March 2023

Kilpatrick Townsend's U.S. Privacy Law Guide

Introduction to State Regulations

KILPATRICK TOWNSEND

Kilpatrick Townsend U.S. Privacy Law E-Book

While there is currently no comprehensive, federal United States law governing data privacy, there are several major state regulations currently in place. We have provided full copies of the comprehensive state privacy laws in this e-book and links to the biometric laws and data broker laws. This e-book is designed to provide you with an easy reference to the comprehensive data privacy laws, biometric laws and data broker laws that have been adopted as of the effective date of this e-book. However, this e-book does not outline what specific compliance steps an organization must take if a law applies, as this will likely vary by organization. Furthermore, this e-book does not include all privacy and security-related laws that have been adopted by states thus far.

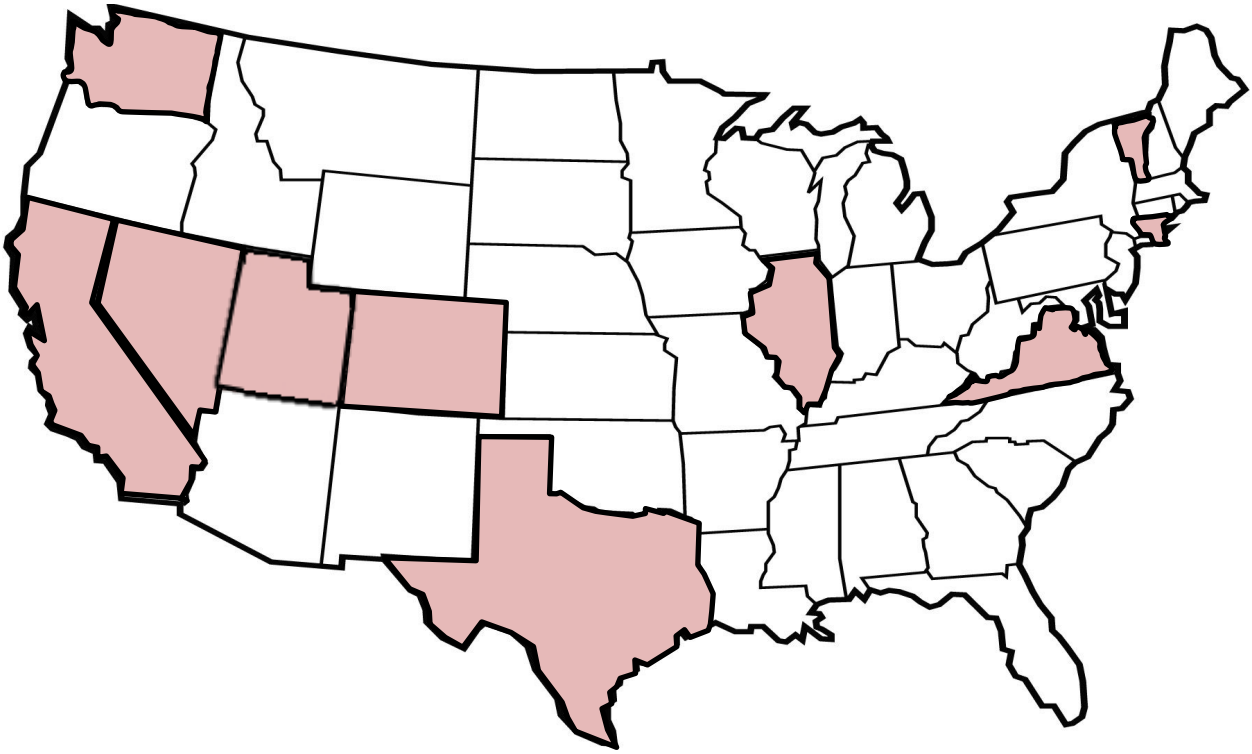
Please note that certain information, including exemptions to the laws described on the following pages, can be complex. The information provided is therefore helpful as a compliance starting point and is neither legal advice nor a finalized compliance determination.

Reading through these different regulations can be overwhelming, but there are opportunities to harmonize compliance across jurisdictions by finding common principles in the various laws. Our team would welcome the opportunity to work with your organization to build a strategic privacy program that meets compliance requirements and aligns with your business strategy.

Table of Contents

Interactive Map

Click the states below to learn more.



Back to Table of Contents

KILPATRICK TOWNSEND

California Consumer Privacy Act

The California Consumer Privacy Act (the "CCPA") was drafted in 2018 and went into effect in January 2020. This legislation was the first comprehensive United States law (state or federal) to regulate consumer data privacy on a large scale. It is often compared to the European General Data Protection Regulation (the "GDPR") that went into effect in 2018.

More recently, in November 2020, California voters passed Proposition 24, the California Privacy Rights Act (the "CPRA"). Substantively, the CPRA aims to create dramatically enhanced consumer rights, including by introducing rights similar to those in the GDPR, which the CCPA does not currently address. Such enhanced consumer rights include the right to opt-out of automated decision-making technology and the introduction of the concept of Sensitive Personal Information, the handling of which will now carry additional obligations and restrictions.

The CPRA's timeline is important to consider. The law will become effective on January 1, 2023 with enforcement set for July 1, 2023.

The full text of the CCPA, the CPRA and their associated regulations are provided below.

Please see the Comprehensive Data Privacy Law Quick Reference Guide for a high-level comparison of the requirements of the CCPA/CPRA compared to other comprehensive data privacy laws.

CCPA Official Text:

CIVIL CODE - CIV

DIVISION 3. OBLIGATIONS [1427 - 3273.16] *(Heading of Division 3 amended by Stats. 1988, Ch. 160, Sec. 14.)*

PART 4. OBLIGATIONS ARISING FROM PARTICULAR TRANSACTIONS [1738 - 3273.16] *(Part 4 enacted 1872.)*

TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100]

(Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3.)

1798.100.

(a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

(b) A business that collects a consumer's personal information 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 shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.

(d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

(e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(Amended by Stats. 2019, Ch. 757, Sec. 1. (AB 1355) Effective January 1, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

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.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 4. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.105.

(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) 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 and direct any service providers to delete the consumer's personal information from their records.

(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider 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 within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

(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 in the public interest that 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 achievement of 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.

(8) Comply with a legal obligation.

(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

(Amended by Stats. 2019, Ch. 751, Sec. 1. (AB 1146) Effective January 1, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

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.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 5. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

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 (8) of subdivision (a) of Section 1798.185.

(Added November 3, 2020, by initiative Proposition 24, Sec. 6. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.110.

(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 or selling personal information.

(4) The categories of third parties with whom the business shares 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 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.

(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 or selling personal information.

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

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

(d) This section does not require a business to do the following:

(1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.

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

(Amended by Stats. 2019, Ch. 757, Sec. 2. (AB 1355) Effective January 1, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

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.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 7. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.115.

(a) A consumer shall have the right to request that a business that sells 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 about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each category of third parties to whom the personal information was sold.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose.

(b) A business that sells 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 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 if the business has not sold 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 the consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell personal information about a consumer that has been sold to 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.

(Amended by Stats. 2019, Ch. 757, Sec. 3. (AB 1355) Effective January 1, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

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.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 8. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.120.

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

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

(c) Notwithstanding subdivision (a), a business shall not sell 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 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. This right may be referred to as the "right to opt-in."

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

(Amended by Stats. 2019, Ch. 757, Sec. 4. (AB 1355) Effective January 1, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

1798.120.

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

(a) 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.

(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.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 9. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

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 (19) 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 (19) 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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 10. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.125.

(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.

(2) Nothing in this subdivision prohibits a business 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.

(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion 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 directly 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.

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

(Amended by Stats. 2019, Ch. 757, Sec. 5. (AB 1355) Effective January 1, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

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.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 11. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.130.

(a) In order to comply with Sections 1798.100, 1798.105, 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, 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.

(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.

(2) Disclose and deliver the required information to a consumer free of charge 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 within 45 days of receipt of the consumer's request. The time period to provide the required 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 shall cover the 12-month period preceding the business' receipt of the verifiable consumer request and 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. If the consumer maintains an account with the business, the business may require the consumer to submit the request through that account.

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

(A) 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.

(B) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

(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 in the preceding 12 months 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 in the preceding 12 months by reference to the enumerated category or categories in

subdivision (c) that most closely describes the personal information sold. 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 in the preceding 12 months by reference to the enumerated category or categories 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 disclosed for a business purpose in the preceding 12 months 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, 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.

(B) For purposes of subdivision (c) of Section 1798.110, 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.

(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 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 if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact.

(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 describe 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.

(D) In the case of a business that sells or discloses deidentified patient information not subject to this title pursuant to clause (i) of subparagraph (A) of paragraph (4) of subdivision (a) of Section 1798.146, whether the business sells or discloses deidentified patient information derived from patient information and if so, whether that patient information was deidentified pursuant to one or more of the following:

(i) The deidentification methodology described in Section 164.514(b)(1) of Title 45 of the Code of Federal Regulations, commonly known as the HIPAA expert determination method.

(ii) The deidentification methodology described in Section 164.514(b)(2) of Title 45 of the Code of Federal Regulations, commonly known as the HIPAA safe harbor method.

(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,

1798.110, 1798.115, and 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.

(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 1798.110 and 1798.115 shall follow the definition of personal information in Section 1798.140.

(Amended by Stats. 2020, Ch. 172, Sec. 1. (AB 713) Effective September 25, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

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's 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 (9) 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's 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.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 12. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.135.

(a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell 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 of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

(2) Include a description of a consumer's rights pursuant to Section 1798.120, along with a separate link to the "Do Not Sell My Personal Information" Internet Web page 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's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 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 of their personal information, refrain from selling personal information collected by the business about the consumer.

(5) For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information.

(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.

(b) 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.

(c) A consumer may authorize another person solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, 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.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 8. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198. Superseded on January 1, 2023; see amendment by Proposition 24.)

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's 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 (20) 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 (20) 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’s privacy practices or the business’s 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 consistent 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.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 13. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.140.

For purposes of this title:

(a) "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.

(b) "Biometric information" means an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can 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.

(c) "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 that 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) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(C) Derives 50 percent or more of its annual revenues from selling 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. "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.

(d) "Business purpose" means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

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

(4) Short-term, transient use, provided that the personal information is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.

(5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.

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

(7) 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.

(e) “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.

(f) “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. “Commercial purposes” do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

(g) “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.

(h) “Deidentified” means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(2) Has implemented business processes that specifically prohibit reidentification of the information.

(3) Has implemented business processes to prevent inadvertent release of deidentified information.

(4) Makes no attempt to reidentify the information.

(i) “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.

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

(k) “Health insurance information” means a consumer’s insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer’s application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.

(l) “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 notice required by subdivision (a) of Section 1798.135, including, but not limited to, before downloading the application.

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

(n) “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.

(o) (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 categories of 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.

(2) “Personal information” does not include publicly available information. For purposes of this paragraph, “publicly available” means information that is lawfully made available from federal, state, or local government records. “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.

(p) “Probabilistic identifier” means the identification of a consumer or a 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.

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

(r) “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.

(s) “Research” means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or 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’s 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.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(4) Subject to business processes that specifically prohibit reidentification of the information.

(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) Not be used for any commercial purpose.

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

(t) (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 another business or 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 disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

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

(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:

(i) The business has provided notice of that information being used or shared in its terms and conditions consistent with Section 1798.135.

(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

(D) 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 Sections 1798.110 and 1798.115. 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 Section 1798.120. 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).

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

(v) "Service provider" means 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 processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the

personal information for a commercial purpose other than providing the services specified in the contract with the business.

(w) “Third party” means a person who is not any of the following:

(1) The business that collects personal information from consumers under this title.

(2) (A) A person to whom the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract:

(i) Prohibits the person receiving the personal information from:

(I) Selling the personal information.

(II) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.

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

(ii) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

(B) A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person 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 person intends to commit such a violation.

(x) “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 Protocol 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. For purposes of this subdivision, “family” means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

(y) “Verifiable consumer request” means a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) 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 1798.100, 1798.105, 1798.110, and 1798.115 if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of 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.

(Amended by Stats. 2019, Ch. 757, Sec. 7.5. (AB 1355) Effective January 1, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

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 paragraph (5) of subdivision (a) of Section 1798.185.

(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.

(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 (11) 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 (10) 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 websites, applications, or services, other than the business, distinctly-branded 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 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) "Personal information" does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this paragraph, "publicly available" means: information that is lawfully made available from federal, state, or local government records, or 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; or 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. "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.

(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 (16) 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, 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.

(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 (10) 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 Protocol 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 (7) 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 and regulations adopted by the Attorney General pursuant to paragraph (7) of 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.

(Amended (as amended November 3, 2020, by Prop. 24, Sec. 14) by Stats. 2021, Ch. 525, Sec. 3. (AB 694) Effective January 1, 2022.)

1798.145.

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

(1) Comply with federal, state, or local laws.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(3) 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.

(4) Exercise or defend legal claims.

(5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.

(6) Collect or sell 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 permit 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.

(b) The obligations imposed on businesses by Sections 1798.110 to 1798.135, inclusive, 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) Information collected as part of a clinical trial subject to 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.

(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 credit worthiness, 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 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 pursuant 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). 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 flotation device approved under Section 160.076 of Title 46 of the Code of Federal Regulations.

(h) (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 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 a 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 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 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) “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) “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, such as a chief executive officer, president, secretary, or treasurer.

(E) “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 not apply to subdivision (b) of Section 1798.100 or Section 1798.150.

(4) This subdivision shall become inoperative on January 1, 2021.

(i) Notwithstanding a business’ obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to any verified consumer request may be extended by up to 90 additional 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 verified consumer request is manifestly unfounded or excessive.

(j) A business that discloses personal information to a service provider shall not be liable under this title if the service provider 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 intends to commit such a violation. A service provider 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.

(k) This title shall not be construed to require a business to collect personal information that it would not otherwise collect in the ordinary course of its business, retain personal information for longer than it would otherwise retain such information in the ordinary course of its business, or reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(l) 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 consumers.

(m) 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.

(n) (1) The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.110, 1798.115, 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 is acting as an employee, owner, director, officer, or 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) “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, 2021.

(Amended (as amended by Stats. 2019, Ch. 763, Sec. 2.3) by Stats. 2021, Ch. 700, Sec. 1. (AB 335) Effective January 1, 2022. Superseded on January 1, 2023; see amendment by Proposition 24. But see now the immediately operative subdivisions (m) and (n) in Prop. 24's amendment. Note: In Prop. 24's amendment, on December 16, 2020, its new subd. (m) becomes operative, and its subd. (n) supsersedes the subd. (n) in this version.)

1798.145.

Exemptions

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

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

(2) 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.

(3) 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.

(4) 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:

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

(B) 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.

(C) 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.

(5) Exercise or defend legal claims.

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

(7) 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.

(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’ 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' 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’ use, disclosure, or sale of particular pieces of a consumer’s personal information if the consumer has consented to the business’ 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.

(Amended (as amended November 3, 2020, by initiative Proposition 24, Section 15) by Stats. 2021, Ch. 700, Sec. 2.5. (AB 335) Effective January 1, 2022. Subdivisions (m) and (n) inoperative January 1, 2023, by their own provisions.)

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.

(Added by Stats. 2020, Ch. 172, Sec. 2. (AB 713) Effective September 25, 2020.)

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.

(Added by Stats. 2020, Ch. 172, Sec. 3. (AB 713) Effective September 25, 2020.)

1798.150.

(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, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's 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.

(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.

(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. 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.

(Amended by Stats. 2019, Ch. 757, Sec. 9. (AB 1355) Effective January 1, 2020. Superseded on January 1, 2023; see amendment by Proposition 24.)

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's 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.

(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.

(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.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 16. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.155.

(a) Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title.

(b) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, 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, 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 civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.

(c) Any civil penalty assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (b), shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with this title.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 12. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198. Superseded on January 1, 2023; see amendment by Proposition 24.)

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 paragraph (5) of subdivision (a) of Section 1798.185, in an administrative enforcement action brought by the California Privacy Protection Agency.

(b) Any administrative fine assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (a), shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent to fully offset any costs incurred by the state courts, the Attorney General, and the California Privacy Protection Agency in connection with this title.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 17. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.160.

Consumer Privacy Fund

(a) 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 first to offset any costs incurred by the state courts in connection with actions brought to enforce this title, the costs incurred by the Attorney

General in carrying out the Attorney General's duties under this title, and then for the purposes of establishing an investment fund in the State Treasury, with any earnings or interest from the fund to be deposited in the General Fund, and making 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) Funds transferred to the Consumer Privacy Fund shall be used exclusively as follows:

(1) To offset any costs incurred by the state courts and the Attorney General in connection with this title.

(2) After satisfying the obligations under paragraph (1), the remaining funds shall be allocated each fiscal year as follows:

(A) Ninety-one percent shall be invested by the Treasurer in financial assets with the goal of maximizing long term yields consistent with a prudent level of risk. The principal shall not be subject to transfer or appropriation, provided that any interest and earnings shall be transferred on an annual basis to the General Fund for appropriation by the Legislature for General Fund purposes.

(B) Nine percent shall be made available to the California Privacy Protection Agency for the purposes of making grants in California, with 3 percent allocated 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.

(c) Funds in the Consumer Privacy Fund shall not be subject to appropriation or transfer by the Legislature for any other purpose.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 18. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.175.

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.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198. Superseded on January 1, 2023; see amendment by Proposition 24.)

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.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 19. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.180.

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.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative September 23, 2018, pursuant to Section 1798.199. Superseded on January 1, 2023; see amendment by Proposition 24.)

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.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 20. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

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) Adjusting the monetary thresholds, in January of every odd-numbered year to reflect any increase in the Consumer Price Index, 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.

(6) 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.

(7) 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's 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's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

(8) 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.

(9) 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.

(10) 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.

(11) 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.

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

(13) 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.

(14) 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.

(15) 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.

(16) Issuing regulations governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling and requiring businesses' 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.

(17) Issuing regulations to further define a "law enforcement agency-approved investigation" for purposes of the exception in paragraph (2) of subdivision (a) of Section 1798.145.

(18) 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.

(19) (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.

(20) 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 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 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.

(21) 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.

(22) 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.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 21. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

1798.190.

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, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198. Superseded on January 1, 2023; see amendment by Proposition 24.)

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.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 22. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.192.

Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's 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 the consumer's personal information after previously opting out.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 14. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198. Superseded on January 1, 2023; see amendment by Proposition 24.)

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.

(Amended November 3, 2020, by initiative Proposition 24, Sec. 23. Effective December 16, 2020. Operative January 1, 2023, pursuant to Sec. 31 of Proposition 24.)

1798.194.

This title shall be liberally construed to effectuate its purposes.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

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.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 15. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

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.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 16. (SB 1121) Effective September 23, 2018.)

1798.199.

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

(Added by Stats. 2018, Ch. 735, Sec. 17. (SB 1121) Effective September 23, 2018. Operative September 23, 2018.)

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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.1. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.2. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.3. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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 biennially to reflect changes in the cost of living, and shall be reimbursed for expenses incurred in performance of their official duties.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.4. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.5. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.6. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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 (15) 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 (18) 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.

(Amended by Stats. 2021, Ch. 525, Sec. 5. (AB 694) Effective January 1, 2022.)

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) 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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.8. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.9. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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), Part 1, Division 3, Title 2, 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 to the Consumer Privacy Fund within the General Fund of the state. When the agency determines that no violation has occurred, it shall publish a declaration so stating.

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

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.10. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.11. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.12. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.13. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.14. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.15. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.16. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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 paragraph (5) of subdivision (a) of Section 1798.185, 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) Any civil penalty recovered by an action brought by the Attorney General for a violation of this title, and the proceeds of any settlement of any said action, shall be deposited in the Consumer Privacy Fund.

(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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.17. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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 2020–2021, 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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.18. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

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.

(Added November 3, 2020, by initiative Proposition 24, Sec. 24.19. Effective December 16, 2020. Operative December 16, 2020, pursuant to Sec. 31 of Proposition 24.)

CCPA Regulations Official Text:

Chapter 20. California Consumer Privacy Act Regulations

Article 1. General Provisions

§ 999.300. Title and Scope.

11 CA ADC § 999.300BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 1. General Provisions

11 CCR § 999.300

§ 999.300. Title and Scope.

(a) This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as “these regulations.” These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have.

(b) A violation of these regulations shall constitute a violation of the CCPA and be subject to the remedies provided for therein.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155 and 1798.185, Civil Code.

HISTORY

1. New chapter 20 (articles 1-6, sections 999.300-999.337), article 1 (sections 999.300-999.301) and section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33). For prior history of chapter 20 (sections 999.500-999.506), see Register 2019, No. 47.

This database is current through 1/7/22 Register 2022, No. 1

11 CCR § 999.300, 11 CA ADC § 999.300

§ 999.301. Definitions.

11 CA ADC § 999.301BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 1. General Provisions

11 CCR § 999.301

§ 999.301. Definitions.

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

(a) “Affirmative authorization” means an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a consumer under 13 years of age, it means that the parent or guardian has provided consent to the sale of the consumer's personal information in accordance with the methods set forth in section 999.330. For consumers 13 years of age and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

(b) “Attorney General” means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General.

(c) “Authorized agent” means a natural person or a business entity registered with the Secretary of State to conduct business in California that a consumer has authorized to act on their behalf subject to the requirements set forth in section 999.326.

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

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

(f) “CCPA” means the California Consumer Privacy Act of 2018, Civil Code sections 1798.100 et seq.

(g) “COPPA” means the Children's Online Privacy Protection Act, 15 U.S.C. sections 6501 to 6508 and 16 Code of Federal Regulations part 312.5.

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

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

(j) “Financial incentive” means a program, benefit, or other offering, including payments to consumers, related to the collection, deletion, or sale of personal information.

(k) “Household” means a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier.

(*l*) “Notice at collection” means the notice given by a business to a consumer at or before the point at which a business collects personal information from the consumer as required by Civil Code section 1798.100, subdivision (b), and specified in these regulations.

(m) “Notice of right to opt-out” means the notice given by a business informing consumers of their right to opt-out of the sale of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations.

(n) “Notice of financial incentive” means the notice given by a business explaining each financial incentive or price or service difference as required by Civil Code section 1798.125, subdivision (b), and specified in these regulations.

(o) “Price or service difference” means (1) any difference in the price or rate charged for any goods or services to any consumer related to the collection, retention, or sale of personal information, including through the use of discounts, financial payments, or other benefits or penalties; or (2) any difference in the level or quality of any goods or services offered to any consumer related to the collection, retention, or sale of personal information, including the denial of goods or services to the consumer.

(p) “Privacy policy,” as referred to in Civil Code section 1798.130, subdivision (a)(5), means the statement that a business shall make available to consumers describing the business's practices, both online and offline, regarding the collection, use, disclosure, and sale of personal information, and of the rights of consumers regarding their own personal information.

(q) “Request to delete” means a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105.

(r) “Request to know” means a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections 1798.100, 1798.110, or 1798.115. It includes a request for any or all of the following:

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

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

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

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

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

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

(s) “Request to opt-in” means the affirmative authorization that the business may sell personal information about the consumer by a parent or guardian of a consumer less than 13 years of age, by a consumer at least 13 and less than 16 years of age, or by a consumer who had previously opted out of the sale of their personal information.

