the agency for these services.

(d) (1) On January 1, 2025, and on January 1 of any odd-numbered year thereafter, the California Privacy Protection Agency shall adjust the monetary thresholds in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.140, subparagraph (A) of paragraph (1) of subdivision (a) of Section 1798.150, subdivision (a) of Section 1798.155, Section 1798.199.25, and subdivision (a) of Section 1798.199.90 to reflect any increase in the Consumer Price Index.

(2) The agency shall use the Consumer Price Index (CPI)—California, All Items, All Urban Consumers percentage change from the previous two years' reports, published by the Department of Industrial Relations, Office of the Director–Research. The agency shall apply the percentage change in the CPI for the August-to-August point in time of the prior two years. The increase in the thresholds shall be rounded to the nearest whole dollar.

(3) The agency shall post the adjusted monetary thresholds on its internet website no later than January 15 of the year in which the adjustment becomes effective.

(4) Notwithstanding any other law, adjustments to monetary thresholds and their publication on the agency's internet website pursuant to this subdivision are not subject to the rulemaking provisions of the Administrative Procedure Act (Chapter 3.5 (commencing with Section 11340) of Part 1 of Division 3 of Title 2 of the Government Code).

1798.199.100.

The agency and any court, as applicable, shall consider the good faith cooperation of the business, service provider, contractor, or other person in determining the amount of any administrative fine or civil penalty for a violation of this title. A business shall not be required by the agency, a court, or otherwise to pay both an administrative fine and a civil penalty for the same violation.