(t) “Request to opt-out” means a consumer request that a business not sell the consumer's personal information to third parties, pursuant to Civil Code section 1798.120, subdivision (a).

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

(v) “Third-party identity verification service” means a security process offered by an independent third party that verifies the identity of the consumer making a request to the business. Third-party identity verification services are subject to the requirements set forth in Article 4 regarding requests to know and requests to delete.

(w) “Value of the consumer's data” means the value provided to the business by the consumer's data as calculated under section 999.337.

(x) “Verify” means to determine that the consumer making a request to know or request to delete is the consumer about whom the business has collected information, or if that consumer is less than 13 years of age, the consumer's parent or legal guardian.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145 and 1798.185, Civil Code.

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/7/22 Register 2022, No. 1

11 CCR § 999.301, 11 CA ADC § 999.301

Article 2. Notices to Consumers

§ 999.304. Overview of Required Notices.

11 CA ADC § 999.304 BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 2. Notices to Consumers

11 CCR § 999.304

§ 999.304. Overview of Required Notices.

(a) Every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and section 999.308.

(b) A business that collects personal information from a consumer shall provide a notice at collection in accordance with the CCPA and section 999.305.

(c) A business that sells personal information shall provide a notice of right to opt-out in accordance with the CCPA and section 999.306.

(d) A business that offers a financial incentive or price or service difference shall provide a notice of financial incentive in accordance with the CCPA and section 999.307.

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

HISTORY

1. New article 2 (sections 999.304-999.308) and section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/7/22 Register 2022, No. 1

11 CCR § 999.304, 11 CA ADC § 999.304

§ 999.305. Notice at Collection of Personal Information.

11 CA ADC § 999.305BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 2. Notices to Consumers

11 CCR § 999.305

§ 999.305. Notice at Collection of Personal Information.

(a) Purpose and General Principles

(1) The purpose of the notice at collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them and the purposes for which the personal information will be used.

(2) The notice at collection shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:

a. Use plain, straightforward language and avoid technical or legal jargon.

b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.

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

d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

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

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

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

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

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

(4) When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection. For example, if the business offers a flashlight application and the application collects geolocation information, the business shall provide a just-in-time notice, such as through a pop-up window when the consumer opens the application, that contains the information required by this subsection.

(5) A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection.

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

(b) A business shall include the following in its notice at collection:

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

(2) The business or commercial purpose(s) for which the categories of personal information will be used.

(3) If the business sells personal information, the link titled “Do Not Sell My Personal Information” required by section 999.315, subsection (a), or in the case of offline notices, where the webpage can be found online.

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

(c) If a business collects personal information from a consumer online, the notice at collection may be given to the consumer by providing a link to the section of the business's privacy policy that contains the information required in subsection (b).

(d) A business that does not collect personal information directly from the consumer does not need to provide a notice at collection to the consumer if it does not sell the consumer's personal information.

(e) A data broker registered with the Attorney General pursuant to Civil Code section 1798.99.80 et seq. does not need to provide a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out.

(f) A business collecting employment-related information shall comply with the provisions of section 999.305 except with regard to the following:

(1) The notice at collection of employment-related information does not need to include the link or web address to the link titled “Do Not Sell My Personal Information”.

(2) The notice at collection of employment-related information is not required to provide a link to the business's privacy policy.

(g) Subsection (f) shall become inoperative on January 1, 2021, unless the CCPA is amended otherwise.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.99.82, 1798.100, 1798.115 and 1798.185, Civil Code.

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/7/22 Register 2022, No. 1

11 CCR § 999.305, 11 CA ADC § 999.305

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

11 CA ADC § 999.306 BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 2. Notices to Consumers

11 CCR § 999.306

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

(a) Purpose and General Principles

(1) The purpose of the notice of right to opt-out is to inform consumers of their right to direct a business that sells their personal information to stop selling their personal information.

(2) The notice of right to opt-out shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:

a. Use plain, straightforward language and avoid technical or legal jargon.

b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.

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

d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1

of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

(b) A business that sells the personal information of consumers shall provide the notice of right to opt-out to consumers as follows:

(1) A business shall post the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the “Do Not Sell My Personal Information” link on the website homepage or the download or landing page of a mobile application. In addition, a business that collects personal information through a mobile application may provide a link to the notice within the application, such as through the application's settings menu. The notice shall include the information specified in subsection (c) or link to the section of the business's privacy policy that contains the same information.

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

(3) A business that sells personal information that it collects in the course of interacting with consumers offline shall also inform consumers by an offline method of their right to opt-out and provide instructions on how to submit a request to opt-out. Illustrative examples follow:

a. A business that sells personal information that it collects from consumers in a brick-and-mortar store may inform consumers of their right to opt-out on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the opt-out information can be found online.

b. A business that sells personal information that it collects over the phone may inform consumers of their right to opt-out orally during the call when the information is collected.

(c) A business shall include the following in its notice of right to opt-out:

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

(2) The interactive form by which the consumer can submit their request to opt-out online, as required by section 999.315, subsection (a), or if the business does not operate a website, the offline method by which the consumer can submit their request to opt-out; and

(3) Instructions for any other method by which the consumer may submit their request to opt-out.

(d) A business does not need to provide a notice of right to opt-out if:

(1) It does not sell personal information; and

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

(e) A business shall not sell the personal information it collected during the time the business did not have a notice of right to opt-out posted unless it obtains the affirmative authorization of the consumer.

(f) Opt-Out Icon.

(1) The following opt-out icon may be used in addition to posting the notice of right to opt-out, but not in lieu of any requirement to post the notice of right to opt-out or a “Do Not Sell My Personal Information” link as required by Civil Code section 1798.135 and these regulations.

(2) The icon shall be approximately the same size as any other icons used by the business on its webpage.

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

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

2. New subsections (b)(3) and (f)-(f)(2) filed 3-12-2021; operative 3-15-2021 pursuant to Government Code section 11343.4(b)(3) (Register 2021, No. 11). Filing deadline specified in Government Code section 11349.3(a) extended 60 calendar days pursuant to Executive Order N-40-20.

This database is current through 1/7/22 Register 2022, No. 1

11 CCR § 999.306, 11 CA ADC § 999.306

§ 999.307. Notice of Financial Incentive.

11 CA ADC § 999.307BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 2. Notices to Consumers

11 CCR § 999.307

§ 999.307. Notice of Financial Incentive.

(a) Purpose and General Principles

(1) The purpose of the notice of financial incentive is to explain to the consumer the material terms of a financial incentive or price or service difference the business is offering so that the consumer may make an informed decision about whether to participate. A business that does not offer a financial incentive or price or service difference is not required to provide a notice of financial incentive.

(2) The notice of financial incentive shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:

a. Use plain, straightforward language and avoid technical or legal jargon.

b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.

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

d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

e. Be readily available where consumers will encounter it before opting-in to the financial incentive or price or service difference.

(3) If the business offers the financial incentive or price or service difference online, the notice may be given by providing a link to the section of a business's privacy policy that contains the information required in subsection (b).

(b) A business shall include the following in its notice of financial incentive:

(1) A succinct summary of the financial incentive or price or service difference offered;

(2) A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data;

(3) How the consumer can opt-in to the financial incentive or price or service difference;

(4) A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and

(5) An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including:

a. A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and

b. A description of the method the business used to calculate the value of the consumer's data.

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

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/7/22 Register 2022, No. 1

11 CCR § 999.307, 11 CA ADC § 999.307

§ 999.308. Privacy Policy.

11 CA ADC § 999.308BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 2. Notices to Consumers

11 CCR § 999.308

§ 999.308. Privacy Policy.

(a) Purpose and General Principles

(1) The purpose of the privacy policy is to provide consumers with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information.

(2) The privacy policy shall be designed and presented in a way that is easy to read and understandable to consumers. The policy shall:

a. Use plain, straightforward language and avoid technical or legal jargon.

b. Use a format that makes the policy readable, including on smaller screens, if applicable.

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

d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the policy in an alternative format.

e. Be available in a format that allows a consumer to print it out as a document.

(b) The privacy policy shall be posted online through a conspicuous link using the word “privacy” on the business's website homepage or on the download or landing page of a mobile application. If the business has a California-specific description of consumers' privacy rights on its website, then the privacy policy shall be included in that description. A business that does not operate a website shall make the privacy policy conspicuously available to consumers. A mobile application may include a link to the privacy policy in the application's settings menu.

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

(1) Right to Know About Personal Information Collected, Disclosed, or Sold.

a. Explanation that a consumer has the right to request that the business disclose what personal information it collects, uses, discloses, and sells.

b. Instructions for submitting a verifiable consumer request to know and links to an online request form or portal for making the request, if offered by the business.

c. General description of the process the business will use to verify the consumer request, including any information the consumer must provide.

d. Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described in a manner that provides consumers a meaningful understanding of the information being collected.

e. Identification of the categories of sources from which the personal information is collected.

f. Identification of the business or commercial purpose for collecting or selling personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected or sold.

g. Disclosure or Sale of Personal Information.

1. Identification of the categories of personal information, if any, that the business has disclosed for a business purpose or sold to third parties in the preceding 12 months.

2. For each category of personal information identified, the categories of third parties to whom the information was disclosed or sold.

3. Statement regarding whether the business has actual knowledge that it sells the personal information of consumers under 16 years of age.

(2) Right to Request Deletion of Personal Information.

a. Explanation that the consumer has a right to request the deletion of their personal information collected by the business.

b. Instructions for submitting a verifiable consumer request to delete and links to an online request form or portal for making the request, if offered by the business.

c. General description of the process the business will use to verify the consumer request, including any information the consumer must provide.

(3) Right to Opt-Out of the Sale of Personal Information.

a. Explanation that the consumer has a right to opt-out of the sale of their personal information by a business.

b. Statement regarding whether or not the business sells personal information. If the business sells personal information, include either the contents of the notice of right to opt-out or a link to it in accordance with section 999.306.

(4) Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights.

a. Explanation that the consumer has a right not to receive discriminatory treatment by the business for the exercise of the privacy rights conferred by the CCPA.

(5) Authorized Agent.

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

(6) Contact for More Information.

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

(7) Date the privacy policy was last updated.

(8) If subject to the requirements set forth in section 999.317, subsection (g), the information compiled in section 999.317, subsection (g)(1), or a link to it.

(9) If the business has actual knowledge that it sells the personal information of consumers under 16 years of age, a description of the processes required by sections 999.330 and 999.331.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.115, 1798.120, 1798.125 and 1798.130, Civil Code.

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/7/22 Register 2022, No. 1

11 CCR § 999.308, 11 CA ADC § 999.308

Article 3. Business Practices for Handling Consumer Requests

§ 999.312. Methods for Submitting Requests to Know and Requests to Delete.

11 CA ADC § 999.312BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 3. Business Practices for Handling Consumer Requests

11 CCR § 999.312

§ 999.312. Methods for Submitting Requests to Know and Requests to Delete.

(a) A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to know. All other businesses shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.

(b) A business shall provide two or more designated methods for submitting requests to delete. Acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a link or form available online through a business's website, a designated email address, a form submitted in person, and a form submitted through the mail.

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

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

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

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

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

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

HISTORY

1. New article 3 (sections 999.312-999.318) and section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/7/22 Register 2022, No. 1

11 CCR § 999.312, 11 CA ADC § 999.312

§ 999.313. Responding to Requests to Know and Requests to Delete.

11 CA ADC § 999.313BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 3. Business Practices for Handling Consumer Requests

11 CCR § 999.313

§ 999.313. Responding to Requests to Know and Requests to Delete.

(a) Upon receiving a request to know or a request to delete, a business shall confirm receipt of the request within 10 business days and provide information about how the business will process the request. The information provided shall describe in general the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request. The confirmation may be given in the same manner in which the request was received. For example, if the request is made over the phone, the confirmation may be given orally during the phone call.

(b) Businesses shall respond to requests to know and requests to delete within 45 calendar days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request. If the business cannot verify the consumer within the 45-day time period, the business may deny the request. If necessary, businesses may take up to an additional 45 calendar days to respond to the consumer's request, for a maximum total of 90 calendar days from the day the request is received, provided that the

business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

(c) Responding to Requests to Know.

(1) For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (c)(2).

(2) For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall provide or direct the consumer to its general business practices regarding the collection, maintenance, and sale of personal information set forth in its privacy policy.

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

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

b. The business maintains the personal information solely for legal or compliance purposes;

c. The business does not sell the personal information and does not use it for any commercial purpose; and

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

(4) A business shall not disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. The business shall, however, inform the consumer with sufficient particularity that it has collected the type of information. For example, a business shall respond that it collects “unique biometric data including a fingerprint scan” without disclosing the actual fingerprint scan data.

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

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

(7) If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 4.

(8) Unless otherwise specified by the business to cover a longer period of time, the 12-month period covered by a consumer's verifiable request to know referenced in Civil Code section 1798.130, subdivision (a)(2), shall run from the date the business receives the request, regardless of the time required to verify the request.

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

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

a. The categories of personal information the business has collected about the consumer in the preceding 12 months;

b. The categories of sources from which the personal information was collected;

c. The business or commercial purpose for which it collected or sold the personal information;

d. The categories of third parties with whom the business shares personal information;

e. The categories of personal information that the business sold in the preceding 12 months, and for each category identified, the categories of third parties to whom it sold that particular category of personal information; and

f. The categories of personal information that the business disclosed for a business purpose in the preceding 12 months, and for each category identified, the categories of third parties to whom it disclosed that particular category of personal information.

(11) A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner that provides consumers a meaningful understanding of the categories listed.

(d) Responding to Requests to Delete.

(1) For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified.

(2) A business shall comply with a consumer's request to delete their personal information by:

a. Permanently and completely erasing the personal information on its existing systems with the exception of archived or back-up systems;

b. Deidentifying the personal information; or

c. Aggregating the consumer information.

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

(4) In responding to a request to delete, a business shall inform the consumer whether or not it has complied with the consumer's request.

(5) If the business complies with the consumer's request, the business shall inform the consumer that it will maintain a record of the request as required by section 999.317, subsection (b). A business may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from the business's records.

(6) In cases where a business denies a consumer's request to delete, the business shall do all of the following:

a. Inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including any conflict with federal or state law, or exception to the CCPA, unless prohibited from doing so by law;

b. Delete the consumer's personal information that is not subject to the exception; and

c. Not use the consumer's personal information retained for any other purpose than provided for by that exception.

(7) If a business that denies a consumer's request to delete sells personal information and the consumer has not already made a request to opt-out, the business shall ask the consumer if they would like to opt-out of the sale of their personal information and shall include either the contents of, or a link to, the notice of right to opt-out in accordance with section 999.306.

(8) In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information only if a global option to delete all personal information is also offered and more prominently presented than the other choices.

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

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/7/22 Register 2022, No. 1

11 CCR § 999.313, 11 CA ADC § 999.313

§ 999.314. Service Providers.

11 CA ADC § 999.314BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 3. Business Practices for Handling Consumer Requests

11 CCR § 999.314

§ 999.314. Service Providers.

(a) A business that provides services to a person or organization that is not a business, and that would otherwise meet the requirements and obligations of a “service provider” under the CCPA and these regulations, shall be deemed a service provider for purposes of the CCPA and these regulations.

(b) To the extent that a business directs a second entity to collect personal information directly from a consumer, or about a consumer, on the first business's behalf, and the second entity would otherwise meet the requirements and obligations of a “service provider” under the CCPA and these regulations, the second entity shall be deemed a service provider of the first business for purposes of the CCPA and these regulations.

(c) A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except:

(1) To process or maintain personal information on behalf of the business that provided the personal information or directed the service provider to collect the personal information, and in compliance with the written contract for services required by the CCPA;

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

(3) For internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source;

(4) To detect data security incidents or protect against fraudulent or illegal activity; or

(5) For the purposes enumerated in Civil Code section 1798.145, subdivisions (a)(1) through (a)(4).

(d) A service provider shall not sell data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business.

(e) If a service provider receives a request to know or a request to delete from a consumer, the service provider shall either act on behalf of the business in responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider.

(f) A service provider that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider.

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

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/7/22 Register 2022, No. 1

11 CCR § 999.314, 11 CA ADC § 999.314

§ 999.315. Requests to Opt-Out.

11 CA ADC § 999.315BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 3. Business Practices for Handling Consumer Requests

11 CCR § 999.315

§ 999.315. Requests to Opt-Out.

(a) A business shall provide two or more designated methods for submitting requests to opt-out, including an interactive form accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information,” on the business's website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information.

(b) A business shall consider the methods by which it interacts with consumers, the manner in which the business sells personal information to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer.

(c) If a business collects personal information from consumers online, the business shall treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.

(1) Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information.

(2) If a global privacy control conflicts with a consumer's existing business-specific privacy setting or their participation in a business's financial incentive program, the business shall respect the global privacy control but may notify the consumer of the conflict and give the consumer the choice to confirm the business-specific privacy setting or participation in the financial incentive program.

(d) In responding to a request to opt-out, a business may present the consumer with the choice to opt-out of sale for certain uses of personal information as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices.

(e) A business shall comply with a request to opt-out as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. If a business sells a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request, it shall notify those third parties that the consumer has exercised their right to opt-out and shall direct those third parties not to sell that consumer's information.

(f) A consumer may use an authorized agent to submit a request to opt-out on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent cannot provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. User-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.

(g) A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent.

(h) A business's methods for submitting request to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out. A business shall not use a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out. Illustrative examples follow:

(1) The business's process for submitting a request to opt-out shall not require more steps than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a request to opt-out is measured from when the consumer clicks on the “Do Not Sell My Personal Information” link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt-out in completion of the request.

(2) A business shall not use confusing language, such as double-negatives (e.g., “Don't Not Sell My Personal Information”), when providing consumers the choice to opt-out.

(3) Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request.

(4) The business's process for submitting a request to opt-out shall not require the consumer to provide personal information that is not necessary to implement the request.

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

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

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

2. New subsections (h)-(h)(5) filed 3-12-2021; operative 3-15-2021 pursuant to Government Code section 11343.4(b)(3) (Register 2021, No. 11). Filing deadline specified in Government Code section 11349.3(a) extended 60 calendar days pursuant to Executive Order N-40-20.

This database is current through 1/7/22 Register 2022, No. 1

11 CCR § 999.315, 11 CA ADC § 999.315

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

11 CA ADC § 999.316BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 3. Business Practices for Handling Consumer Requests

11 CCR § 999.316

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

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

(b) If a consumer who has opted-out of the sale of their personal information initiates a transaction or attempts to use a product or service that requires the sale of their personal information, a business may inform the consumer that the transaction, product, or service requires the sale of their personal information and provide instructions on how the consumer can opt-in.

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

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/7/22 Register 2022, No. 1

11 CCR § 999.316, 11 CA ADC § 999.316

§ 999.317. Training; Record-Keeping.

11 CA ADC § 999.317BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 3. Business Practices for Handling Consumer Requests

11 CCR § 999.317

§ 999.317. Training; Record-Keeping.

(a) All individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA shall be informed of all of the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.

(b) A business shall maintain records of consumer requests made pursuant to the CCPA and how it responded to the requests for at least 24 months. The business shall implement and maintain reasonable security procedures and practices in maintaining these records.

(c) The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.

(d) A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.

(e) Information maintained for record-keeping purposes shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and these regulations. Information maintained for record-keeping purposes shall not be shared with any third party except as necessary to comply with a legal obligation.

(f) Other than as required by subsection (b), a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.

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

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

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

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

c. The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and

d. The median or mean number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.

(2) Disclose, by July 1 of every calendar year, the information compiled in subsection (g)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy.

a. In its disclosure pursuant to subsection (g)(2), a business may choose to disclose the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.

(3) Establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.

(h) A business may choose to compile and disclose the information required by subsection (g)(1) for requests received from all individuals, rather than requests received from consumers. The business shall state whether

it has done so in its disclosure and shall, upon request, compile and provide to the Attorney General the information required by subsection (g)(1) for requests received from consumers.

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

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/7/22 Register 2022, No. 1

11 CCR § 999.317, 11 CA ADC § 999.317

§ 999.318. Requests to Know or Delete Household Information.

11 CA ADC § 999.318 BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 3. Business Practices for Handling Consumer Requests

11 CCR § 999.318

§ 999.318. Requests to Know or Delete Household Information.

(a) Where a household does not have a password-protected account with a business, a business shall not comply with a request to know specific pieces of personal information about the household or a request to delete household personal information unless all of the following conditions are satisfied:

(1) All consumers of the household jointly request to know specific pieces of information for the household or the deletion of household personal information;

(2) The business individually verifies all the members of the household subject to the verification requirements set forth in section 999.325; and

(3) The business verifies that each member making the request is currently a member of the household.

(b) Where a consumer has a password-protected account with a business that collects personal information about a household, the business may process requests to know and requests to delete relating to household information through the business's existing business practices and in compliance with these regulations.

(c) If a member of a household is a consumer under the age of 13, a business must obtain verifiable parental consent before complying with a request to know specific pieces of information for the household or the deletion of household personal information pursuant to the parental consent provisions in section 999.330.

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

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/7/22 Register 2022, No. 1

11 CCR § 999.318, 11 CA ADC § 999.318

Article 4. Verification of Requests

§ 999.323. General Rules Regarding Verification.

11 CA ADC § 999.323 BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 4. Verification of Requests

11 CCR § 999.323

§ 999.323. General Rules Regarding Verification.

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

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

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

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

(3) Consider the following factors:

a. The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive or valuable personal information shall warrant a more stringent verification process. The types of personal information identified in Civil Code section 1798.81.5, subdivision (d), shall be considered presumptively sensitive;

b. The risk of harm to the consumer posed by any unauthorized access or deletion. A greater risk of harm to the consumer by unauthorized access or deletion shall warrant a more stringent verification process;

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

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

e. The manner in which the business interacts with the consumer; and

f. Available technology for verification.

(c) A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, security, or fraud-prevention. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 999.317.

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

(e) A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information.

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

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

HISTORY

1. New article 4 (sections 999.323-999.326) and section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/14/22 Register 2022, No. 2

11 CCR § 999.323, 11 CA ADC § 999.323

§ 999.324. Verification for Password-Protected Accounts.

11 CA ADC § 999.324 BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 4. Verification of Requests

11 CCR § 999.324

§ 999.324. Verification for Password-Protected Accounts.

(a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 999.323. The business shall also require a consumer to re-authenticate themself before disclosing or deleting the consumer's data.

(b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to know or request to delete until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 999.325 to further verify the identity of the consumer.

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

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/14/22 Register 2022, No. 2

11 CCR § 999.324, 11 CA ADC § 999.324

§ 999.325. Verification for Non-Accountholders.

11 CA ADC § 999.325 BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 4. Verification of Requests

11 CCR § 999.325

§ 999.325. Verification for Non-Accountholders.

(a) If a consumer does not have or cannot access a password-protected account with a business, the business shall comply with this section, in addition to section 999.323.

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

(c) A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. If a business uses this method for verification, the business shall maintain all signed declarations as part of its record-keeping obligations.

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

(e) Illustrative examples follow:

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

(2) *Example 2*: If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the personal information. For example, a business may have a mobile application that collects personal information about the consumer but does not require an account. The business may determine whether, based on the facts and considering the factors set forth in section 999.323, subsection (b)(3), it may reasonably verify a consumer by asking them to provide information that only the person who used the mobile application may know or by requiring the consumer to respond to a notification sent to their device.

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

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

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

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/14/22 Register 2022, No. 2

11 CCR § 999.325, 11 CA ADC § 999.325

§ 999.326. Authorized Agent.

11 CA ADC § 999.326 BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 4. Verification of Requests

11 CCR § 999.326

§ 999.326. Authorized Agent.

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

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

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

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

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

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

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

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

2. Amendment of subsection (a), repealer and new subsection (a)(1) and new subsection (a)(2) filed 3-12-2021; operative 3-15-2021 pursuant to Government Code section 11343.4(b)(3) (Register 2021, No. 11). Filing deadline specified in Government Code section 11349.3(a) extended 60 calendar days pursuant to Executive Order N-40-20.

This database is current through 1/14/22 Register 2022, No. 2

11 CCR § 999.326, 11 CA ADC § 999.326

Article 5. Special Rules Regarding Consumers Under 16 Years of Age

§ 999.330. Consumers Under 13 Years of Age.

11 CA ADC § 999.330 BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 5. Special Rules Regarding Consumers Under 16 Years of Age

11 CCR § 999.330

§ 999.330. Consumers Under 13 Years of Age.

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

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

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

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

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

c. Having a parent or guardian call a toll-free telephone number staffed by trained personnel;

d. Having a parent or guardian connect to trained personnel via video-conference;

e. Having a parent or guardian communicate in person with trained personnel; and

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

(b) When a business receives an affirmative authorization pursuant to subsection (a), the business shall inform the parent or guardian of the right to opt-out and of the process for doing so on behalf of their child pursuant to section 999.315, subsections (a)-(f).

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

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

HISTORY

1. New article 5 (sections 999.330-999.332) and section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/14/22 Register 2022, No. 2

11 CCR § 999.330, 11 CA ADC § 999.330

§ 999.331. Consumers 13 to 15 Years of Age.

11 CA ADC § 999.331 BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 5. Special Rules Regarding Consumers Under 16 Years of Age

11 CCR § 999.331

§ 999.331. Consumers 13 to 15 Years of Age.

(a) A business that has actual knowledge that it sells the personal information of consumers at least 13 years of age and less than 16 years of age shall establish, document, and comply with a reasonable process for allowing such consumers to opt-in to the sale of their personal information, pursuant to section 999.316.

(b) When a business receives a request to opt-in to the sale of personal information from a consumer at least 13 years of age and less than 16 years of age, the business shall inform the consumer of the right to opt-out at a later date and of the process for doing so pursuant to section 999.315.

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

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/14/22 Register 2022, No. 2

11 CCR § 999.331, 11 CA ADC § 999.331

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

11 CA ADC § 999.332 BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 5. Special Rules Regarding Consumers Under 16 Years of Age

11 CCR § 999.332

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

(a) A business subject to sections 999.330 and/or 999.331 shall include a description of the processes set forth in those sections in its privacy policy.

(b) A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell the personal information without the affirmative authorization of consumers at least 13 years of age and less than 16 years of age, or the affirmative authorization of their parent or guardian for consumers under 13 years of age, is not required to provide the notice of right to opt-out.

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

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

2. Amendment of subsection (a) filed 3-12-2021; operative 3-15-2021 pursuant to Government Code section 11343.4(b)(3) (Register 2021, No. 11). Filing deadline specified in Government Code section 11349.3(a) extended 60 calendar days pursuant to Executive Order N-40-20.

This database is current through 1/14/22 Register 2022, No. 2

11 CCR § 999.332, 11 CA ADC § 999.332

Article 6. Non-Discrimination

§ 999.336. Discriminatory Practices.

11 CA ADC § 999.336 BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 6. Non-Discrimination

11 CCR § 999.336

§ 999.336. Discriminatory Practices.

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

(b) A business may offer a financial incentive or price or service difference if it is reasonably related to the value of the consumer's data. If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference.

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

(d) Illustrative examples follow:

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

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

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

(4) *Example 4*: An online bookseller collects information about consumers, including their email addresses. It offers coupons to consumers through browser pop-up windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information that the bookseller has collected about them, including their email address and their browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide

coupons is discriminatory unless the value of the coupons is reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete with regard to the email address because the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(e) A business shall notify consumers of any financial incentive or price or service difference subject to Civil Code section 1798.125 that it offers in accordance with section 999.307.

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

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

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

HISTORY

1. New article 6 (sections 999.336-999.337) and section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/14/22 Register 2022, No. 2

11 CCR § 999.336, 11 CA ADC § 999.336

§ 999.337. Calculating the Value of Consumer Data

11 CA ADC § 999.337 BARCLAYS OFFICIAL CALIFORNIA CODE OF REGULATIONS

Barclays Official California Code of Regulations Currentness

Title 11. Law

Division 1. Attorney General

Chapter 20. California Consumer Privacy Act Regulations

Article 6. Non-Discrimination

11 CCR § 999.337

§ 999.337. Calculating the Value of Consumer Data

(a) A business offering a financial incentive or price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data. The business shall consider one or more of the following:

(1) The marginal value to the business of the sale, collection, or deletion of a consumer's data.

(2) The average value to the business of the sale, collection, or deletion of a consumer's data.

(3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers.

(4) Revenue generated by the business from sale, collection, or retention of consumers' personal information.

(5) Expenses related to the sale, collection, or retention of consumers' personal information.

(6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference.

(7) Profit generated by the business from sale, collection, or retention of consumers' personal information.

(8) Any other practical and reasonably reliable method of calculation used in good faith.

(b) For the purpose of calculating the value of consumer data, a business may consider the value to the business of the data of all natural persons in the United States and not just consumers.

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

HISTORY

1. New section filed 8-14-2020; operative 8-14-2020 pursuant to Government Code section 11343.4(b)(3) (Register 2020, No. 33).

This database is current through 1/14/22 Register 2022, No. 2

11 CCR § 999.337, 11 CA ADC § 999.337

FINAL REGULATIONS TEXT

CALIFORNIA PRIVACY PROTECTION AGENCY

TITLE 11. LAW

DIVISION 6. CALIFORNIA PRIVACY PROTECTION AGENCY

CHAPTER 1. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

Article 1. GENERAL PROVISIONS

§ 7000. Title and Scope.

(a) This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as "these regulations." These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have.

(b) A violation of these regulations shall constitute a violation of the CCPA and be subject to the remedies provided for therein.

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

§ 7001. Definitions.

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

~~(a) "Affirmative authorization" means an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a consumer under 13 years of age, it means that the parent or guardian has provided consent to the sale of the consumer's personal information in accordance with the methods set forth in section 7070. For consumers 13 years of age and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.~~

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

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

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

(d) ~~(c)~~ "Authorized agent" means a natural person or a business entity ~~registered with the Secretary of State to conduct business in California~~ that a consumer has authorized to act on their behalf subject to the requirements set forth in section 7063.

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

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

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

(h) ~~(g)~~ "COPPA" means the Children's Online Privacy Protection Act, 15 U.S.C. sections 6501 to 6506~~6508~~ and 16 Code of Federal Regulations part 312~~.5~~.

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

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

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

~~(k) "Household" means a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier.~~

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

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

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

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

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

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

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

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

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

(u) "Opt-out preference signal" means a signal that is sent by a platform, technology, or mechanism, on behalf of the consumer, that communicates the consumer choice to opt-out

of the sale and sharing of personal information and that complies with the requirements set forth in section 7025, subsection (b).

(v) ~~(o)~~ "Price or service difference" means (1) any difference in the price or rate charged for any goods or services to any consumer related to the collection, retention, ~~or~~ sale, or sharing of personal information, ~~including through the use of discounts, financial payments, or other benefits or penalties;~~ or (2) any difference in the level or quality of any goods or services offered to any consumer related to the collection, retention, ~~or~~ sale, or sharing of personal information, including the denial of goods or services to the consumer.

(w) ~~(p)~~ "Privacy policy," as referred to in Civil Code section 1798.130, subdivision (a)(5), means the statement that a business shall make available to consumers describing the business's ~~practices, both~~ online and offline Information Practices~~, regarding the collection, use, disclosure, and sale of personal information~~, and of the rights of consumers regarding their own personal information.

(x) "Request to correct" means a consumer request that a business correct inaccurate personal information that it maintains about the consumer, pursuant to Civil Code section 1798.106.

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

(z) ~~(r)~~ "Request to know" means a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections ~~1798.100,~~ 1798.110~~,~~ or 1798.115. It includes a request for any or all of the following:

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

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

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

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

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

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

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

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

~~less than 16~~ years of age~~, or by a consumer who had previously opted out of the sale of their personal information~~.

(cc) ~~(t)~~ "Request to opt-out of sale/sharing" means a consumer request that a business ~~not~~neither sell nor share the consumer's personal information to third parties, pursuant to Civil Code section 1798.120, subdivision (a).

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

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

(ff) "Right to know" means the consumer's right to request that a business disclose personal information that it has collected, sold, or shared about the consumer as set forth in Civil Code sections 1798.110 and 1798.115.

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

(hh) "Right to opt-out of sale/sharing" means the consumer's right to direct a business that sells or shares personal information about the consumer to third parties to stop doing so as set forth in Civil Code section 1798.120.

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

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

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

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

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

Note: Authority cited: Sections 1798.175 and 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130,

1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.175, ~~and~~ 1798.185, 1798.199.40, 1798.199.45, 1798.199.50, 1798.199.55 and 1798.199.65, Civil Code.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) The strength of the link between subsection (c)(1) and subsection (c)(2). For example, a strong link exists between the consumer's expectations that the personal information will be used to provide them with a requested service at the time of collection, and the use of the information to repair errors that impair the intended functionality of that requested service. This would weigh in favor of compatibility. By contrast, for example, a weak link exists between the consumer's reasonable expectations that the personal information will be collected to provide a requested cloud storage service at the time of collection, and the use of the information to research and develop an unrelated facial recognition service.

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

achieve the purpose identified in subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent, shall be based on the following:

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

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

(3) The existence of additional safeguards for the personal information to specifically address the possible negative impacts on consumers considered by the business in subsection (d)(2). For example, a business may consider encryption or automatic deletion of personal information within a specific window of time as potential safeguards.

(e) A business shall obtain the consumer's consent in accordance with section 7004 before collecting or processing personal information for any purpose that does not meet the requirements set forth in subsection (a).

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

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

§ 7003. Requirements for Disclosures and Communications to Consumers.

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

(b) Disclosures required under Article 2 shall also:

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

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

(3) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the policy in an alternative format.

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

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

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

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

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

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

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

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

(B) A choice to opt-in to the sale of personal information that provides only the two choices, "Yes" and "Ask me later," is not equal or symmetrical because there is

no option to decline the opt-in. "Ask me later" implies that the consumer has not declined but delayed the decision and that the business will continue to ask the consumer to opt-in. Framing the consumer's options in this manner impairs the consumer's ability to make a choice. An equal or symmetrical choice could be "Yes" and "No."

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

(3) Avoid language or interactive elements that are confusing to the consumer. The methods should not use double negatives. Toggles or buttons must clearly indicate the consumer's choice. Illustrative examples follow.

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

(B) Toggles or buttons that state "on" or "off" may be confusing to a consumer and may require further clarifying language.

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

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

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

(B) Bundling choices so that the consumer is only offered the option to consent to using personal information for purposes that meet the requirements set forth in section 7002, subsection (a), together with purposes that are incompatible with the context in which the personal information was collected is a choice architecture that impairs or interferes with the consumer's ability to make a choice. For example, a business that provides a location-based service, such as a mobile application that posts gas prices within the consumer's location, shall not require

the consumer to consent to incompatible uses (*e.g.*, sale of the consumer's geolocation to data brokers) together with a reasonably necessary and proportionate use of geolocation information for providing the location-based services, which does not require consent. This type of choice architecture does not allow consent to be freely given, specific, informed, or unambiguous because it requires the consumer to consent to incompatible uses in order to obtain the expected service. The business should provide the consumer a separate option to consent to the business's use of personal information that does not meet the requirements set forth in section 7002, subsection (a).

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

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

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

(C) Businesses that require the consumer to unnecessarily wait on a webpage as the business processes the request may be in violation of this regulation.

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

(c) A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice. A business's intent in designing the interface is not determinative in whether the user interface is a dark pattern, but a factor to be considered. If a business did not intend to design the user interface to subvert or impair user choice, but the business knows of and does not remedy a user interface that has that effect, the user interface may still be a dark pattern. Similarly, a business's deliberate ignorance of the effect of its user interface may also weigh in favor of establishing a dark pattern.

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

ARTICLE 2. ~~NOTICES~~REQUIRED DISCLOSURES TO CONSUMERS

§ 7010. Overview of Required ~~Notices~~ Disclosures.

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

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

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

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

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

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

§ 7011. Privacy Policy.

(a) ~~Purpose and General Principles (1)~~ The purpose of the privacy policy is to provide consumers with a comprehensive description of a business's online and offline Information ~~p~~Practices ~~regarding the collection, use, disclosure, and sale of personal information~~. It shall also inform consumers about ~~and of~~ the rights ~~of consumers~~ they have regarding their personal information and provide any information necessary for them to exercise those rights.

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

(c) ~~(2)~~ The privacy policy shall ~~be designed and presented in a way that is easy to read and understandable to consumers. The policy shall:~~

~~(A) Use plain, straightforward language and avoid technical or legal jargon.~~

~~(B) Use a format that makes the policy readable, including on smaller screens, if applicable.~~

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

~~(D) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the policy in an alternative format. (E) B~~be available in a format that allows a consumer to print it out as a document.

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

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

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

(A) Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described using the specific terms set forth in Civil Code section 1798.140, subdivisions (v)(1)(A) to (K) and (ae)(1) to (3). To the extent that the business has discretion in its description, the business shall describe the category in a manner that provides consumers a meaningful understanding of the information being collected.

(B) Identification of the categories of sources from which the personal information is collected.

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

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

(E) For each category of personal information identified in subsection (e)(1)(D), the categories of third parties to whom the information was sold or shared.

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

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

(H) Identification of the categories of personal information, if any, that the business has disclosed for a business purpose to third parties in the preceding 12 months. If the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(I) For each category of personal information identified in subsection (e)(1)(H), the categories of third parties to whom the information was disclosed.

(J) Identification of the specific business or commercial purpose for disclosing the consumer's personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is disclosed.

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

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

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

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

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

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

(E) If the business uses or discloses sensitive personal information for reasons other than those set forth in section 7027, subsection (m), the right to limit the use or disclosure of sensitive personal information by the business.

(F) The right not to receive discriminatory treatment by the business for the exercise of privacy rights conferred by the CCPA, including an employee's, applicant's, or independent contractor's right not to be retaliated against for the exercise of their CCPA rights.

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

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

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

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

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

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

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

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

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

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

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

(4) Date the privacy policy was last updated.

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

~~(1) Right to Know About Personal Information Collected, Disclosed, or Sold.~~

~~a. Explanation that a consumer has the right to request that the business disclose what personal information it collects, uses, discloses, and sells.~~

b. Instructions for submitting a verifiable consumer request to know and links to an online request form or portal for making the request, if offered by the business.

c. General description of the process the business will use to verify the consumer request, including any information the consumer must provide.

d. Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described in a manner that provides consumers a meaningful understanding of the information being collected.

e. Identification of the categories of sources from which the personal information is collected.

f. Identification of the business or commercial purpose for collecting or selling personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected or sold.

g. Disclosure or Sale of Personal Information.

1. Identification of the categories of personal information, if any, that the business has disclosed for a business purpose or sold to third parties in the preceding 12 months.

2. For each category of personal information identified, the categories of third parties to whom the information was disclosed or sold.

3. Statement regarding whether the business has actual knowledge that it sells the personal information of consumers under 16 years of age.

(2) Right to Request Deletion of Personal Information.

a. Explanation that the consumer has a right to request the deletion of their personal information collected by the business.

b. Instructions for submitting a verifiable consumer request to delete and links to an online request form or portal for making the request, if offered by the business.

c. General description of the process the business will use to verify the consumer request, including any information the consumer must provide.

(3) Right to Opt-Out of the Sale of Personal Information.

a. Explanation that the consumer has a right to opt-out of the sale of their personal information by a business.

b. Statement regarding whether or not the business sells personal information. If the business sells personal information, include either the contents of the notice of right to opt-out or a link to it in accordance with section 7013.

(4) Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights.

a. Explanation that the consumer has a right not to receive discriminatory treatment by the business for the exercise of the privacy rights conferred by the CCPA.

(5) Authorized Agent.

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

(6) Contact for More Information.

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

(7) Date the privacy policy was last updated.

(8) If subject to the requirements set forth in section 7102, subsection (a), the information compiled in section 7102, subsection (a)(1), or a link to it.

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

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

§ 7012. Notice at Collection of Personal Information.

(a) Purpose and General Principles (1) The purpose of the nNotice at eCollection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them, and the purposes for which the personal information will be used. is collected or used, and whether that information is sold or shared, so that consumers have a tool to exercise meaningful control over the business's use of their personal information. For example, upon receiving the Notice at Collection, the consumer can use the information in the notice as a tool to choose whether to engage with the business, or to direct the business not to sell or share their personal information and to limit the use and disclosure of their sensitive personal information.

(2) The notice at collection shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:

(A) Use plain, straightforward language and avoid technical or legal jargon.

(B) Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.

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

~~(D) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.~~

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

(c) ~~(3)~~ The ~~n~~Notice at ~~c~~Collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information. Illustrative examples follow.~~:~~

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

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

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

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

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

~~(4) When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection. For example, if the business offers a flashlight application and the application collects geolocation information, the business shall provide a just-in-time notice, such as through a pop-up window when the consumer opens the application, that contains the information required by this subsection.~~

~~(5) A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection.~~

(d) ~~(6)~~ If a business does not give the ~~n~~Notice at ~~c~~Collection to the consumer at or before the point of collection of their personal information, the business shall not collect personal information from the consumer.

(e) ~~(b)~~ A business shall include the following in its ~~n~~Notice at ~~c~~Collection:

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

(2) The ~~business or commercial~~ purpose(s) for which the categories of personal information, including categories of sensitive personal information, are collected ~~will be~~ and used.

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

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

(5) ~~(3)~~ If the business sells or shares personal information, the link to the Notice of Right to Opt-out of Sale/Sharing ~~titled "Do Not Sell or Share My Personal Information" required by section 7026, subsection (a)~~, or in the case of offline notices, where the webpage can be found online.

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

(f) ~~(c)~~ If a business collects personal information from a consumer online, the ~~n~~Notice at ~~c~~Collection may be given to the consumer by providing a link that takes the consumer directly to the specific section of the business's privacy policy that contains the information required in subsection ~~(b)~~(e)(1) through (6). Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain the required information, so that the consumer is required to scroll through other information in order to determine the categories of personal information to be collected and/or whether the business sells or shares the personal information collected, does not satisfy this standard.

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

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

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

(3) Illustrative examples follow.

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

(B) Business H, a coffee shop, allows Business I, a business providing Wi-Fi services, to collect personal information from consumers using Business I's services on Business H's premises. Business H may post conspicuous signage at the entrance of the store or at the point-of-sale directing consumers to where the Notice at Collection for Business H can be found online. In addition, Business I shall post its own Notice at Collection on the first webpage or other interface consumers see before connecting to the Wi-Fi services offered.

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

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

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

~~(f) A business collecting employment-related information shall comply with the provisions of section 7012, except with regard to the following:~~

~~(1) The notice at collection of employment-related information does not need to include the link or web address to the link titled "Do Not Sell My Personal Information".~~

~~(2) The notice at collection of employment-related information is not required to provide a link to the business's privacy policy.~~

~~(g) Subsection (f) shall become inoperative on January 1, 2021, unless the CCPA is amended otherwise.~~

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

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

(a) ~~Purpose and General Principles. (1)~~ The purpose of the ~~n~~Notice of ~~r~~Right to ~~o~~Opt-out of Sale/Sharing is to inform consumers of their right to direct a business that sells or shares their personal information to stop selling or sharing their personal information and to provide them with the opportunity to exercise that right. The purpose of the "Do Not Sell or Share My Personal Information" link is to immediately effectuate the consumer's right to opt-out of sale/sharing, or in the alternative, direct the consumer to the Notice of Right to Opt-out of Sale/Sharing. Accordingly, clicking the business's "Do Not Sell or Share My Personal Information" link will either have the immediate effect of opting the consumer out of the sale or sharing of personal information or lead the consumer to a webpage where the consumer can learn about and make that choice.

~~(2) The notice of right to opt-out shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:~~

~~(A) Use plain, straightforward language and avoid technical or legal jargon.~~

~~(B) Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.~~

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

~~(D) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.~~

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

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

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

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

(1) A business shall post the ~~n~~Notice of ~~r~~Right to ~~o~~Opt-out of Sale/Sharing on the ~~I~~internet webpage to which the consumer is directed after clicking on the "Do Not Sell or Share My Personal Information" link ~~on the website homepage or the download or landing page of a mobile application. In addition, a business that collects personal information through a mobile application may provide a link to the notice within the application, such as through the application's settings menu~~. The notice shall include the information specified in subsection (~~e~~f) or be a link that takes the consumer directly to the specific section of the business's privacy policy that contains the same information. If clicking on the "Do Not Sell or Share My Personal Information" link immediately effectuates the consumer's right to opt-out of sale/sharing or if the business processes opt-out preference signals in a frictionless manner and chooses not to post a link, the business shall provide the notice within its privacy policy.

(2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to opt-out of sale/sharing. That method shall comply with the requirements set forth in section 7004 ~~subsection (a)(2)~~.

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

(A) A business that sells or shares personal information that it collects in the course of interacting with consumers offline, such as in a brick-and-mortar store, shall ~~also inform consumers by an offline method of their right to opt-out and provide instructions on how to submit a request to opt-out~~ provide notice through an offline method, e.g., ~~. Illustrative examples follow: (A) A business that sells personal information that it collects from consumers in a brick-and-mortar store may inform consumers of their right to opt-out~~ on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the notice ~~opt-out information~~ can be found online.

(B) A business that sells or shares personal information that it collects over the phone ~~may~~ shall provide notice ~~inform consumers of their right to opt-out~~ orally during the call when the information is collected.

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

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

(2) Instructions on how the consumer can submit a request to opt-out of sale/sharing. If notice is provided online, the notice shall include t~~T~~he interactive form by which the consumer can submit their request to opt-out of sale/sharing online, as required by section 7026, subsection (a)(1). ~~, or i~~If the business does not operate a website, the notice shall explain the offline method by which the consumer can submit their request to opt-out of sale/sharing.~~; and~~

~~(3) Instructions for any other method by which the consumer may submit their request to opt-out.~~

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

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

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

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

~~(f) Opt-Out Icon.~~

~~(1) The following opt-out icon may be used in addition to posting the notice of right to opt-out, but not in lieu of any requirement to post the notice of right to opt-out or a "Do Not Sell My Personal Information" link as required by Civil Code section 1798.135 and these regulations.~~

~~(2) The icon shall be approximately the same size as any other icons used by the business on its webpage.~~

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

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

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

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

(c) The "Limit the Use of My Sensitive Personal Information" link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business's internet Homepage(s).

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

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

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

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

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

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

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

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

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

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

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

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

§ 7015. Alternative Opt-Out Link.

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

webpage that would inform them of both their right to opt-out of sale/sharing and right to limit and provide them with the opportunity to exercise both rights.

(b) A business that chooses to use an Alternative Opt-out Link shall title the link, "Your Privacy Choices" or "Your California Privacy Choices," and shall include the following opt-out icon adjacent to the title. The link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business's internet Homepage(s). The icon shall be approximately the same size as other icons used by the business in the header or footer of its webpage.

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

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

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

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

§ 7016. Notice of Financial Incentive.

(a) ~~Purpose and General Principles. (1)~~ The purpose of the ~~n~~Notice of ~~f~~Financial ~~i~~Incentive is to explain to the consumer the material terms of a financial incentive or price or service difference the business is offering so that the consumer may make an informed decision about whether to participate. A business that does not offer a financial incentive or price or service difference is not required to provide a ~~n~~Notice of ~~f~~Financial ~~i~~Incentive.

(b) The Notice of Financial Incentive shall comply with section 7003, subsections (a) and (b).

(c) ~~(2)~~ The ~~n~~Notice of ~~f~~Financial ~~i~~Incentive shall be ~~designed and presented in a way that is easy to read and understandable to consumers. The notice shall:~~

~~(A) Use plain, straightforward language and avoid technical or legal jargon.~~

~~(B) Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.~~

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

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

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

~~(E) Be~~ readily available where consumers will encounter it before opting-in to the financial incentive or price or service difference. ~~(3)~~ If the business offers the financial incentive or price or service difference online, the notice may be given by providing a link that takes the consumer directly to the specific section of a business's privacy policy that contains the information required in subsection (~~b~~d).

(d) ~~(b)~~ A business shall include the following in its ~~n~~Notice of ~~f~~Financial ~~i~~Incentive:

(1) A succinct summary of the financial incentive or price or service difference offered;

(2) A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data;

(3) How the consumer can opt-in to the financial incentive or price or service difference;

(4) A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and

(5) An explanation of how the ~~financial incentive or~~ price or service difference is reasonably related to the value of the consumer's data, including:

(A) A good-faith estimate of the value of the consumer's data that forms the basis for offering the ~~financial incentive or~~ price or service difference; and

(B) A description of the method(s) the business used to calculate the value of the consumer's data.

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

ARTICLE 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

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

(a) A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to delete, requests to correct, and requests to know. ~~All other businesses shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.~~

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

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

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

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

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

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

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

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

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

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

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

§ 7022. Requests to Delete.

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

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

(1) Permanently and completely erasing the personal information ~~on~~ from its existing systems ~~with the~~ except~~ion of~~ archived or back-up systems~~; (2) D~~, deidentifying the personal information~~; (3) A~~, or aggregating the consumer information;~~.~~

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

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

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

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

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

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

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

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

(e) ~~(d)~~ In responding to a request to delete, a business shall inform the consumer whether ~~or not~~ it has complied with the consumer's request. ~~(c) If the business complies with the consumer's request, t~~The business shall also inform the consumer that it will maintain a record of the request as required by section ~~7030~~ 7101, subsection ~~(b)~~(a). A business, service provider, contractor, or third party may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from ~~the business's~~ its records.

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

(1) ~~Inform the consumer that it will not comply with the consumer's request and describe~~Provide to the consumer a detailed explanation of the basis for the denial, including any conflict with federal or state law, ~~or~~ exception to the CCPA, or factual basis for contending that compliance would be impossible or involve disproportionate effort, unless prohibited from doing so by law~~;~~.

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

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

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

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

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

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

§ 7023. Requests to Correct.

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

(b) In determining the accuracy of the personal information that is the subject of a consumer's request to correct, the business shall consider the totality of the circumstances relating to the contested personal information. A business may deny a consumer's request to correct if it determines that the contested personal information is more likely than not accurate based on the totality of the circumstances.

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

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

(B) How the business obtained the contested information.

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

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

(c) A business that complies with a consumer's request to correct shall correct the personal information at issue on its existing systems. The business shall also instruct all service

providers and contractors that maintain the personal information at issue pursuant to their written contract with the business to make the necessary corrections in their respective systems. Service providers and contractors shall comply with the business's instructions to correct the personal information or enable the business to make the corrections. If a business, service provider, or contractor stores any personal information that is the subject of the request to correct on archived or backup systems, it may delay compliance with the consumer's request to correct, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or used.

(d) Documentation.

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

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

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

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

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

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

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

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

(e) A business may delete the contested personal information as an alternative to correcting the information if the deletion of the personal information does not negatively impact the consumer, or the consumer consents to the deletion. For example, if deleting instead of correcting inaccurate personal information would make it harder for the consumer to obtain

a job, housing, credit, education, or other type of opportunity, the business shall process the request to correct or obtain the consumer's consent to delete the information.

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

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

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

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

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

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

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

(i) Where the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer's request, the business may provide the consumer with the name of the source from which the business received the alleged inaccurate information.

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

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

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

§ 7024. Requests to Know.

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

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

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

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

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

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

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

(d) A business shall not disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. The business shall, however, inform the consumer with sufficient particularity that it has collected the type of information. For example, a business shall respond that it collects "unique biometric data including a fingerprint scan" without disclosing the actual fingerprint scan data.

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

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

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

(h) In response to a request to know, a business shall provide all the personal information it has collected and maintains about the consumer on or after January 1, 2022, including beyond the 12-month period preceding the business's receipt of the request, unless doing so proves impossible or would involve disproportionate effort, or the consumer requests data for a specific time period. That information shall include any personal information that the business's service providers or contractors Collected pursuant to their written contract with the business. If a business claims that providing personal information beyond the 12-month

period would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot provide personal information beyond the 12-month period. The business shall not simply state that it is impossible or would require disproportionate effort. ~~Unless otherwise specified by the business to cover a longer period of time, the 12-month period covered by a consumer's verifiable request to know referenced in Civil Code section 1798.130, subdivision (a)(2), shall run from the date the business receives the request, regardless of the time required to verify the request.~~

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

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

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

(1) The categories of personal information the business has collected about the consumer ~~in the preceding 12 months;~~.

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

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

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

(5) The categories of personal information that the business sold ~~in the preceding 12 months~~, and for each category identified, the categories of third parties to whom it sold that particular category of personal information~~; and~~.

(6) The categories of personal information that the business disclosed for a business ~~p~~Purpose ~~in the preceding 12 months~~, and for each category identified, the categories of third parties to whom it disclosed that particular category of personal information.

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

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

§ 7025. Opt-Out Preference Signals.

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

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

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

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

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

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

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

(3) If the opt-out preference signal conflicts with a consumer's business-specific privacy setting that allows the business to sell or share their personal information, the business

shall process the opt-out preference signal as a valid request to opt-out of sale/sharing, but may notify the consumer of the conflict and provide the consumer with an opportunity to consent to the sale or sharing of their personal information. The business shall comply with section 7004 in obtaining the consumer's consent to the sale or sharing of their personal information. If the consumer consents to the sale or sharing of their personal information, the business may ignore the opt-out preference signal for as long as the consumer is known to the business.

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

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

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

(7) Illustrative examples follow.

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

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

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

(D) Ramona participates in Business P's financial incentive program where she receives coupons in exchange for allowing the business to pseudonymously track and share her online browsing habits to marketing partners. Ramona enables an opt-out preference signal on her browser and then visits Business P's website. Business P knows that it is Ramona through a cookie that has been placed on her browser, but also detects the opt-out preference signal. Business P may ignore the opt-out preference signal and notify Ramona that her opt-out preference signal conflicts with her participation in the financial incentive program and ask whether she intends to withdraw from the financial incentive program. If Ramona does not affirm her intent to withdraw, Business P may ignore the opt-out preference signal and place Ramona on a whitelist so that Business P does not have to notify Ramona of the conflict again.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing. ~~, including an interactive form accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," on the business's website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email~~

~~address, a form submitted in person, a form submitted through the mail, and user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information. (b)~~ A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the ~~sells~~ personal information that it makes available to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow.

(1) ~~(c) If a~~ A business that collects personal information from consumers online~~, the business~~ shall, at a minimum, allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and at least one of the following methods—an interactive form accessible via the "Do Not Sell or Share My Personal Information" link, the Alternative Opt-out Link, or the business's privacy policy if the business processes an opt-out preference signal in a frictionless manner. ~~treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer. (1) Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information. (2) If a global privacy control conflicts with a consumer's existing business-specific privacy setting or their participation in a business's financial incentive program, the business shall respect the global privacy control but may notify the consumer of the conflict and give the consumer the choice to confirm the business-specific privacy setting or participation in the financial incentive program.~~

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

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

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

(b) ~~(h)~~ A business's methods for submitting requests to opt-out of sale/sharing shall be easy for consumers to execute, ~~and~~ shall require minimal steps, and shall comply with section 7004 ~~to allow the consumer to opt-out~~. ~~A business shall not use a method is designed with the~~

~~purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out. Illustrative examples follow:~~

~~(1) The business's process for submitting a request to opt-out shall not require more steps than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a request to opt-out is measured from when the consumer clicks on the "Do Not Sell My Personal Information" link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request.~~

~~(2) A business shall not use confusing language, such as double-negatives (e.g., "Don't Not Sell My Personal Information"), when providing consumers the choice to opt-out.~~

~~(3) Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request.~~

~~(4) The business's process for submitting a request to opt-out shall not require the consumer to provide personal information that is not necessary to implement the request.~~

~~(5) Upon clicking the "Do Not Sell My Personal Information" link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out.~~

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

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

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

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

(1) Ceasing to sell to and/or share with third parties the consumer's personal information as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. Service providers or contractors Collecting personal information

pursuant to the written contract with the business required by the CCPA and these regulations does not constitute a sale or sharing of personal information. ~~If a business sells a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request, it shall notify those third parties that the consumer has exercised their right to opt-out and shall direct those third parties not to sell that consumer's information.~~

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

(g) A business may provide a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business. For example, the business may display on its website "Consumer Opted Out of Sale/Sharing" or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.

(h) ~~(d)~~ In responding to a request to opt-out of sale/sharing, a business may present the consumer with the choice to opt-out of the sale or sharing ~~for certain uses~~ of personal information for certain uses as long as a ~~global~~ single option to opt-out of the sale or sharing of all personal information is also offered ~~more prominently presented than the other choices~~. However, doing so in response to an opt-out preference signal will prevent the business from using the exception set forth in Civil Code section 1798.135, subdivision (b)(1).

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

(j) ~~(f)~~ A consumer may use an authorized agent to submit a request to opt-out of sale/sharing on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent ~~cannot~~ does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. The requirement to obtain and provide written permission from the consumer does not apply to requests made by an opt-out preference signal. ~~User-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.~~

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

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

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

(a) The unauthorized use or disclosure of sensitive personal information creates a heightened risk of harm for the consumer. The purpose of the request to limit is to give consumers meaningful control over how their sensitive personal information is collected, used, and disclosed. It gives the consumer the ability to limit the business's use of sensitive personal information to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, with some narrowly tailored exceptions, which are set forth in subsection (m). Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to requests to limit.

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

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

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

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

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

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

(d) A business shall not require a consumer submitting a request to limit to create an account or provide additional information beyond what is necessary to direct the business to limit the use or disclosure of the consumer's sensitive personal information.

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

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

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

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

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

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

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

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

(j) A consumer may use an authorized agent to submit a request to limit on the consumer's behalf if the consumer provides the authorized agent written permission signed by the

consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf.

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

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

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

(1) To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services. For example, a consumer's precise geolocation may be used by a mobile application that is providing the consumer with directions on how to get to specific location. A consumer's precise geolocation may not, however, be used by a gaming application where the average consumer would not expect the application to need this piece of sensitive personal information.

(2) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information. For example, a business may disclose a consumer's log-in information to a data security company that it has hired to investigate and remediate a data breach that involved that consumer's account.

(3) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions. For example, a business may use information about a consumer's ethnicity and/or the contents of email and text messages to investigate claims of racial discrimination or hate speech.

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

(5) For short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business. For example, a business that sells religious books can use information about its customers' interest in its religious content to serve

contextual advertising for other kinds of religious merchandise within its store or on its website, so long as the business does not use sensitive personal information to create a profile about an individual consumer or disclose personal information that reveals consumers' religious beliefs to third parties.

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

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

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

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

§ 7028. Requests to Opt-In After Opting-Out of the Sale or Sharing of Personal Information.

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

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

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

~~**§ 7031. Requests to Know or Delete Household Information.**~~

~~(a) Where a household does not have a password-protected account with a business, a business shall not comply with a request to know specific pieces of personal information about the household or a request to delete household personal information unless all of the following conditions are satisfied:~~

~~(1) All consumers of the household jointly request to know specific pieces of information for the household or the deletion of household personal information;~~

~~(2) The business individually verifies all the members of the household subject to the verification requirements set forth in section 7062; and~~

~~(3) The business verifies that each member making the request is currently a member of the household.~~

~~(b) Where a consumer has a password-protected account with a business that collects personal information about a household, the business may process requests to know and requests to delete relating to household information through the business's existing business practices and in compliance with these regulations.~~

~~(c) If a member of a household is a consumer under the age of 13, a business must obtain verifiable parental consent before complying with a request to know specific pieces of information for the household or the deletion of household personal information pursuant to the parental consent provisions in section 7070.~~

~~*Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.140 and 1798.185, Civil Code.*~~

ARTICLE 4. SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES

§ 7050.~~§ 7051.~~ Service Providers and Contractors.

~~(a) A business that provides services to a person or organization that is not a business, and that would otherwise meet the requirements and obligations of a "service provider" under the CCPA and these regulations, shall be deemed a service provider for purposes of the CCPA and these regulations.~~

~~(b) To the extent that a business directs a second entity to collect personal information directly from a consumer, or about a consumer, on the first business's behalf, and the second entity would otherwise meet the requirements and obligations of a "service provider" under the CCPA and these regulations, the second entity shall be deemed a service provider of the first business for purposes of the CCPA and these regulations.~~

(a) ~~(c)~~ A service provider or contractor shall not retain, use, or disclose personal information Collected pursuant to its written contract with the business ~~obtained in the course of providing services~~ except:

~~(1) To process or maintain personal information on behalf of the business that provided the personal information or directed the service provider to collect the personal information~~

(1) For the specific Business Purpose(s) set forth in~~, and in compliance with~~ the written contract between the business and the service provider or contractor that is ~~for services~~ required by the CCPA and these regulations.~~;~~

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

(3) For internal use by the service provider or contractor to build or improve the quality of ~~its~~the services it is providing to the business, even if this Business Purpose is not specified in the written contract required by the CCPA and these regulations, provided that the service provider or contractor ~~use~~ does not use the personal information to perform services on behalf of another person ~~include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source;~~. Illustrative examples follow.

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

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

(4) To prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent or illegal activity, even if this Business Purpose is not specified in the written contract required by the CCPA and these regulations.~~; or~~

(5) For the purposes enumerated in Civil Code section 1798.145, subdivisions (a)(1) through (a)(74).

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

interaction with consumers. A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor with respect to cross-contextual behavioral advertising services. Illustrative examples follow.

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

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

~~(d) A service provider shall not sell data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business.~~

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

(d) ~~(f)~~ A service provider or contractor that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider or contractor.

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

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

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

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

§ 7051. Contract Requirements for Service Providers and Contractors.

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

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

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

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

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

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

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

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

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

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

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

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

(c) Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.

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

§ 7052. Third Parties.

(a) A third party that does not have a contract that complies with section 7053, subsection (a), shall not collect, use, process, retain, sell, or share the personal information that the business made available to it.

(b) A third party shall comply with the terms of the contract required by the CCPA and these regulations, which include treating the personal information that the business made available to it in a manner consistent with the business's obligations under the CCPA and these regulations.

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

§ 7053. Contract Requirements for Third Parties.

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

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

(2) Specifies that the business is making the personal information available to the third party only for the limited and specified purposes set forth within the contract and requires the third party to use it only for those limited and specified purposes.

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

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

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

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

(b) Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract might not be able to rely on the defense that it did not have reason to believe that the third party intends to use the personal information in violation of the CCPA and these regulations at the time of the business disclosed the personal information to the third party.

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

ARTICLE 5. VERIFICATION OF REQUESTS

§ 7060. General Rules Regarding Verification.

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

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

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

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

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

(3) Consider the following factors:

(A) The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive ~~or valuable~~ personal information shall warrant a more stringent verification process. ~~The types of personal information identified in Civil Code section 1798.81.5, subdivision (d), shall be considered presumptively sensitive;~~

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

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

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

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

(F) Available technology for verification.

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

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

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

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

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

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

§ 7061. Verification for Password-Protected Accounts.

(a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 7060. The business shall also require a consumer to re-authenticate themselves~~f~~ before ~~disclosing or~~ deleting, correcting, or disclosing the consumer's data.

(b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request ~~to know or request~~ to delete, request to correct, or request to know until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 7062 to further verify the identity of the consumer.

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

§ 7062. Verification for Non-Accountholders.

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

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

(c) A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. If a business uses this method for verification, the business shall maintain all signed declarations as part of its record-keeping obligations.

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

(e) Illustrative examples follow:

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

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

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

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

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

§ 7063. Authorized Agents.

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

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

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

(b) Subsection (a) does not apply when a consumer has provided the authorized agent with

power of attorney pursuant to Probate Code sections 4121 to 4130. A business shall not require power of attorney in order for a consumer to use an authorized agent to act on their behalf.

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

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

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

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

§ 7070. Consumers Less Than ~~Under~~ 13 Years of Age.

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

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

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

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

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

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

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

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

(F) Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information, as long as the parent

or guardian's identification is deleted by the business from its records promptly after such verification is complete.

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

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

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

§ 7071. Consumers at Least 13 Years of Age and Less Than 16 ~~to 15~~ Years of Age.

(a) A business that has actual knowledge that it sells or shares the personal information of consumers at least 13 years of age and less than 16 years of age shall establish, document, and comply with a reasonable process for allowing such consumers to opt-in to the sale or sharing of their personal information, pursuant to section 7028.

(b) When a business receives a request to opt-in to the sale or sharing of personal information from a consumer at least 13 years of age and less than 16 years of age, the business shall inform the consumer of their ongoing right to opt-out of sale/sharing at any point in the future ~~a later date~~ and of the process for doing so pursuant to section 7026.

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

§ 7072. Notices to Consumers Less Than ~~Under~~ 16 Years of Age.

(a) A business subject to sections 7070 and/or 7071 shall include a description of the processes set forth in those sections in its privacy policy.

(b) A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell or share the personal information without the ~~affirmative authorization~~ consent of consumers at least 13 years of age and less than 16 years of age, or the ~~affirmative authorization~~ consent of their parent or guardian for consumers under 13 years of age, is not required to provide the ~~n~~Notice of ~~r~~Right to ~~o~~Opt-out of Sale/Sharing.

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

ARTICLE 7. NON-DISCRIMINATION

§ 7080. Discriminatory Practices.

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

(b) A business may offer a ~~financial incentive or~~ price or service difference that is non-discriminatory. A price or service difference is non-discriminatory if it is reasonably related to the value of the consumer's data. If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the ~~financial incentive or~~ price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the ~~financial incentive or~~ price or service difference.

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

(d) Illustrative examples follow:

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

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

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

(4) *Example 4:* An online bookseller collects information about consumers, including their email addresses. It offers coupons to consumers through browser pop-up

windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information that the bookseller has collected about them, including their email address and their browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide coupons is discriminatory unless the value of the coupons is reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete with regard to the email address because the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

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

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

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

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

§ 7081. Calculating the Value of Consumer Data

(a) A business offering a ~~financial incentive or~~ price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data. The business shall consider one or more of the following:

(1) The marginal value to the business of the sale, collection, or deletion of a consumer's data.

(2) The average value to the business of the sale, collection, or deletion of a consumer's data.

(3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers.

(4) Revenue generated by the business from sale, collection, or retention of consumers' personal information.

(5) Expenses related to the sale, collection, or retention of consumers' personal information.

(6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference.

(7) Profit generated by the business from sale, collection, or retention of consumers' personal information.

(8) Any other practical and reasonably reliable method of calculation used in good faith.

(b) For the purpose of calculating the value of consumer data, a business may consider the value to the business of the data of all natural persons in the United States and not just consumers.

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

ARTICLE 8. TRAINING~~,~~ AND RECORD-KEEPING

§ 7100. Training.

(a) All individuals responsible for handling consumer inquiries about the business's ~~privacy~~Information ~~p~~Practices or the business's compliance with the CCPA shall be informed of all of the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.

(b) A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.

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

§ 7101. Record-Keeping.

(a) A business shall maintain records of consumer requests made pursuant to the CCPA and how it responded to the requests for at least 24 months. The business shall implement and maintain reasonable security procedures and practices in maintaining these records.

(b) The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.

(c) A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.

(d) Information maintained for record-keeping purposes shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and these regulations. Information maintained for record-keeping purposes shall not be shared with any third party except as necessary to comply with a legal obligation.

(e) Other than as required by subsection (b), a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.

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

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

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

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

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

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

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

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

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

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

(2) Disclose, by July 1 of every calendar year, the information compiled in subsection (a)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy. ~~(A)~~ In its disclosure ~~pursuant to subsection (a)(2)~~, a business may choose to disclose the number of requests that it denied in whole or in

part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.

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

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

ARTICLE 9. INVESTIGATIONS AND ENFORCEMENT

§ 7300. Sworn Complaints Filed with the Agency.

(a) Requirements for filing a sworn complaint. Sworn complaints may be filed with the Enforcement Division via the electronic complaint system available on the Agency's website at https://cppa.ca.gov/ or submitted in person or by mail to the headquarters office of the Agency.

A complaint must:

(1) Identify the business, service provider, contractor, or person who allegedly violated the CCPA;

(2) State the facts that support each alleged violation and include any documents or other evidence supporting this conclusion;

(3) Authorize the alleged violator and Agency to communicate regarding the complaint, including disclosing the complaint and any information relating to the complaint;

(4) Include the name and current contact information of the complainant; and

(5) Be signed and submitted under penalty of perjury.

(b) The Enforcement Division will notify the complainant in writing of the action, if any, the Agency has taken or plans to take on the complaint, together with the reasons for that action or nonaction. Duplicate complaints submitted by the same complainant may be rejected without notice.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.199.45, Civil Code.

§ 7301. Investigations.

(a) The Agency may initiate investigations from referrals from government agencies or private organizations, and sworn, nonsworn, or anonymous complaints, or on the Agency's own initiative.

(b) As part of the Agency's decision to pursue investigations of possible or alleged violations of the CCPA, the Agency may consider all facts it determines to be relevant, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good faith efforts to comply with those requirements.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.199.45, Civil Code.

§ 7302. Probable Cause Proceedings.

(a) Probable Cause. Under Civil Code section 1798.199.50, probable cause exists when the evidence supports a reasonable belief that the CCPA has been violated.

(b) Probable Cause Notice. The Enforcement Division will provide the alleged violator with notice of the probable cause proceeding as required by Civil Code section 1798.199.50.

(c) Probable Cause Proceeding.

(1) The proceeding shall be closed to the public unless the alleged violator files, at least 10 business days before the proceeding, a written request for a public proceeding. If the proceeding is not open to the public, then the proceeding may be conducted in whole or in part by telephone or videoconference.

(2) The Agency shall conduct the proceeding informally. Only the alleged violator(s), their legal counsel, and Enforcement Division shall have the right to participate at the proceeding. The Agency shall determine whether there is probable cause based on the probable cause notice and any information or arguments presented at the probable cause proceeding by the parties.

(3) If the alleged violator(s) fails to participate or appear at the probable cause proceeding, the alleged violator(s) waives the right to further probable cause proceedings under Civil Code section 1798.199.50, and the Agency shall determine whether there is probable cause based on the notice and any information or argument provided by the Enforcement Division.

(d) Probable Cause Determination. The Agency shall issue a written decision with its probable cause determination and serve it on the alleged violator electronically or by mail. The Agency's probable cause determination is final and not subject to appeal.

(e) Notices of probable cause and probable cause determinations shall not be open to the public nor admissible in evidence in any action or special proceeding other than one enforcing the CCPA.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.199.50, Civil Code.

§ 7303. Stipulated Orders.

(a) At any time before or during an administrative hearing and in lieu of such a hearing, the Head of Enforcement and the alleged violator may stipulate to the entry of a final order. If a stipulation has been agreed upon and the scheduled date of the hearing is set to occur before the next Board meeting, the Enforcement Division will apply for a continuance of the hearing.

(b) The final order must be approved by the Board, which may consider the matter in closed session.

(c) The stipulated final order shall be public and have the force of an order of the Board.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.199.35 and 1798.199.55, Civil Code.

§ 7304. Agency Audits.

(a) Scope. The Agency may audit a business, service provider, contractor, or person to ensure compliance with any provision of the CCPA.

(b) Criteria for Selection. The Agency may conduct an audit to investigate possible violations of the CCPA. Alternatively, the Agency may conduct an audit if the subject's collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law.

(c) Audits may be announced or unannounced as determined by the Agency.

(d) Failure to Cooperate. A subject's failure to cooperate during the Agency's audit may result in the Agency issuing a subpoena, seeking a warrant, or otherwise exercising its powers to ensure compliance with the CCPA.

(e) Protection of Personal Information. Consumer personal information disclosed to the Agency during an audit shall be maintained in compliance with the Information Practices Act of 1977, Civil Code section 1798, et seq.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.185, 1798.199.40 and 1798.199.65, Civil Code; Section 11180, Government Code.

KILPATRICK TOWNSEND

Colorado Privacy Act

On July 7, the Colorado Privacy Act ("CPA") was signed into law, making the CPA the third comprehensive data privacy law passed in the United States.

The CPA will take effect on July 1, 2023. The full text of the CPA is provided below.

Please see the Comprehensive Data Privacy Law Quick Reference Guide for a high-level comparison of the requirements of the CPA compared to other comprehensive data privacy laws.

CPA Official Text:

SENATE BILL 21-190[1]

BY SENATOR(S) Rodriguez and Lundeen, Bridges, Buckner, Coleman, Cooke, Danielson, Donovan, Fenberg, Gardner, Ginal, Gonzales, Hansen, Hisey, Holbert, Jaquez Lewis, Kirkmeyer, Kolker, Lee, Liston, Moreno, Pettersen, Priola, Rankin, Scott, Simpson, Sonnenberg, Story, Winter, Woodward, Garcia; also REPRESENTATIVE(S) Duran and Carver, Bernett, Bird, Cutter, Exum, Gonzales-Gutierrez, Gray, Herod, Jodeh, Lynch, McCluskie, McCormick, Mullica, Ricks, Snyder, Titone, Valdez A., Woodrow.

CONCERNING ADDITIONAL PROTECTION OF DATA RELATING TO PERSONAL PRIVACY.

Be it enacted by the General Assembly of the State of Colorado:

SECTION 1. In Colorado Revised Statutes, add part 13 to article 1 of title 6 as follows:

PART 13

COLORADO PRIVACY ACT

6-1-1301. Short title. THE SHORT TITLE OF THIS PART 13 IS THE "COLORADO PRIVACY ACT".

6-1-1302. Legislative declaration. (1) THE GENERAL ASSEMBLY HEREBY:

(a) FINDS THAT:

(I) THE PEOPLE OF COLORADO REGARD THEIR PRIVACY AS A FUNDAMENTAL RIGHT AND AN ESSENTIAL ELEMENT OF THEIR INDIVIDUAL FREEDOM;

(II) COLORADO'S CONSTITUTION EXPLICITLY PROVIDES THE RIGHT TO PRIVACY UNDER SECTION 7 OF ARTICLE II, AND FUNDAMENTAL PRIVACY RIGHTS HAVE LONG BEEN, AND CONTINUE TO BE, INTEGRAL TO PROTECTING COLORADANS AND TO SAFEGUARDING OUR DEMOCRATIC REPUBLIC;

[1] Capital letters or bold & italic numbers indicate new material added to existing law; dashes through words or numbers indicate deletions from existing law and such material is not part of the act.

(III) ONGOING ADVANCES IN TECHNOLOGY HAVE PRODUCED EXPONENTIAL GROWTH IN THE VOLUME AND VARIETY OF PERSONAL DATA BEING GENERATED, COLLECTED, STORED, AND ANALYZED AND THESE ADVANCES PRESENT BOTH PROMISE AND POTENTIAL PERIL;

(IV) THE ABILITY TO HARNESS AND USE DATA IN POSITIVE WAYS IS DRIVING INNOVATION AND BRINGS BENEFICIAL TECHNOLOGIES TO SOCIETY, BUT IT HAS ALSO CREATED RISKS TO PRIVACY AND FREEDOM; AND

(V) THE UNAUTHORIZED DISCLOSURE OF PERSONAL INFORMATION AND LOSS OF PRIVACY CAN HAVE DEVASTATING IMPACTS RANGING FROM FINANCIAL FRAUD, IDENTITY THEFT, AND UNNECESSARY COSTS IN PERSONAL TIME AND FINANCES TO DESTRUCTION OF PROPERTY, HARASSMENT, REPUTATIONAL DAMAGE, EMOTIONAL DISTRESS, AND PHYSICAL HARM;

(b) DETERMINES THAT:

(I) TECHNOLOGICAL INNOVATION AND NEW USES OF DATA CAN HELP SOLVE SOCIETAL PROBLEMS AND IMPROVE LIVES, AND IT IS POSSIBLE TO BUILD A WORLD WHERE TECHNOLOGICAL INNOVATION AND PRIVACY CAN COEXIST; AND

(II) STATES ACROSS THE UNITED STATES ARE LOOKING TO THIS PART 13 AND SIMILAR MODELS TO ENACT STATE-BASED DATA PRIVACY REQUIREMENTS AND TO EXERCISE THE LEADERSHIP THAT IS LACKING AT THE NATIONAL LEVEL; AND

(c) DECLARES THAT:

(I) BY ENACTING THIS PART 13, COLORADO WILL BE AMONG THE STATES THAT EMPOWER CONSUMERS TO PROTECT THEIR PRIVACY AND REQUIRE COMPANIES TO BE RESPONSIBLE CUSTODIANS OF DATA AS THEY CONTINUE TO INNOVATE;

(II) THIS PART 13 ADDRESSES ISSUES OF STATEWIDE CONCERN AND:

(A) PROVIDES CONSUMERS THE RIGHT TO ACCESS, CORRECT, AND DELETE PERSONAL DATA AND THE RIGHT TO OPT OUT NOT ONLY OF THE SALE OF PERSONAL DATA BUT ALSO OF THE COLLECTION AND USE OF PERSONAL DATA;

(B) IMPOSES AN AFFIRMATIVE OBLIGATION UPON COMPANIES TO SAFEGUARD PERSONAL DATA; TO PROVIDE CLEAR, UNDERSTANDABLE, AND TRANSPARENT INFORMATION TO CONSUMERS ABOUT HOW THEIR PERSONAL DATA ARE USED; AND TO STRENGTHEN COMPLIANCE AND ACCOUNTABILITY BY REQUIRING DATA PROTECTION ASSESSMENTS IN THE COLLECTION AND USE OF PERSONAL DATA; AND

(C) EMPOWERS THE ATTORNEY GENERAL AND DISTRICT ATTORNEYS TO ACCESS AND EVALUATE A COMPANY'S DATA PROTECTION ASSESSMENTS, TO IMPOSE PENALTIES WHERE VIOLATIONS OCCUR, AND TO PREVENT FUTURE VIOLATIONS.

6-1-1303. Definitions. AS USED IN THIS PART 13, UNLESS THE CONTEXT OTHERWISE REQUIRES:

(1) "AFFILIATE" MEANS A LEGAL ENTITY THAT CONTROLS, IS CONTROLLED BY, OR IS UNDER COMMON CONTROL WITH ANOTHER LEGAL ENTITY. AS USED IN THIS SUBSECTION (1), "CONTROL" MEANS:

(a) OWNERSHIP OF, CONTROL OF, OR POWER TO VOTE TWENTY-FIVE PERCENT OR MORE OF THE OUTSTANDING SHARES OF ANY CLASS OF VOTING SECURITY OF THE ENTITY, DIRECTLY OR INDIRECTLY, OR ACTING THROUGH ONE OR MORE OTHER PERSONS;

(b) CONTROL IN ANY MANNER OVER THE ELECTION OF A MAJORITY OF THE DIRECTORS, TRUSTEES, OR GENERAL PARTNERS OF THE ENTITY OR OF INDIVIDUALS EXERCISING SIMILAR FUNCTIONS; OR

(c) THE POWER TO EXERCISE, DIRECTLY OR INDIRECTLY, A CONTROLLING INFLUENCE OVER THE MANAGEMENT OR POLICIES OF THE ENTITY AS DETERMINED BY THE APPLICABLE PRUDENTIAL REGULATOR, AS THAT TERM IS DEFINED IN 12 U.S.C. SEC. 5481 (24), IF ANY.

(2) "AUTHENTICATE" MEANS TO USE REASONABLE MEANS TO DETERMINE THAT A REQUEST TO EXERCISE ANY OF THE RIGHTS IN SECTION 6-1-1306 (1) IS BEING MADE BY OR ON BEHALF OF THE CONSUMER WHO IS ENTITLED TO EXERCISE THE RIGHTS.

(3) "BUSINESS ASSOCIATE" HAS THE MEANING ESTABLISHED IN 45 CFR 160.103.

(4) "CHILD" MEANS AN INDIVIDUAL UNDER THIRTEEN YEARS OF AGE.

(5) "CONSENT" MEANS A CLEAR, AFFIRMATIVE ACT SIGNIFYING A CONSUMER'S FREELY GIVEN, SPECIFIC, INFORMED, AND UNAMBIGUOUS AGREEMENT, SUCH AS BY A WRITTEN STATEMENT, INCLUDING BY ELECTRONIC MEANS, OR OTHER CLEAR, AFFIRMATIVE ACTION BY WHICH THE CONSUMER SIGNIFIES AGREEMENT TO THE PROCESSING OF PERSONAL DATA. THE FOLLOWING DOES NOT CONSTITUTE CONSENT:

(a) ACCEPTANCE OF A GENERAL OR BROAD TERMS OF USE OR SIMILAR DOCUMENT THAT CONTAINS DESCRIPTIONS OF PERSONAL DATA PROCESSING ALONG WITH OTHER, UNRELATED INFORMATION;

(b) HOVERING OVER, MUTING, PAUSING, OR CLOSING A GIVEN PIECE OF CONTENT; AND

(c) AGREEMENT OBTAINED THROUGH DARK PATTERNS.

(6) "CONSUMER":

(a) MEANS AN INDIVIDUAL WHO IS A COLORADO RESIDENT ACTING ONLY IN AN INDIVIDUAL OR HOUSEHOLD CONTEXT; AND

(b) DOES NOT INCLUDE AN INDIVIDUAL ACTING IN A COMMERCIAL OR EMPLOYMENT CONTEXT, AS A JOB APPLICANT, OR AS A BENEFICIARY OF SOMEONE ACTING IN AN EMPLOYMENT CONTEXT.

(7) "CONTROLLER" MEANS A PERSON THAT, ALONE OR JOINTLY WITH OTHERS, DETERMINES THE PURPOSES FOR AND MEANS OF PROCESSING PERSONAL DATA.

(8) "COVERED ENTITY" HAS THE MEANING ESTABLISHED IN 45 CFR 160.103.

(9) "DARK PATTERN" MEANS A USER INTERFACE DESIGNED OR MANIPULATED WITH THE SUBSTANTIAL EFFECT OF SUBVERTING OR IMPAIRING USER AUTONOMY, DECISION-MAKING, OR CHOICE.

(10) "DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS CONCERNING A CONSUMER" MEANS A DECISION THAT RESULTS IN THE PROVISION OR DENIAL OF FINANCIAL OR LENDING SERVICES, HOUSING, INSURANCE, EDUCATION ENROLLMENT OR OPPORTUNITY, CRIMINAL JUSTICE, EMPLOYMENT OPPORTUNITIES, HEALTH-CARE SERVICES, OR ACCESS TO ESSENTIAL GOODS OR SERVICES.

(11) "DE-IDENTIFIED DATA" MEANS DATA THAT CANNOT REASONABLY BE USED TO INFER INFORMATION ABOUT, OR OTHERWISE BE LINKED TO, AN IDENTIFIED OR IDENTIFIABLE INDIVIDUAL, OR A DEVICE LINKED TO SUCH AN INDIVIDUAL, IF THE CONTROLLER THAT POSSESSES THE DATA:

(a) TAKES REASONABLE MEASURES TO ENSURE THAT THE DATA CANNOT BE ASSOCIATED WITH AN INDIVIDUAL;

(b) PUBLICLY COMMITS TO MAINTAIN AND USE THE DATA ONLY IN A DE-IDENTIFIED FASHION AND NOT ATTEMPT TO RE-IDENTIFY THE DATA; AND

(c) CONTRACTUALLY OBLIGATES ANY RECIPIENTS OF THE INFORMATION TO COMPLY WITH THE REQUIREMENTS OF THIS SUBSECTION (11).

(12) "HEALTH-CARE FACILITY" MEANS ANY ENTITY THAT IS LICENSED, CERTIFIED, OR OTHERWISE AUTHORIZED OR PERMITTED BY LAW TO ADMINISTER MEDICAL TREATMENT IN THIS STATE.

(13) "HEALTH-CARE INFORMATION" MEANS INDIVIDUALLY IDENTIFIABLE INFORMATION RELATING TO THE PAST, PRESENT, OR FUTURE HEALTH STATUS OF AN INDIVIDUAL.

(14) "HEALTH-CARE PROVIDER" MEANS A PERSON LICENSED, CERTIFIED, OR REGISTERED IN THIS STATE TO PRACTICE MEDICINE, PHARMACY, CHIROPRACTIC, NURSING, PHYSICAL THERAPY, PODIATRY, DENTISTRY, OPTOMETRY, OCCUPATIONAL THERAPY, OR OTHER HEALING ARTS UNDER TITLE 12.

(15) "HIPAA" MEANS THE FEDERAL "HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996", AS AMENDED, 42 U.S.C. SECS. 1320d TO 1320d-9.

(16) "IDENTIFIED OR IDENTIFIABLE INDIVIDUAL" MEANS AN INDIVIDUAL WHO CAN BE READILY IDENTIFIED, DIRECTLY OR INDIRECTLY, IN PARTICULAR BY REFERENCE TO AN IDENTIFIER SUCH AS A NAME, AN IDENTIFICATION NUMBER, SPECIFIC GEOLOCATION DATA, OR AN ONLINE IDENTIFIER.

(17) "PERSONAL DATA":

(a) MEANS INFORMATION THAT IS LINKED OR REASONABLY LINKABLE TO AN IDENTIFIED OR IDENTIFIABLE INDIVIDUAL; AND

(b) DOES NOT INCLUDE DE-IDENTIFIED DATA OR PUBLICLY AVAILABLE INFORMATION. AS USED IN THIS SUBSECTION (17)(b), "PUBLICLY AVAILABLE INFORMATION" MEANS INFORMATION THAT IS LAWFULLY MADE AVAILABLE FROM FEDERAL, STATE, OR LOCAL GOVERNMENT RECORDS AND INFORMATION THAT A CONTROLLER HAS A REASONABLE BASIS TO BELIEVE THE CONSUMER HAS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC.

(18) "PROCESS" OR "PROCESSING" MEANS THE COLLECTION, USE, SALE, STORAGE, DISCLOSURE, ANALYSIS, DELETION, OR MODIFICATION OF PERSONAL DATA AND INCLUDES THE ACTIONS OF A CONTROLLER DIRECTING A PROCESSOR TO PROCESS PERSONAL DATA.

(19) "PROCESSOR" MEANS A PERSON THAT PROCESSES PERSONAL DATA ON BEHALF OF A CONTROLLER.

(20) "PROFILING" MEANS ANY FORM OF AUTOMATED PROCESSING OF PERSONAL DATA TO EVALUATE, ANALYZE, OR PREDICT PERSONAL ASPECTS CONCERNING AN IDENTIFIED OR IDENTIFIABLE INDIVIDUAL'S ECONOMIC SITUATION, HEALTH, PERSONAL PREFERENCES, INTERESTS, RELIABILITY, BEHAVIOR, LOCATION, OR MOVEMENTS.

(21) "PROTECTED HEALTH INFORMATION" HAS THE MEANING ESTABLISHED IN 45 CFR 160.103.

(22) "PSEUDONYMOUS DATA" MEANS PERSONAL DATA THAT CAN NO LONGER BE ATTRIBUTED TO A SPECIFIC INDIVIDUAL WITHOUT THE USE OF ADDITIONAL INFORMATION IF THE ADDITIONAL INFORMATION IS KEPT SEPARATELY AND IS SUBJECT TO TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THAT THE PERSONAL DATA ARE NOT ATTRIBUTED TO A SPECIFIC INDIVIDUAL.

(23) (a) "SALE", "SELL", OR "SOLD" MEANS THE EXCHANGE OF PERSONAL DATA FOR MONETARY OR OTHER VALUABLE CONSIDERATION BY A CONTROLLER TO A THIRD PARTY.

(b) "SALE", "SELL", OR "SOLD" DOES NOT INCLUDE THE FOLLOWING:

(I) THE DISCLOSURE OF PERSONAL DATA TO A PROCESSOR THAT PROCESSES THE PERSONAL DATA ON BEHALF OF A CONTROLLER;

(II) THE DISCLOSURE OF PERSONAL DATA TO A THIRD PARTY FOR PURPOSES OF PROVIDING A PRODUCT OR SERVICE REQUESTED BY THE CONSUMER;

(III) THE DISCLOSURE OR TRANSFER OF PERSONAL DATA TO AN AFFILIATE OF THE CONTROLLER;

(IV) THE DISCLOSURE OR TRANSFER TO A THIRD PARTY OF PERSONAL DATA AS AN ASSET THAT IS PART OF A PROPOSED OR ACTUAL MERGER, ACQUISITION, BANKRUPTCY, OR OTHER TRANSACTION IN WHICH THE THIRD PARTY ASSUMES CONTROL OF ALL OR PART OF THE CONTROLLER'S ASSETS; OR

(V) THE DISCLOSURE OF PERSONAL DATA:

(A) THAT A CONSUMER DIRECTS THE CONTROLLER TO DISCLOSE OR INTENTIONALLY DISCLOSES BY USING THE CONTROLLER TO INTERACT WITH A THIRD PARTY; OR

(B) INTENTIONALLY MADE AVAILABLE BY A CONSUMER TO THE GENERAL PUBLIC VIA A CHANNEL OF MASS MEDIA.

(24) "SENSITIVE DATA" MEANS:

(a) PERSONAL DATA REVEALING RACIAL OR ETHNIC ORIGIN, RELIGIOUS BELIEFS, A MENTAL OR PHYSICAL HEALTH CONDITION OR DIAGNOSIS, SEX LIFE OR SEXUAL ORIENTATION, OR CITIZENSHIP OR CITIZENSHIP STATUS;

(b) GENETIC OR BIOMETRIC DATA THAT MAY BE PROCESSED FOR THE PURPOSE OF UNIQUELY IDENTIFYING AN INDIVIDUAL; OR

(c) PERSONAL DATA FROM A KNOWN CHILD.

(25) "TARGETED ADVERTISING":

(a) MEANS DISPLAYING TO A CONSUMER AN ADVERTISEMENT THAT IS SELECTED BASED ON PERSONAL DATA OBTAINED OR INFERRED OVER TIME FROM THE CONSUMER'S ACTIVITIES ACROSS NONAFFILIATED WEBSITES, APPLICATIONS, OR ONLINE SERVICES TO PREDICT CONSUMER PREFERENCES OR INTERESTS; AND

(b) DOES NOT INCLUDE:

(I) ADVERTISING TO A CONSUMER IN RESPONSE TO THE CONSUMER'S REQUEST FOR INFORMATION OR FEEDBACK;

(II) ADVERTISEMENTS BASED ON ACTIVITIES WITHIN A CONTROLLER'S OWN WEBSITES OR ONLINE APPLICATIONS;

(III) ADVERTISEMENTS BASED ON THE CONTEXT OF A CONSUMER'S CURRENT SEARCH QUERY, VISIT TO A WEBSITE, OR ONLINE APPLICATION; OR

(IV) PROCESSING PERSONAL DATA SOLELY FOR MEASURING OR REPORTING ADVERTISING PERFORMANCE, REACH, OR FREQUENCY.

(26) "THIRD PARTY" MEANS A PERSON, PUBLIC AUTHORITY, AGENCY, OR BODY OTHER THAN A CONSUMER, CONTROLLER, PROCESSOR, OR AFFILIATE OF THE PROCESSOR OR THE CONTROLLER.

6-1-1304. Applicability of part. (1) EXCEPT AS SPECIFIED IN SUBSECTION (2) OF THIS SECTION, THIS PART 13 APPLIES TO A CONTROLLER THAT:

(a) CONDUCTS BUSINESS IN COLORADO OR PRODUCES OR DELIVERS COMMERCIAL PRODUCTS OR SERVICES THAT ARE INTENTIONALLY TARGETED TO RESIDENTS OF COLORADO; AND

(b) SATISFIES ONE OR BOTH OF THE FOLLOWING THRESHOLDS:

(I) CONTROLS OR PROCESSES THE PERSONAL DATA OF ONE HUNDRED THOUSAND CONSUMERS OR MORE DURING A CALENDAR YEAR; OR

(II) DERIVES REVENUE OR RECEIVES A DISCOUNT ON THE PRICE OF GOODS OR SERVICES FROM THE SALE OF PERSONAL DATA AND PROCESSES OR CONTROLS THE PERSONAL DATA OF TWENTY-FIVE THOUSAND CONSUMERS OR MORE.

(2) THIS PART 13 DOES NOT APPLY TO:

(a) PROTECTED HEALTH INFORMATION THAT IS COLLECTED, STORED, AND PROCESSED BY A COVERED ENTITY OR ITS BUSINESS ASSOCIATES;

(b) HEALTH-CARE INFORMATION THAT IS GOVERNED BY PART 8 OF ARTICLE 1 OF TITLE 25 SOLELY FOR THE PURPOSE OF ACCESS TO MEDICAL RECORDS;

(c) PATIENT IDENTIFYING INFORMATION, AS DEFINED IN 42 CFR 2.11, THAT ARE GOVERNED BY AND COLLECTED AND PROCESSED PURSUANT TO 42 CFR 2, ESTABLISHED PURSUANT TO 42 U.S.C. SEC. 290dd-2;

(d) IDENTIFIABLE PRIVATE INFORMATION, AS DEFINED IN 45 CFR 46.102, FOR PURPOSES OF THE FEDERAL POLICY FOR THE PROTECTION OF HUMAN SUBJECTS PURSUANT TO 45 CFR 46; IDENTIFIABLE PRIVATE INFORMATION THAT IS COLLECTED AS PART OF HUMAN SUBJECTS RESEARCH PURSUANT TO THE ICH E6 GOOD CLINICAL PRACTICE GUIDELINE ISSUED BY THE INTERNATIONAL COUNCIL FOR HARMONISATION OF TECHNICAL REQUIREMENTS FOR PHARMACEUTICALS FOR HUMAN USE OR THE PROTECTION OF HUMAN SUBJECTS UNDER 21 CFR 50 AND 56; OR PERSONAL DATA USED OR SHARED IN RESEARCH CONDUCTED IN ACCORDANCE WITH ONE OR MORE OF THE CATEGORIES SET FORTH IN THIS SUBSECTION (2)(d);

(e) INFORMATION AND DOCUMENTS CREATED BY A COVERED ENTITY FOR PURPOSES OF COMPLYING WITH HIPAA AND ITS IMPLEMENTING REGULATIONS;

(f) PATIENT SAFETY WORK PRODUCT, AS DEFINED IN 42 CFR 3.20, THAT IS CREATED FOR PURPOSES OF PATIENT SAFETY IMPROVEMENT PURSUANT TO 42 CFR 3, ESTABLISHED PURSUANT TO 42 U.S.C. SECS. 299b-21 TO 299b-26;

(g) INFORMATION THAT IS: (I) DE-IDENTIFIED IN ACCORDANCE WITH THE REQUIREMENTS FOR DE-IDENTIFICATION SET FORTH IN 45 CFR 164; AND

(II) DERIVED FROM ANY OF THE HEALTH-CARE-RELATED INFORMATION DESCRIBED IN THIS SECTION.

(h) INFORMATION MAINTAINED IN THE SAME MANNER AS INFORMATION UNDER SUBSECTIONS (2)(a) TO (2)(g) OF THIS SECTION BY:

(I) A COVERED ENTITY OR BUSINESS ASSOCIATE;

(II) A HEALTH-CARE FACILITY OR HEALTH-CARE PROVIDER; OR

(III) A PROGRAM OF A QUALIFIED SERVICE ORGANIZATION AS DEFINED IN 42 CFR 2.11;

(i) (I) EXCEPT AS PROVIDED IN SUBSECTION (2)(i)(II) OF THIS SECTION, AN ACTIVITY INVOLVING THE COLLECTION, MAINTENANCE, DISCLOSURE, SALE, COMMUNICATION, OR USE OF ANY PERSONAL DATA BEARING ON A CONSUMER'S CREDITWORTHINESS, CREDIT STANDING, CREDIT CAPACITY, CHARACTER, GENERAL REPUTATION, PERSONAL CHARACTERISTICS, OR MODE OF LIVING BY:

(A) A CONSUMER REPORTING AGENCY AS DEFINED IN 15 U.S.C. SEC. 1681a (f);

(B) A FURNISHER OF INFORMATION AS SET FORTH IN 15 U.S.C. SEC. 1681s-2 THAT PROVIDES INFORMATION FOR USE IN A CONSUMER REPORT, AS DEFINED IN 15 U.S.C. SEC. 1681a (d); OR

(C) A USER OF A CONSUMER REPORT AS SET FORTH IN 15 U.S.C. SEC. 1681b.

(II) THIS SUBSECTION (2)(i) APPLIES ONLY TO THE EXTENT THAT THE ACTIVITY IS REGULATED BY THE FEDERAL "FAIR CREDIT REPORTING ACT", 15 U.S.C. SEC. 1681 ET SEQ., AS AMENDED, AND THE PERSONAL DATA ARE NOT COLLECTED, MAINTAINED, DISCLOSED, SOLD, COMMUNICATED, OR USED EXCEPT AS AUTHORIZED BY THE FEDERAL "FAIR CREDIT REPORTING ACT", AS AMENDED.

(j) PERSONAL DATA:

(I) COLLECTED AND MAINTAINED FOR PURPOSES OF ARTICLE 22 OF TITLE 10;

(II) COLLECTED, PROCESSED, SOLD, OR DISCLOSED PURSUANT TO THE FEDERAL "GRAMM-LEACH-BLILEY ACT", 15 U.S.C. SEC. 6801 ET SEQ., AS AMENDED, AND IMPLEMENTING REGULATIONS, IF THE COLLECTION, PROCESSING, SALE, OR DISCLOSURE IS IN COMPLIANCE WITH THAT LAW;

(III) COLLECTED, PROCESSED, SOLD, OR DISCLOSED PURSUANT TO THE FEDERAL "DRIVER'S PRIVACY PROTECTION ACT OF 1994", 18 U.S.C. SEC. 2721 ET SEQ., AS AMENDED, IF THE COLLECTION, PROCESSING, SALE, OR DISCLOSURE IS REGULATED BY THAT LAW, INCLUDING IMPLEMENTING RULES, REGULATIONS, OR EXEMPTIONS;

(IV) REGULATED BY THE FEDERAL "CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998", 15 U.S.C. SECS. 6501TO 6506, AS AMENDED, IF COLLECTED, PROCESSED, AND MAINTAINED IN COMPLIANCE WITH THAT LAW; OR

(V) REGULATED BY THE FEDERAL "FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT OF 1974", 20 U.S.C. SEC. 1232g ET SEQ., AS AMENDED, AND ITS IMPLEMENTING REGULATIONS;

(k) DATA MAINTAINED FOR EMPLOYMENT RECORDS PURPOSES;

(l) AN AIR CARRIER AS DEFINED IN AND REGULATED UNDER 49 U.S.C. SEC. 40101 ET SEQ., AS AMENDED, AND 49 U.S.C. SEC. 41713, AS AMENDED;

(m) A NATIONAL SECURITIES ASSOCIATION REGISTERED PURSUANT TO THE FEDERAL "SECURITIES EXCHANGE ACT OF 1934", 15 U.S.C. SEC. 78o-3, AS AMENDED, OR IMPLEMENTING REGULATIONS;

(n) CUSTOMER DATA MAINTAINED BY A PUBLIC UTILITY AS DEFINED IN SECTION 40-1-103 (1)(a)(I) OR AN AUTHORITY AS DEFINED IN SECTION 43-4-503 (1), IF THE DATA ARE NOT COLLECTED, MAINTAINED, DISCLOSED, SOLD, COMMUNICATED, OR USED EXCEPT AS AUTHORIZED BY STATE AND FEDERAL LAW;

(o) DATA MAINTAINED BY A STATE INSTITUTION OF HIGHER EDUCATION, AS DEFINED IN SECTION 23-18-102 (10), THE STATE, THE JUDICIAL DEPARTMENT OF THE STATE, OR A COUNTY, CITY AND COUNTY, OR MUNICIPALITY IF THE DATA IS COLLECTED, MAINTAINED, DISCLOSED, COMMUNICATED, AND USED AS AUTHORIZED BY STATE AND FEDERAL LAW FOR NONCOMMERCIAL PURPOSES. THIS SUBSECTION (2)(o) DOES NOT EFFECT ANY OTHER EXEMPTION AVAILABLE UNDER THIS PART 13.

(p) INFORMATION USED AND DISCLOSED IN COMPLIANCE WITH 45 CFR 164.512; OR

(q) A FINANCIAL INSTITUTION OR AN AFFILIATE OF A FINANCIAL INSTITUTION AS DEFINED BY AND THAT IS SUBJECT TO THE FEDERAL "GRAMM-LEACH-BLILEY ACT", 15 U.S.C. SEC. 6801 ET SEQ., AS AMENDED, AND IMPLEMENTING REGULATIONS, INCLUDING REGULATION P, 12 CFR 1016.

(3) THE OBLIGATIONS IMPOSED ON CONTROLLERS OR PROCESSORS UNDER THIS PART 13 DO NOT:

(a) RESTRICT A CONTROLLER'S OR PROCESSOR'S ABILITY TO:

(I) COMPLY WITH FEDERAL, STATE, OR LOCAL LAWS, RULES, OR REGULATIONS;

(II) COMPLY WITH A CIVIL, CRIMINAL, OR REGULATORY INQUIRY, INVESTIGATION, SUBPOENA, OR SUMMONS BY FEDERAL, STATE, LOCAL, OR OTHER GOVERNMENTAL AUTHORITIES;

(III) COOPERATE WITH LAW ENFORCEMENT AGENCIES CONCERNING CONDUCT OR ACTIVITY THAT THE CONTROLLER OR PROCESSOR REASONABLY AND IN GOOD FAITH BELIEVES MAY VIOLATE FEDERAL, STATE, OR LOCAL LAW;

(IV) INVESTIGATE, EXERCISE, PREPARE FOR, OR DEFEND ACTUAL OR ANTICIPATED LEGAL CLAIMS;

(V) CONDUCT INTERNAL RESEARCH TO IMPROVE, REPAIR, OR DEVELOP PRODUCTS, SERVICES, OR TECHNOLOGY;

(VI) IDENTIFY AND REPAIR TECHNICAL ERRORS THAT IMPAIR EXISTING OR INTENDED FUNCTIONALITY;

(VII) PERFORM INTERNAL OPERATIONS THAT ARE REASONABLY ALIGNED WITH THE EXPECTATIONS OF THE CONSUMER BASED ON THE CONSUMER'S EXISTING RELATIONSHIP WITH THE CONTROLLER;

(VIII) PROVIDE A PRODUCT OR SERVICE SPECIFICALLY REQUESTED BY A CONSUMER OR THE PARENT OR GUARDIAN OF A CHILD, PERFORM A CONTRACT TO WHICH THE CONSUMER IS A PARTY, OR TAKE STEPS AT THE REQUEST OF THE CONSUMER PRIOR TO ENTERING INTO A CONTRACT;

(IX) PROTECT THE VITAL INTERESTS OF THE CONSUMER OR OF ANOTHER INDIVIDUAL;

(X) PREVENT, DETECT, PROTECT AGAINST, OR RESPOND TO SECURITY INCIDENTS, IDENTITY THEFT, FRAUD, HARASSMENT, OR MALICIOUS, DECEPTIVE, OR ILLEGAL ACTIVITY; PRESERVE THE INTEGRITY OR SECURITY OF SYSTEMS; OR INVESTIGATE, REPORT, OR PROSECUTE THOSE RESPONSIBLE FOR ANY SUCH ACTION;

(XI) PROCESS PERSONAL DATA FOR REASONS OF PUBLIC INTEREST IN THE AREA OF PUBLIC HEALTH, BUT SOLELY TO THE EXTENT THAT THE PROCESSING:

(A) IS SUBJECT TO SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE RIGHTS OF THE CONSUMER WHOSE PERSONAL DATA ARE PROCESSED; AND

(B) IS UNDER THE RESPONSIBILITY OF A PROFESSIONAL SUBJECT TO CONFIDENTIALITY OBLIGATIONS UNDER FEDERAL, STATE, OR LOCAL LAW; OR

(XII) ASSIST ANOTHER PERSON WITH ANY OF THE ACTIVITIES SET FORTH IN THIS SUBSECTION (3);

(b) APPLY WHERE COMPLIANCE BY THE CONTROLLER OR PROCESSOR WITH THIS PART 13 WOULD VIOLATE AN EVIDENTIARY PRIVILEGE UNDER COLORADO LAW;

(c) PREVENT A CONTROLLER OR PROCESSOR FROM PROVIDING PERSONAL DATA CONCERNING A CONSUMER TO A PERSON COVERED BY AN EVIDENTIARY PRIVILEGE UNDER COLORADO LAW AS PART OF A PRIVILEGED COMMUNICATION;

(d) APPLY TO INFORMATION MADE AVAILABLE BY A THIRD PARTY THAT THE CONTROLLER HAS A REASONABLE BASIS TO BELIEVE IS PROTECTED SPEECH PURSUANT TO APPLICABLE LAW; AND

(e) APPLY TO THE PROCESSING OF PERSONAL DATA BY AN INDIVIDUAL IN THE COURSE OF A PURELY PERSONAL OR HOUSEHOLD ACTIVITY.

(4) PERSONAL DATA THAT ARE PROCESSED BY A CONTROLLER PURSUANT TO AN EXCEPTION PROVIDED BY THIS SECTION:

(a) SHALL NOT BE PROCESSED FOR ANY PURPOSE OTHER THAN A PURPOSE EXPRESSLY LISTED IN THIS SECTION OR AS OTHERWISE AUTHORIZED BY THIS PART 13; AND

(b) SHALL BE PROCESSED SOLELY TO THE EXTENT THAT THE PROCESSING IS NECESSARY, REASONABLE, AND PROPORTIONATE TO THE SPECIFIC PURPOSE OR PURPOSES LISTED IN THIS SECTION OR AS OTHERWISE AUTHORIZED BY THIS PART 13.

(5) IF A CONTROLLER PROCESSES PERSONAL DATA PURSUANT TO AN EXEMPTION IN THIS SECTION, THE CONTROLLER BEARS THE BURDEN OF DEMONSTRATING THAT THE PROCESSING QUALIFIES FOR THE EXEMPTION AND COMPLIES WITH THE REQUIREMENTS IN SUBSECTION (4) OF THIS SECTION.

6-1-1305. Responsibility according to role. (1) CONTROLLERS AND PROCESSORS SHALL MEET THEIR RESPECTIVE OBLIGATIONS ESTABLISHED UNDER THIS PART 13.

(2) PROCESSORS SHALL ADHERE TO THE INSTRUCTIONS OF THE CONTROLLER AND ASSIST THE CONTROLLER TO MEET ITS OBLIGATIONS UNDER THIS PART 13. TAKING INTO ACCOUNT THE NATURE OF PROCESSING AND THE INFORMATION AVAILABLE TO THE PROCESSOR, THE PROCESSOR SHALL ASSIST THE CONTROLLER BY:

(a) TAKING APPROPRIATE TECHNICAL AND ORGANIZATIONAL MEASURES, INSOFAR AS THIS IS POSSIBLE, FOR THE FULFILLMENT OF THE CONTROLLER'S OBLIGATION TO RESPOND TO CONSUMER REQUESTS TO EXERCISE THEIR RIGHTS PURSUANT TO SECTION 6-1-1306;

(b) HELPING TO MEET THE CONTROLLER'S OBLIGATIONS IN RELATION TO THE SECURITY OF PROCESSING THE PERSONAL DATA AND IN RELATION TO THE NOTIFICATION OF A BREACH OF THE SECURITY OF THE SYSTEM PURSUANT TO SECTION 6-1-716; AND

(c) PROVIDING INFORMATION TO THE CONTROLLER NECESSARY TO ENABLE THE CONTROLLER TO CONDUCT AND DOCUMENT ANY DATA PROTECTION ASSESSMENTS REQUIRED BY SECTION 6-1-1309. THE CONTROLLER AND PROCESSOR ARE EACH RESPONSIBLE FOR ONLY THE MEASURES ALLOCATED TO THEM.

(3) NOTWITHSTANDING THE INSTRUCTIONS OF THE CONTROLLER, A PROCESSOR SHALL:

(a) ENSURE THAT EACH PERSON PROCESSING THE PERSONAL DATA IS SUBJECT TO A DUTY OF CONFIDENTIALITY WITH RESPECT TO THE DATA; AND

(b) ENGAGE A SUBCONTRACTOR ONLY AFTER PROVIDING THE CONTROLLER WITH AN OPPORTUNITY TO OBJECT AND PURSUANT TO A WRITTEN CONTRACT IN ACCORDANCE WITH SUBSECTION (5) OF THIS SECTION THAT REQUIRES THE SUBCONTRACTOR TO MEET THE OBLIGATIONS OF THE PROCESSOR WITH RESPECT TO THE PERSONAL DATA.

(4) TAKING INTO ACCOUNT THE CONTEXT OF PROCESSING, THE CONTROLLER AND THE PROCESSOR SHALL IMPLEMENT APPROPRIATE TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE A LEVEL OF SECURITY APPROPRIATE TO THE RISK AND ESTABLISH A CLEAR ALLOCATION OF THE RESPONSIBILITIES BETWEEN THEM TO IMPLEMENT THE MEASURES.

(5) PROCESSING BY A PROCESSOR MUST BE GOVERNED BY A CONTRACT BETWEEN THE CONTROLLER AND THE PROCESSOR THAT IS BINDING ON BOTH PARTIES AND THAT SETS OUT:

(a) THE PROCESSING INSTRUCTIONS TO WHICH THE PROCESSOR IS BOUND, INCLUDING THE NATURE AND PURPOSE OF THE PROCESSING;

(b) THE TYPE OF PERSONAL DATA SUBJECT TO THE PROCESSING, AND THE DURATION OF THE PROCESSING;

(c) THE REQUIREMENTS IMPOSED BY THIS SUBSECTION (5) AND SUBSECTIONS (3) AND (4) OF THIS SECTION; AND

(d) THE FOLLOWING REQUIREMENTS:

(I) AT THE CHOICE OF THE CONTROLLER, THE PROCESSOR SHALL DELETE OR RETURN ALL PERSONAL DATA TO THE CONTROLLER AS REQUESTED AT THE END OF THE PROVISION OF SERVICES, UNLESS RETENTION OF THE PERSONAL DATA IS REQUIRED BY LAW;

(II) (A) THE PROCESSOR SHALL MAKE AVAILABLE TO THE CONTROLLER ALL INFORMATION NECESSARY TO DEMONSTRATE COMPLIANCE WITH THE OBLIGATIONS IN THIS PART 13; AND

(B) THE PROCESSOR SHALL ALLOW FOR, AND CONTRIBUTE TO, REASONABLE AUDITS AND INSPECTIONS BY THE CONTROLLER OR THE CONTROLLER'S DESIGNATED AUDITOR. ALTERNATIVELY, THE PROCESSOR MAY, WITH THE CONTROLLER'S CONSENT, ARRANGE FOR A QUALIFIED AND INDEPENDENT AUDITOR TO CONDUCT, AT LEAST ANNUALLY AND AT THE PROCESSOR'S EXPENSE, AN AUDIT OF THE PROCESSOR'S POLICIES AND TECHNICAL AND ORGANIZATIONAL MEASURES Ii\I SUPPORT OF THE OBLIGATIONS UNDER THIS PART 13 USING AN APPROPRIATE AND ACCEPTED CONTROL STANDARD OR FRAMEWORK AND AUDIT PROCEDURE FOR THE AUDITS AS APPLICABLE. THE PROCESSOR SHALL PROVIDE A REPORT OF THE AUDIT TO THE CONTROLLER UPON REQUEST.

(6) IN NO EVENT MAY A CONTRACT RELIEVE A CONTROLLER OR A PROCESSOR FROM THE LIABILITIES IMPOSED ON THEM BY VIRTUE OF ITS ROLE IN THE PROCESSING RELATIONSHIP AS DEFINED BY THIS PART 13.

(7) DETERMINING WHETHER A PERSON IS ACTING AS A CONTROLLER OR PROCESSOR WITH RESPECT TO A SPECIFIC PROCESSING OF DATA IS A FACT-BASED DETERMINATION THAT DEPENDS UPON THE CONTEXT IN WHICH PERSONAL DATA ARE TO BE PROCESSED. A PERSON THAT IS NOT LIMITED IN ITS PROCESSING OF PERSONAL DATA PURSUANT TO A CONTROLLER'S INSTRUCTIONS, OR THAT FAILS TO ADHERE TO THE INSTRUCTIONS, IS A CONTROLLER AND NOT A PROCESSOR WITH RESPECT TO A SPECIFIC PROCESSING OF DATA. A PROCESSOR THAT CONTINUES TO ADHERE TO A CONTROLLER'S INSTRUCTIONS WITH RESPECT TO A SPECIFIC PROCESSING OF PERSONAL DATA REMAINS A PROCESSOR. IF A PROCESSOR BEGINS, ALONE OR JOINTLY WITH OTHERS, DETERMINING THE PURPOSES AND MEANS OF THE PROCESSING OF PERSONAL DATA, IT IS A CONTROLLER WITH RESPECT TO THE PROCESSING.

(8) (a) A CONTROLLER OR PROCESSOR THAT DISCLOSES PERSONAL DATA TO ANOTHER CONTROLLER OR PROCESSOR IN COMPLIANCE WITH THIS PART 13 DOES NOT VIOLATE THIS PART 13 IF THE RECIPIENT PROCESSES THE PERSONAL DATA IN VIOLATION OF THIS PART 13, AND, AT THE TIME OF DISCLOSING THE PERSONAL DATA, THE DISCLOSING CONTROLLER OR PROCESSOR DID NOT HAVE ACTUAL KNOWLEDGE THAT THE RECIPIENT INTENDED TO COMMIT A VIOLATION.

(b) A CONTROLLER OR PROCESSOR RECEIVING PERSONAL DATA FROM A CONTROLLER OR PROCESSOR IN COMPLIANCE WITH THIS PART 13 AS SPECIFIED IN SUBSECTION (8)(a) OF THIS SECTION DOES NOT VIOLATE THIS PART 13 IF THE CONTROLLER OR PROCESSOR FROM WHICH IT RECEIVES THE PERSONAL DATA FAILS TO COMPLY WITH APPLICABLE OBLIGATIONS UNDER THIS PART 13.

6-1-1306. Consumer personal data rights - repeal. (1) CONSUMERS MAY EXERCISE THE FOLLOWING RIGHTS BY SUBMITTING A REQUEST USING THE METHODS SPECIFIED BY THE CONTROLLER IN THE PRIVACY NOTICE REQUIRED UNDER SECTION 6-1-1308 (1)(a). THE METHOD MUST TAKE INTO ACCOUNT THE WAYS IN WHICH CONSUMERS NORMALLY INTERACT WITH THE CONTROLLER, THE NEED FOR SECURE AND RELIABLE COMMUNICATION RELATING TO THE REQUEST, AND THE ABILITY OF THE CONTROLLER TO AUTHENTICATE THE IDENTITY OF THE CONSUMER MAKING THE REQUEST. CONTROLLERS SHALL NOT REQUIRE A CONSUMER TO CREATE A NEW ACCOUNT IN ORDER TO EXERCISE CONSUMER RIGHTS PURSUANT TO THIS SECTION BUT MAY REQUIRE A CONSUMER TO USE AN EXISTING ACCOUNT. A CONSUMER MAY SUBMIT A REQUEST AT ANY TIME TO A CONTROLLER SPECIFYING WHICH OF THE FOLLOWING RIGHTS THE CONSUMER WISHES TO EXERCISE:

(a) **Right to opt out.** (I) A CONSUMER HAS THE RIGHT TO OPT OUT OF THE PROCESSING OF PERSONAL DATA CONCERNING THE CONSUMER FOR PURPOSES OF:

(A) TARGETED ADVERTISING;

(B) THE SALE OF PERSONAL DATA; OR

(C) PROFILING IN FURTHERANCE OF DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS CONCERNING A CONSUMER.

(II) A CONSUMER MAY AUTHORIZE ANOTHER PERSON, ACTING ON THE CONSUMER'S BEHALF, TO OPT OUT OF THE PROCESSING OF THE CONSUMER'S PERSONAL DATA FOR ONE OR MORE OF THE PURPOSES SPECIFIED IN SUBSECTION (1)(a)(I) OF THIS SECTION, INCLUDING THROUGH A TECHNOLOGY INDICATING THE CONSUMER'S INTENT TO OPT OUT SUCH AS A WEB LINK INDICATING A PREFERENCE OR BROWSER SETTING, BROWSER EXTENSION, OR GLOBAL DEVICE SETTING. A CONTROLLER SHALL COMPLY WITH AN OPT-OUT REQUEST RECEIVED FROM A PERSON AUTHORIZED BY THE CONSUMER TO ACT ON THE CONSUMER'S BEHALF IF THE CONTROLLER IS ABLE TO AUTHENTICATE, WITH COMMERCIALLY REASONABLE EFFORT, THE IDENTITY OF THE CONSUMER AND THE AUTHORIZED AGENT'S AUTHORITY TO ACT ON THE CONSUMER'S BEHALF.

(III) A CONTROLLER THAT PROCESSES PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA SHALL PROVIDE A CLEAR AND CONSPICUOUS

METHOD TO EXERCISE THE RIGHT TO OPT OUT OF THE PROCESSING OF PERSONAL DATA CONCERNING THE CONSUMER PURSUANT TO SUBSECTION (1)(a)(I) OF THIS SECTION. THE CONTROLLER SHALL PROVIDE THE OPT-OUT METHOD CLEARLY AND CONSPICUOUSLY IN ANY PRIVACY NOTICE REQUIRED TO BE PROVIDED TO CONSUMERS UNDER THIS PART 13, AND IN A CLEAR, CONSPICUOUS, AND READILY ACCESSIBLE LOCATION OUTSIDE THE PRIVACY NOTICE.

(IV) (A) A CONTROLLER THAT PROCESSES PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA MAY ALLOW CONSUMERS TO EXERCISE THE RIGHT TO OPT OUT OF THE PROCESSING OF PERSONAL DATA CONCERNING THE CONSUMER FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA PURSUANT TO SUBSECTIONS (1)(a)(I)(A) AND (1)(a)(I)(B) OF THIS SECTION BY CONTROLLERS THROUGH A USER-SELECTED UNIVERSAL OPT-OUT MECHANISM THAT MEETS THE TECHNICAL SPECIFICATIONS ESTABLISHED BY THE ATTORNEY GENERAL PURSUANT TO SECTION 6-1-1313. THIS SUBSECTION (1)(a)(IV)(A) IS REPEALED, EFFECTIVE JULY 1, 2024.

(B) EFFECTIVE JULY 1, 2024, A CONTROLLER THAT PROCESSES PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA SHALL ALLOW CONSUMERS TO EXERCISE THE RIGHT TO OPT OUT OF THE PROCESSING OF PERSONAL DATA CONCERNING THE CONSUMER FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA PURSUANT TO SUBSECTIONS (1)(a)(I)(A) AND (1)(a)(I)(B) OF THIS SECTION BY CONTROLLERS THROUGH A USER-SELECTED UNIVERSAL OPT-OUT MECHANISM THAT MEETS THE TECHNICAL SPECIFICATIONS ESTABLISHED BY THE ATTORNEY GENERAL PURSUANT TO SECTION 6-1-1313.

(C) NOTWITHSTANDING A CONSUMER'S DECISION TO EXERCISE THE RIGHT TO OPT OUT OF THE PROCESSING OF PERSONAL DATA THROUGH A UNIVERSAL OPT-OUT MECHANISM PURSUANT TO SUBSECTION (1)(a)(IV)(B) OF THIS SECTION, A CONTROLLER MAY ENABLE THE CONSUMER TO CONSENT, THROUGH A WEB PAGE, APPLICATION, OR A SIMILAR METHOD, TO THE PROCESSING OF THE CONSUMER'S PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA, AND THE CONSENT TAKES PRECEDENCE OVER ANY CHOICE REFLECTED THROUGH THE UNIVERSAL OPT-OUT MECHANISM. BEFORE OBTAINING A CONSUMER'S CONSENT TO PROCESS PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA PURSUANT TO THIS SUBSECTION (1)(a)(IV)(C), A CONTROLLER SHALL PROVIDE THE CONSUMER WITH A CLEAR AND CONSPICUOUS NOTICE INFORMING THE CONSUMER ABOUT THE CHOICES AVAILABLE UNDER THIS SECTION, DESCRIBING THE CATEGORIES OF PERSONAL DATA TO BE PROCESSED AND THE PURPOSES FOR WHICH THEY WILL BE PROCESSED, AND EXPLAINING HOW AND WHERE THE CONSUMER MAY WITHDRAW CONSENT. THE WEB PAGE, APPLICATION, OR OTHER MEANS BY WHICH A CONTROLLER OBTAINS A CONSUMER'S CONSENT TO PROCESS PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA MUST ALSO ALLOW THE CONSUMER TO REVOKE THE CONSENT AS EASILY AS IT IS AFFIRMATIVELY PROVIDED.

(b) **Right of access**. A CONSUMER HAS THE RIGHT TO CONFIRM WHETHER A CONTROLLER IS PROCESSING PERSONAL DATA CONCERNING THE CONSUMER AND TO ACCESS THE CONSUMER'S PERSONAL DATA.

(c) **Right to correction**. A CONSUMER HAS THE RIGHT TO CORRECT INACCURACIES IN THE CONSUMER'S PERSONAL DATA, TAKING INTO ACCOUNT THE NATURE OF THE PERSONAL DATA AND THE PURPOSES OF THE PROCESSING OF THE CONSUMER'S PERSONAL DATA.

(d) **Right to deletion**. A CONSUMER HAS THE RIGHT TO DELETE PERSONAL DATA CONCERNING THE CONSUMER.

(e) **Right to data portability**. WHEN EXERCISING THE RIGHT TO ACCESS PERSONAL DATA PURSUANT TO SUBSECTION (1)(b) OF THIS SECTION, A CONSUMER HAS THE RIGHT TO OBTAIN THE PERSONAL DATA IN A PORTABLE AND, TO THE EXTENT TECHNICALLY FEASIBLE, READILY USABLE FORMAT THAT ALLOWS THE CONSUMER TO TRANSMIT THE DATA TO ANOTHER ENTITY WITHOUT HINDRANCE. A CONSUMER MAY EXERCISE THIS RIGHT NO MORE THAN TWO TIMES PER CALENDAR YEAR. NOTHING IN THIS SUBSECTION (1)(e) REQUIRES A CONTROLLER TO PROVIDE THE DATA TO THE CONSUMER IN A MANNER THAT WOULD DISCLOSE THE CONTROLLER'S TRADE SECRETS.

(2) **Responding to consumer requests**. (a) A CONTROLLER SHALL INFORM A CONSUMER OF ANY ACTION TAKEN ON A REQUEST UNDER SUBSECTION (1) OF THIS SECTION WITHOUT UNDUE DELAY AND, IN ANY EVENT, WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF THE REQUEST. THE CONTROLLER MAY EXTEND THE FORTY-FIVE-DAY PERIOD BY FORTY-FIVE ADDITIONAL DAYS WHERE REASONABLY NECESSARY, TAKING INTO ACCOUNT THE COMPLEXITY AND NUMBER OF THE REQUESTS. THE CONTROLLER SHALL INFORM THE CONSUMER OF AN EXTENSION WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF THE REQUEST, TOGETHER WITH THE REASONS FOR THE DELAY.

(b) IF A CONTROLLER DOES NOT TAKE ACTION ON THE REQUEST OF A CONSUMER, THE CONTROLLER SHALL INFORM THE CONSUMER, WITHOUT UNDUE DELAY AND, AT THE LATEST, WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF THE REQUEST, OF THE REASONS FOR NOT TAKING ACTION AND INSTRUCTIONS FOR HOW TO APPEAL THE DECISION WITH THE CONTROLLER AS DESCRIBED IN SUBSECTION (3) OF THIS SECTION.

(c) UPON REQUEST, A CONTROLLER SHALL PROVIDE TO THE CONSUMER THE INFORMATION SPECIFIED IN THIS SECTION FREE OF CHARGE; EXCEPT THAT, FOR A SECOND OR SUBSEQUENT REQUEST WITHIN A TWELVE-MONTH PERIOD, THE CONTROLLER MAY CHARGE AN AMOUNT CALCULATED IN THE MANNER SPECIFIED IN SECTION 24-72-205 (5)(a).

(d) A CONTROLLER IS NOT REQUIRED TO COMPLY WITH A REQUEST TO EXERCISE ANY OF THE RIGHTS UNDER SUBSECTION (1) OF THIS SECTION IF THE CONTROLLER IS UNABLE TO AUTHENTICATE THE REQUEST USING COMMERCIALLY REASONABLE EFFORTS, IN WHICH CASE THE CONTROLLER MAY REQUEST THE PROVISION OF ADDITIONAL INFORMATION REASONABLY NECESSARY TO AUTHENTICATE THE REQUEST.

(3) (a) A CONTROLLER SHALL ESTABLISH AN INTERNAL PROCESS WHEREBY CONSUMERS MAY APPEAL A REFUSAL TO TAKE ACTION ON A REQUEST TO EXERCISE ANY OF THE RIGHTS UNDER SUBSECTION (1) OF THIS SECTION WITHIN A REASONABLE PERIOD AFTER THE CONSUMER'S RECEIPT OF THE NOTICE SENT BY THE CONTROLLER UNDER SUBSECTION (2)(b) OF THIS SECTION. THE APPEAL PROCESS MUST BE CONSPICUOUSLY AVAILABLE AND AS EASY TO USE AS THE PROCESS FOR SUBMITTING A REQUEST UNDER THIS SECTION.

(b) WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF AN APPEAL, A CONTROLLER SHALL INFORM THE CONSUMER OF ANY ACTION TAKEN OR NOT TAKEN IN RESPONSE TO THE APPEAL, ALONG WITH A WRITTEN EXPLANATION OF THE REASONS IN SUPPORT OF THE RESPONSE. THE CONTROLLER MAY EXTEND THE FORTY-FIVE-DAY PERIOD BY SIXTY ADDITIONAL DAYS WHERE REASONABLY NECESSARY, TAKING INTO ACCOUNT THE COMPLEXITY AND NUMBER OF REQUESTS SERVING AS THE BASIS FOR THE APPEAL. THE CONTROLLER SHALL INFORM THE CONSUMER OF AN EXTENSION WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF THE APPEAL, TOGETHER WITH THE REASONS FOR THE DELAY.

(c) THE CONTROLLER SHALL INFORM THE CONSUMER OF THE CONSUMER'S ABILITY TO CONTACT THE ATTORNEY GENERAL IF THE CONSUMER HAS CONCERNS ABOUT THE RESULT OF THE APPEAL.

6-1-1307. Processing de-identified data. (1) THIS PART 13 DOES NOT REQUIRE A CONTROLLER OR PROCESSOR TO DO ANY OF THE FOLLOWING SOLELY FOR PURPOSES OF COMPLYING WITH THIS PART 13:

(a) REIDENTIFY DE-IDENTIFIED DATA;

(b) COMPLY WITH AN AUTHENTICATED CONSUMER REQUEST TO ACCESS, CORRECT, DELETE, OR PROVIDE PERSONAL DATA IN A PORTABLE FORMAT PURSUANT TO SECTION 6-1-1306 (1), IF ALL OF THE FOLLOWING ARE TRUE:

(I) (A) THE CONTROLLER IS NOT REASONABLY CAPABLE OF ASSOCIATING THE REQUEST WITH THE PERSONAL DATA; OR

(B) IT WOULD BE UNREASONABLY BURDENSOME FOR THE CONTROLLER TO ASSOCIATE THE REQUEST WITH THE PERSONAL DATA;

(II) THE CONTROLLER DOES NOT USE THE PERSONAL DATA TO RECOGNIZE OR RESPOND TO THE SPECIFIC CONSUMER WHO IS THE SUBJECT OF THE PERSONAL DATA OR ASSOCIATE THE PERSONAL DATA WITH OTHER PERSONAL DATA ABOUT THE SAME SPECIFIC CONSUMER; AND

(III) THE CONTROLLER DOES NOT SELL THE PERSONAL DATA TO ANY THIRD PARTY OR OTHERWISE VOLUNTARILY DISCLOSE THE PERSONAL DATA TO ANY THIRD PARTY, EXCEPT AS OTHERWISE AUTHORIZED BY THE CONSUMER; OR

(c) MAINTAIN DATA IN IDENTIFIABLE FORM OR COLLECT, OBTAIN, RETAIN, OR ACCESS ANY DATA OR TECHNOLOGY IN ORDER TO ENABLE THE CONTROLLER TO ASSOCIATE AN AUTHENTICATED CONSUMER REQUEST WITH PERSONAL DATA.

(2) A CONTROLLER THAT USES DE-IDENTIFIED DATA SHALL EXERCISE REASONABLE OVERSIGHT TO MONITOR COMPLIANCE WITH ANY CONTRACTUAL COMMITMENTS TO WHICH THE DE-IDENTIFIED DATA ARE SUBJECT AND SHALL TAKE APPROPRIATE STEPS TO ADDRESS ANY BREACHES OF CONTRACTUAL COMMITMENTS.

(3) THE RIGHTS CONTAINED IN SECTION 6-1-1306 (1)(b) TO (1)(e) DO NOT APPLY TO PSEUDONYMOUS DATA IF THE CONTROLLER CAN DEMONSTRATE THAT THE INFORMATION NECESSARY TO IDENTIFY THE CONSUMER IS KEPT SEPARATELY AND IS SUBJECT TO EFFECTIVE TECHNICAL AND ORGANIZATIONAL CONTROLS THAT PREVENT THE CONTROLLER FROM ACCESSING THE INFORMATION.

6-1-1308. Duties of controllers. (1) Duty of transparency. (a) A CONTROLLER SHALL PROVIDE CONSUMERS WITH A REASONABLY ACCESSIBLE, CLEAR, AND MEANINGFUL PRIVACY NOTICE THAT INCLUDES:

(I) THE CATEGORIES OF PERSONAL DATA COLLECTED OR PROCESSED BY THE CONTROLLER OR A PROCESSOR;

(II) THE PURPOSES FOR WHICH THE CATEGORIES OF PERSONAL DATA ARE PROCESSED;

(III) How AND WHERE CONSUMERS MAY EXERCISE THE RIGHTS PURSUANT TO SECTION 6-1-1306, INCLUDING THE CONTROLLER'S CONTACT INFORMATION AND HOW A CONSUMER MAY APPEAL A CONTROLLER'S ACTION WITH REGARD TO THE CONSUMER'S REQUEST;

(IV) THE CATEGORIES OF PERSONAL DATA THAT THE CONTROLLER SHARES WITH THIRD PARTIES, IF ANY; AND

(V) THE CATEGORIES OF THIRD PARTIES, IF ANY, WITH WHOM THE CONTROLLER SHARES PERSONAL DATA.

(b) IF A CONTROLLER SELLS PERSONAL DATA TO THIRD PARTIES OR PROCESSES PERSONAL DATA FOR TARGETED ADVERTISING, THE CONTROLLER SHALL CLEARLY AND CONSPICUOUSLY DISCLOSE THE SALE OR PROCESSING, AS WELL AS THE MANNER IN WHICH A CONSUMER MAY EXERCISE THE RIGHT TO OPT OUT OF THE SALE OR PROCESSING.

(c) A CONTROLLER SHALL NOT:

(I) REQUIRE A CONSUMER TO CREATE A NEW ACCOUNT IN ORDER TO EXERCISE A RIGHT; OR

(II) BASED SOLELY ON THE EXERCISE OF A RIGHT AND UNRELATED TO FEASIBILITY OR THE VALUE OF A SERVICE, INCREASE THE COST OF, OR DECREASE THE AVAILABILITY OF, THE PRODUCT OR SERVICE.

(d) NOTHING IN THIS PART 13 SHALL BE CONSTRUED TO REQUIRE A CONTROLLER TO PROVIDE A PRODUCT OR SERVICE THAT REQUIRES THE PERSONAL DATA OF A CONSUMER THAT THE CONTROLLER DOES NOT COLLECT OR MAINTAIN OR TO PROHIBIT A CONTROLLER FROM OFFERING A DIFFERENT PRICE, RATE, LEVEL, QUALITY, OR SELECTION OF GOODS OR SERVICES TO A CONSUMER, INCLUDING OFFERING GOODS OR SERVICES FOR NO FEE, IF THE OFFER IS RELATED TO A CONSUMER'S VOLUNTARY PARTICIPATION IN A BONA FIDE LOYALTY, REWARDS, PREMIUM FEATURES, DISCOUNT, OR CLUB CARD PROGRAM.

(2) **Duty of purpose specification**. A CONTROLLER SHALL SPECIFY THE EXPRESS PURPOSES FOR WHICH PERSONAL DATA ARE COLLECTED AND PROCESSED.

(3) **Duty of data minimization**. A CONTROLLER'S COLLECTION OF PERSONAL DATA MUST BE ADEQUATE, RELEVANT, AND LIMITED TO WHAT IS REASONABLY NECESSARY IN RELATION TO THE SPECIFIED PURPOSES FOR WHICH THE DATA ARE PROCESSED.

(4) **Duty to avoid secondary use**. A CONTROLLER SHALL NOT PROCESS PERSONAL DATA FOR PURPOSES THAT ARE NOT REASONABLY NECESSARY TO OR COMPATIBLE WITH THE SPECIFIED PURPOSES FOR WHICH THE PERSONAL DATA ARE PROCESSED, UNLESS THE CONTROLLER FIRST OBTAINS THE CONSUMER'S CONSENT.

(5) **Duty of care.** A CONTROLLER SHALL TAKE REASONABLE MEASURES TO SECURE PERSONAL DATA DURING BOTH STORAGE AND USE FROM UNAUTHORIZED ACQUISITION. THE DATA SECURITY PRACTICES MUST BE APPROPRIATE TO THE VOLUME, SCOPE, AND NATURE OF THE PERSONAL DATA PROCESSED AND THE NATURE OF THE BUSINESS.

(6) **Duty to avoid unlawful discrimination.** A CONTROLLER SHALL NOT PROCESS PERSONAL DATA IN VIOLATION OF STATE OR FEDERAL LAWS THAT PROHIBIT UNLAWFUL DISCRIMINATION AGAINST CONSUMERS.

(7) **Duty regarding sensitive data.** A CONTROLLER SHALL NOT PROCESS A CONSUMER'S SENSITIVE DATA WITHOUT FIRST OBTAINING THE CONSUMER'S CONSENT OR, IN THE CASE OF THE PROCESSING OF PERSONAL DATA CONCERNING A KNOWN CHILD, WITHOUT FIRST OBTAINING CONSENT FROM THE CHILD'S PARENT OR LAWFUL GUARDIAN.

6-1-1309. Data protection assessments - attorney general access and evaluation - definition. (1) A CONTROLLER SHALL NOT CONDUCT PROCESSING THAT PRESENTS A HEIGHTENED RISK OF HARM TO A CONSUMER WITHOUT CONDUCTING AND DOCUMENTING A DATA PROTECTION ASSESSMENT OF EACH OF ITS PROCESSING ACTIVITIES THAT INVOLVE PERSONAL DATA ACQUIRED ON OR AFTER THE EFFECTIVE DATE OF THIS SECTION THAT PRESENT A HEIGHTENED RISK OF HARM TO A CONSUMER.

(2) FOR PURPOSES OF THIS SECTION, "PROCESSING THAT PRESENTS A HEIGHTENED RISK OF HARM TO A CONSUMER" INCLUDES THE FOLLOWING:

(a) PROCESSING PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR FOR PROFILING IF THE PROFILING PRESENTS A REASONABLY FORESEEABLE RISK OF:

(I) UNFAIR OR DECEPTIVE TREATMENT OF, OR UNLAWFUL DISPARATE IMPACT ON, CONSUMERS;

(II) FINANCIAL OR PHYSICAL INJURY TO CONSUMERS;

(III) A PHYSICAL OR OTHER INTRUSION UPON THE SOLITUDE OR SECLUSION, OR THE PRIVATE AFFAIRS OR CONCERNS, OF CONSUMERS IF THE INTRUSION WOULD BE OFFENSIVE TO A REASONABLE PERSON; OR

(IV) OTHER SUBSTANTIAL INJURY TO CONSUMERS;

(b) SELLING PERSONAL DATA; AND

(c) PROCESSING SENSITIVE DATA.

(3) DATA PROTECTION ASSESSMENTS MUST IDENTIFY AND WEIGH THE BENEFITS THAT MAY FLOW, DIRECTLY AND INDIRECTLY, FROM THE PROCESSING TO THE CONTROLLER, THE CONSUMER, OTHER STAKEHOLDERS, AND THE PUBLIC AGAINST THE POTENTIAL RISKS TO THE RIGHTS OF THE CONSUMER ASSOCIATED WITH THE PROCESSING, AS MITIGATED BY SAFEGUARDS THAT THE CONTROLLER CAN EMPLOY TO REDUCE THE RISKS. THE CONTROLLER SHALL FACTOR INTO THIS ASSESSMENT THE USE OF DE-IDENTIFIED DATA AND THE REASONABLE EXPECTATIONS OF CONSUMERS, AS WELL AS THE CONTEXT OF THE PROCESSING AND THE RELATIONSHIP BETWEEN THE CONTROLLER AND THE CONSUMER WHOSE PERSONAL DATA WILL BE PROCESSED.

(4) A CONTROLLER SHALL MAKE THE DATA PROTECTION ASSESSMENT AVAILABLE TO THE ATTORNEY GENERAL UPON REQUEST. THE ATTORNEY GENERAL MAY EVALUATE THE DATA PROTECTION ASSESSMENT FOR COMPLIANCE WITH THE DUTIES CONTAINED IN SECTION 6-1-1308 AND WITH OTHER LAWS, INCLUDING THIS ARTICLE 1. DATA PROTECTION ASSESSMENTS ARE CONFIDENTIAL AND EXEMPT FROM PUBLIC INSPECTION AND COPYING UNDER THE "COLORADO OPEN RECORDS ACT", PART 2 OF ARTICLE 72 OF TITLE 24. THE DISCLOSURE OF A DATA PROTECTION ASSESSMENT PURSUANT TO A REQUEST FROM THE ATTORNEY GENERAL UNDER THIS SUBSECTION (4) DOES NOT CONSTITUTE A WAIVER OF ANY ATTORNEY-CLIENT PRIVILEGE OR WORK-PRODUCT PROTECTION THAT MIGHT OTHERWISE EXIST WITH RESPECT TO THE ASSESSMENT AND ANY INFORMATION CONTAINED IN THE ASSESSMENT.

(5) A SINGLE DATA PROTECTION ASSESSMENT MAY ADDRESS A COMPARABLE SET OF PROCESSING OPERATIONS THAT INCLUDE SIMILAR ACTIVITIES.

(6) DATA PROTECTION ASSESSMENT REQUIREMENTS APPLY TO PROCESSING ACTIVITIES CREATED OR GENERATED AFTER JULY 1, 2023, AND ARE NOT RETROACTIVE.

6-1-1310. Liability. (1) NOTWITHSTANDING ANY PROVISION IN PART 1 OF THIS ARTICLE 1, THIS PART 13 DOES NOT AUTHORIZE A PRIVATE RIGHT OF ACTION FOR A VIOLATION OF THIS PART 13 OR ANY OTHER PROVISION OF LAW. THIS SUBSECTION (1) NEITHER RELIEVES ANY PARTY FROM ANY DUTIES OR OBLIGATIONS IMPOSED, NOR ALTERS ANY INDEPENDENT RIGHTS THAT

CONSUMERS HAVE, UNDER OTHER LAWS, INCLUDING THIS ARTICLE 1, THE PAGE 26-SENATE BILL 21-190 STATE CONSTITUTION, OR THE UNITED STATES CONSTITUTION.

(2) WHERE MORE THAN ONE CONTROLLER OR PROCESSOR, OR BOTH A CONTROLLER AND A PROCESSOR, INVOLVED IN THE SAME PROCESSING VIOLATES THIS PART 13, THE LIABILITY SHALL BE ALLOCATED AMONG THE PARTIES ACCORDING TO PRINCIPLES OF COMPARATIVE FAULT.

6-1-1311. Enforcement - penalties - repeal. (1) (a) NOTWITHSTANDING ANY OTHER PROVISION OF THIS ARTICLE 1, THE ATTORNEY GENERAL AND DISTRICT ATTORNEYS HAVE EXCLUSIVE AUTHORITY TO ENFORCE THIS PART 13 BY BRINGING AN ACTION IN THE NAME OF THE STATE OR AS PARENS PATRIAE ON BEHALF OF PERSONS RESIDING IN THE STATE TO ENFORCE THIS PART 13 AS PROVIDED IN THIS ARTICLE 1, INCLUDING SEEKING AN INJUNCTION TO ENJOIN A VIOLATION OF THIS PART 13.

(b) NOTWITHSTANDING ANY OTHER PROVISION OF THIS ARTICLE 1, NOTHING IN THIS PART 13 SHALL BE CONSTRUED AS PROVIDING THE BASIS FOR, OR BEING SUBJECT TO, A PRIVATE RIGHT OF ACTION FOR VIOLATIONS OF THIS PART 13 OR ANY OTHER LAW.

(c) FOR PURPOSES ONLY OF ENFORCEMENT OF THIS PART 13 BY THE ATTORNEY GENERAL OR A DISTRICT ATTORNEY, A VIOLATION OF THIS PART 13 IS A DECEPTIVE TRADE PRACTICE.

(d) PRIOR TO ANY ENFORCEMENT ACTION PURSUANT TO SUBSECTION (1)(a) OF THIS SECTION, THE ATTORNEY GENERAL OR DISTRICT ATTORNEY MUST ISSUE A NOTICE OF VIOLATION TO THE CONTROLLER IF A CURE IS DEEMED POSSIBLE. IF THE CONTROLLER FAILS TO CURE THE VIOLATION WITHIN SIXTY DAYS AFTER RECEIPT OF THE NOTICE OF VIOLATION, AN ACTION MAY BE BROUGHT PURSUANT TO THIS SECTION. THIS SUBSECTION (1)(d) IS REPEALED, EFFECTIVE JANUARY 1, 2025.

(2) THE STATE TREASURER SHALL CREDIT ALL RECEIPTS FROM THE IMPOSITION OF CIVIL PENALTIES UNDER THIS PART 13 PURSUANT TO SECTION 24-31-108.

6-1-1312. Preemption - local governments. THIS PART 13 SUPERSEDES AND PREEMPTS LAWS, ORDINANCES, RESOLUTIONS, REGULATIONS, OR THE EQUIVALENT ADOPTED BY ANY STATUTORY OR HOME RULE MUNICIPALITY, COUNTY, OR CITY AND COUNTY REGARDING THE PROCESSING OF PERSONAL DATA BY CONTROLLERS OR PROCESSORS.

6-1-1313. Rules - opt-out mechanism. (1) THE ATTORNEY GENERAL MAY PROMULGATE RULES FOR THE PURPOSE OF CARRYING OUT THIS PART 13.

(2) BY JULY 1, 2023, THE ATTORNEY GENERAL SHALL ADOPT RULES THAT DETAIL THE TECHNICAL SPECIFICATIONS FOR ONE OR MORE UNIVERSAL OPT-OUT MECHANISMS THAT CLEARLY COMMUNICATE A CONSUMER'S AFFIRMATIVE, FREELY GIVEN, AND UNAMBIGUOUS CHOICE TO OPT OUT OF THE PROCESSING OF PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA PURSUANT TO SECTION 6-1-1306 (1)(a)(I)(A) OR (1)(a)(I)(B). THE ATTORNEY GENERAL MAY UPDATE THE RULES THAT DETAIL THE TECHNICAL

SPECIFICATIONS FOR THE MECHANISMS FROM TIME TO TIME TO REFLECT THE MEANS BY WHICH CONSUMERS INTERACT WITH CONTROLLERS. THE RULES MUST:

(a) NOT PERMIT THE MANUFACTURER OF A PLATFORM, BROWSER, DEVICE, OR ANY OTHER PRODUCT OFFERING A UNIVERSAL OPT-OUT MECHANISM TO UNFAIRLY DISADVANTAGE ANOTHER CONTROLLER;

(b) REQUIRE CONTROLLERS TO INFORM CONSUMERS ABOUT THE OPT-OUT CHOICES AVAILABLE UNDER SECTION 6-1-1306 (1)(a)(I);

(c) NOT ADOPT A MECHANISM THAT IS A DEFAULT SETTING, BUT RATHER CLEARLY REPRESENTS THE CONSUMER'S AFFIRMATIVE, FREELY GIVEN, AND UNAMBIGUOUS CHOICE TO OPT OUT OF THE PROCESSING OF PERSONAL DATA PURSUANT TO SECTION 6-1-1306 (1)(a)(I)(A) OR (1)(a)(I)(B);

(d) ADOPT A MECHANISM THAT IS CONSUMER-FRIENDLY, CLEARLY DESCRIBED, AND EASY TO USE BY THE AVERAGE CONSUMER;

(e) ADOPT A MECHANISM THAT IS AS CONSISTENT AS POSSIBLE WITH ANY OTHER SIMILAR MECHANISM REQUIRED BY LAW OR REGULATION IN THE UNITED STATES; AND

(f) PERMIT THE CONTROLLER TO ACCURATELY AUTHENTICATE THE CONSUMER AS A RESIDENT OF THIS STATE AND DETERMINE THAT THE MECHANISM REPRESENTS A LEGITIMATE REQUEST TO OPT OUT OF THE PROCESSING OF PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA PURSUANT TO SECTION 6-1-1306 (1)(a)(I)(A) OR (1)(a)(I)(B).

(3) BY JANUARY 1, 2025, THE ATTORNEY GENERAL MAY ADOPT RULES THAT GOVERN THE PROCESS OF ISSUING OPINION LETTERS AND INTERPRETIVE GUIDANCE TO DEVELOP AN OPERATIONAL FRAMEWORK FOR BUSINESS THAT INCLUDES A GOOD FAITH RELIANCE DEFENSE OF AN ACTION THAT MAY OTHERWISE CONSTITUTE A VIOLATION OF THIS PART 13. THE RULES MUST BECOME EFFECTIVE BY JULY 1, 2025.

SECTION 2. In Colorado Revised Statutes, amend 6-1-104 as follows:

6-1-104. Cooperative reporting. The district attorneys may cooperate in a statewide reporting system by receiving, on forms provided by the attorney general, complaints from persons concerning deceptive trade practices listed in section 6-1-105 and OR part 7 OR 13 of this article ARTICLE 1 and transmitting such THE complaints to the attorney general.

SECTION 3. In Colorado Revised Statutes, 6-1-105, **add** (1)(nnn) as follows:

6-1-105. Unfair or deceptive trade practices. (1) A person engages in a deceptive trade practice when, in the course of the person's business, vocation, or occupation, the person:

(nnn) VIOLATES ANY PROVISION OF PART 13 OF THIS ARTICLE 1 AS SPECIFIED IN SECTION 6-1-1311 (1)(c).

SECTION 4. In Colorado Revised Statutes, 6-1-107, amend (1) introductory portion as follows:

6-1-107. Powers of attorney general and district attorneys. (1) When the attorney general or a district attorney has reasonable cause to believe that any person, whether in this state or elsewhere, has engaged in or is engaging in any deceptive trade practice listed in section 6-1-105 or part 7 OR 13 of this ~~article~~ ARTICLE 1, the attorney general or district attorney may:

SECTION 5. In Colorado Revised Statutes, 6-1-108, amend (1) as follows:

6-1-108. Subpoenas - hearings - rules. (1) When the attorney general or a district attorney has reasonable cause to believe that a person, whether in this state or elsewhere, has engaged in or is engaging in a deceptive trade practice listed in section 6-1-105 or part 7 OR 13 of this article 1, the attorney general or a district attorney, in addition to other powers conferred upon him-or her THE ATTORNEY GENERAL OR A DISTRICT ATTORNEY by this article 1, may issue subpoenas to require the attendance of witnesses or the production of documents, administer oaths, conduct hearings in aid of any investigation or inquiry, and prescribe such forms and promulgate such rules as may be necessary to administer the provisions of this article 1.

SECTION 6. In Colorado Revised Statutes, 6-1-110, **amend** (1) and (2) as follows:

6-1-110. Restraining orders - injunctions - assurances of discontinuance. (1) Whenever the attorney general or a district attorney has cause to believe that a person has engaged in or is engaging in any deceptive trade practice listed in section 6-1-105 or part 7 OR 13 of this ARTICLE 1, the attorney general or district attorney may apply for and obtain, in an action in the appropriate district court of this state, a temporary restraining order or injunction, or both, pursuant to the Colorado rules of civil procedure, prohibiting such THE person from continuing such THE practices, or engaging therein, or doing any act in furtherance thereof. The court may make such orders or judgments as may be necessary to prevent the use or employment by such THE person of any such deceptive trade practice or which THAT may be necessary to completely compensate or restore to the original position of any person injured by means of any such practice or to prevent any unjust enrichment by any person through the use or employment of any deceptive trade practice.

(2) Where the attorney general or a district attorney has authority to institute a civil action or other proceeding pursuant to the provisions of this ~~article~~ ARTICLE 1, the attorney general or district attorney may accept, in lieu thereof or as a part thereof, an assurance of discontinuance of any deceptive trade practice listed in section 6-1-105 or part 7 OR 13 of this ~~article. Such~~ ARTICLE 1. THE assurance may include a stipulation for the voluntary payment by the alleged violator of the costs of investigation and any action or proceeding by the attorney general or a district attorney and any amount necessary to restore to any person any money or property that may have been acquired ~~by such~~ THE alleged violator by means of any such deceptive trade practice. Any such assurance of discontinuance accepted by the attorney general or a district attorney and any such stipulation filed with the court as a part of any such action or proceeding ~~shall be~~ is a matter of public record unless the attorney general or the district attorney determines, at ~~his or her~~ THE discretion OF THE ATTORNEY GENERAL OR DISTRICT ATTORNEY, that it will be confidential to the parties to the action or proceeding and to the court and its employees. Upon the filing of a civil action by the attorney general or a district attorney alleging that a confidential assurance of discontinuance or stipulation accepted pursuant to this subsection (2) has been violated, said THE assurance of discontinuance or stipulation shall

~~thereupon be deemed~~ BECOMES a public record and open to inspection by any person. Proof by a preponderance of the evidence of a violation of any such assurance or stipulation ~~shall constitute~~ CONSTITUTES prima facie evidence of a deceptive trade practice for the purposes of any civil action or proceeding brought thereafter by the attorney general or a district attorney, whether a new action or a subsequent motion or petition in any pending action or proceeding.

SECTION 7. Act subject to petition - effective date - applicability. (1) This act takes effect July 1, 2023; except that, if a referendum petition is filed pursuant to section 1 (3) of article V of the state constitution against this act or an item, section, or part of this act within the ninety-day period after final adjournment of the general assembly, then the act, item, section, or part will not take effect unless approved by the people at the general election to be held in November 2022 and, in such case, will take effect July 1, 2023, or on the date of the official declaration of the vote thereon by the governor, whichever is later.

(2) This act applies to conduct occurring on or after the applicable effective date of this act.

CPA Rules:

COLORADO DEPARTMENT OF LAW

Consumer Protection Section

Colorado Privacy Act Rules

4 CCR-904-3

PART 1 GENERAL APPLICABILITY

Rule 1.01 AUTHORITY

The statutory authority for this Part 904-3 is sections C.R.S. §§ 6-1-108(1) and 6-1-1313.

Rule 1.02 SEVERABILITY

If any provision of these Colorado Privacy Act Rules, 4 CCR 904-3, is found to be invalid by a court of competent jurisdiction, the remaining provisions of the Rules shall remain in full force and effect.

PART 2 DEFINITIONS

Rule 2.01 AUTHORITY AND PURPOSE

The statutory authority for the rules in this Part 2 is C.R.S. §§ 6-1-108(1), 6-1-1303, and 6-1-1313. The purpose of these rules is to define certain undefined terms that are used throughout the Colorado Privacy Act, C.R.S. § 6-1-1301, *et seq.*, and these Colorado Privacy Act Rules, 4 CCR 904-3, including but not limited to certain undefined terms that are used in the definitions set forth in C.R.S. § 6-1-1303. The terms defined by this rule and C.R.S. § 6-1-1303 are capitalized where they appear in the rules to let the reader know to refer back to the definitions. When a term is used in a conventional sense, and is not intended to be a defined term, it is not capitalized.

Rule 2.02 DEFINED TERMS

The following definitions of terms, in addition to those set forth in C.R.S. § 6-1-1303, apply to these Colorado Privacy Act Rules, 4 CCR 904-3, promulgated pursuant to the Colorado Privacy Act, unless the context requires otherwise:

"**Authorized Agent**" as referred to in C.R.S. § 6-1-1306(1)(a)(II) means a person or entity authorized by the Consumer to act on the Consumer's behalf.

"**Automated Processing**" as referred to in CRS § 6-1-1303(20) means the Processing of Personal Data that is automated through the use of computers, computer programs or software, or other digital technology.

"**Biometric Data**" as referred to in C.R.S. § 6-1-1303(24)(b) means Biometric Identifiers that are used or intended to be used, singly or in combination with each other or with other Personal Data, for identification purposes. Unless such data is used for identification purposes, "Biometric Data" does not include (a) a digital or physical photograph, (b) an audio or voice recording, or (c) any data generated from a digital or physical photograph or an audio or video recording.

"**Biometric Identifiers**" means data generated by the technological processing, measurement, or analysis of an individual's biological, physical, or behavioral characteristics, including but not limited to a fingerprint, a voiceprint, eye retinas, irises, facial mapping, facial geometry, facial templates, or other unique biological, physical, or behavioral patterns or characteristics.

"**Bona Fide Loyalty Program**" as referred to in C.R.S. § 1-6-1308(1)(d) is defined as a loyalty, rewards, premium feature, discount, or club card program established for the genuine purpose of providing discounts, rewards, or other actual value to Consumers that voluntarily participate in that program.

"**Bona Fide Loyalty Program Benefit**" is defined as an offer of superior price, rate, level, quality, or selection of goods or services provided to a Consumer through a Bona Fide Loyalty Program.

"**Data Broker**" is defined as a Controller that knowingly collects and sells to Third Parties the Personal Data of a Consumer with whom the Controller does not have a direct relationship.

"**Data Right**" or "**Data Rights**" means the Consumer Personal Data rights granted in C.R.S. § 6-11306(1).

"**Disability**" or "**Disabilities**" has the same meaning as set forth in C.R.S. § 24-85-102(2.3).

"**Human Involved Automated Processing**" means the Automated Processing of Personal Data where human involvement in the Processing includes meaningful consideration of available data used in the Processing as well as the authority to change or influence the outcome of the Processing.

"**Human Reviewed Automated Processing**" means the Automated Processing of Personal Data where a human reviews the Processing but the level of human review does not rise to the level required for Human Involved Automated Processing. Reviewing the output of the Automated Processing with no meaningful consideration does not rise to the level of Human Involved Automated Processing.

"**Information that a Controller has a reasonable basis to believe the Consumer has lawfully made available to the general public**" as referred to in C.R.S. § 6-1-1303(17)(b) means the type of information known to be available to the general public, information that a Consumer has intentionally made available to the general public, or information that a Consumer has made available under federal or state law, including but not limited to:

1. Personal Data found in a telephone book, a television or radio program, or a national or local news publication;

2. Personal Data that has been intentionally made available by the Consumer through a website or online service where the Consumer has not restricted the information to a specific audience;

3. A visual observation of an individual's physical presence in a public place by another person, not including data collected by a device in the individual's possession; and

4. A disclosure that has been made to the general public as required by federal, state, or local law.

"**Intimate Image**" means any visual depiction, photograph, film, video, recording, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, that depicts an identified or identifiable person's private parts, or a person engaged in a private act, in circumstances in which a reasonable person would reasonably expect to be afforded privacy. For purposes of this defined term, the term "private parts" includes:

1. Exposed human genitals or pubic area, with less than an opaque covering;

2. A female breast or any portion of the female breast below the top of the areola, with less than an opaque covering;

3. A part of the body that, if revealed publicly, the subject would find sensitive or offensive based on their religious beliefs.

"**Opt-Out Purpose**" or "**Opt-Out Purposes**" means the categories of data Processing from which the Consumer may opt out pursuant to C.R.S. § 6-1-1306(1)(a).

''**Publicly Available Information**" as referred to in C.R.S. § 6-1-1303(17) does not include:

1. Any Personal Data obtained or processed in in violation of C.R.S. §§ 18-7-107 or 18-7801.

2. Inferences made exclusively from multiple independent sources of publicly available information;

3. Biometric Data;

4. Genetic Information;

5. Publicly Available Information that has been combined with non-publicly available Personal Data; or

6. Nonconsensual Intimate Images known to the Controller.

"**Revealing**" as referred to in C.R.S. § 6-1-1303(24)(a) includes Sensitive Data Inferences. For example:

1. While geolocation information at a high level may not be considered Sensitive Data, geolocation data which shows an individual visited a mosque and is used to indicate that individual's religious beliefs is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a). Similarly, geolocation data which shows an individual visited a reproductive health clinic and is used to indicate an individual's health condition or sex life is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a).

2. While web browsing data at a high level may not be considered Sensitive Data, web browsing data which, alone or in combination with other Personal Data, creates a profile that indicates an individual's sexual orientation and is considered Sensitive Data under C.R.S. § 6-1-1303(24)(a).

"**Sensitive Data Inference**" or "**Sensitive Data Inferences**" means inferences made by a Controller based on Personal Data, alone or in combination with other data, which indicate an individual's racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status.

"**Solely Automated Processing**" means the Automated Processing of Personal Data with no human review, oversight, involvement, or intervention.

"Universal Opt-Out Mechanism" or "Universal Opt-Out Mechanisms" means mechanisms that clearly communicate a Consumer's affirmative, freely given, and unambiguous choice to opt out of the Processing of Personal Data for purposes of Targeted Advertising or the Sale of Personal Data pursuant to C.R.S. § 6-1-1306 (1)(a)(I)(A) OR (1)(a)(I)(B), which meets the technical specifications set forth pursuant to C.R.S. § 6-1-1313(2).

PART 3 CONSUMER DISCLOSURES

Rule 3.01

A. **The statutory authority for the rules in this Part 3 is C.R.S. §§ 6-1-108(1) and 6-1-1313. The purpose of the rules in Part 3 is to ensure that disclosures, notifications, and other communications to Consumers are clear, accessible, and understandable to Consumers so that Consumers can understand and are able to exercise the full scope of their rights under the Colorado Privacy Act, C.R.S. § 6-1-1303, *et seq*.**

Rule 3.02 REQUIREMENTS FOR DISCLOSURES, NOTIFICATIONS, AND OTHER COMMUNICATIONS TO CONSUMERS

A. Disclosures to Consumers pursuant to 4 CCR 904, Rules 3-4.02, 5.03, 6.01, 6.05, and 7.04 must be:

1. Understandable and accessible to a Controller's target audiences, considering the vulnerabilities or unique characteristics of the audience and paying particular attention to the vulnerabilities of Children. For example, they shall use plain, straightforward language and avoid technical or legal jargon.

2. Reasonably accessible to Consumers with Disabilities, including through the use of digital accessibility tools. For notices provided online, the Controller shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference as described at 4 CCR 903-3-10.02. In other contexts, the Controller shall provide information on how a Consumer with a Disability may access the disclosure or communication in an alternative format.

3. Available in the languages in which the Controller in its ordinary course provides web pages, interfaces, contracts, disclaimers, sale announcements, and other information to Consumers. Disclosures and communications sent directly to Consumers must be sent in the language in which the Consumer ordinarily interacts with the Controller.

4. Available through an interface regularly used in conjunction with the Controller's product or service.

5. Readable on all devices through which Consumers interact with the Controller, including on smaller screens and through mobile applications, if applicable.

6. Unless otherwise stated, notifications from Controllers to Consumers shall be communicated in a manner by which the Controller regularly interacts with Consumers.

PART 4 CONSUMER PERSONAL DATA RIGHTS

Rule 4.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in this Part 4 is C.R.S. §§ 6-1-108(1), 6-1-1306, and 6-11313. The purpose of the rules in Part 4 is to clarify the scope of Consumer Personal Data rights and standards for the processes required to facilitate the exercise of those rights.

Rule 4.02 SUBMITTING REQUESTS TO EXERCISE PERSONAL DATA RIGHTS

A. Pursuant to C.R.S. § 6-1-1306(1), a Controller's privacy notice must include specific methods through which a Consumer may submit requests to exercise Data Rights. Any method specified by a Controller must comply with each of the following:

1. Consider the ways in which Consumers normally interact with the Controller:

   a. A Controller that operates exclusively online and has a direct relationship with a Consumer from whom it collects Personal Data shall only be required to provide an email address for submitting access, correction, deletion, or data portability requests.

   b. A Controller that does not fall within subsection (A)(1)(a), above, shall provide two or more designated methods for submitting a Data Rights request. If a Controller maintains a website, mobile application, or other digital presence, one method for submitting requests shall be through its website, mobile application, or digital interface, such as through a webform;

   c. If a Controller interacts with Consumers in person, the Controller shall consider providing an in-person method such as a printed form the Consumer can directly submit or send by mail; a tablet or computer portal that allows the Consumer to complete and submit an online form; or a telephone by which the Consumer can call the Controller's toll-free number.

2. Comply with requirements provided in 4 CCR 904-3, Rule 3.01;

3. Use reasonable data security measures, consistent with 4 CCR 904-3, Rule 6.09, when exchanging information in furtherance of Data Rights requests, considering the volume, scope and nature of Personal Data that may be exchanged;

4. Be easy for Consumers to execute, requiring a minimal number of steps; and

5. Not use Dark Patterns, as defined by C.R.S. § 6-1-1303(9) and prohibited by 4 CCR 9043, Rule 7.09.

B. The Data Rights request method does not have to be specific to Colorado, so long as the request method:

1. Clearly indicates which rights are available to Colorado Consumers;

2. Provides all Data Rights available to Colorado Consumers;

3. Provides Colorado Consumers a clear understanding of how to exercise their rights; and

4. Meets all other requirements of this part, 4 CCR 904-3, Rule 4.02.

C. When a Consumer submits a Data Rights request, a Controller may only collect Personal Data through the request process if the Personal Data is reasonably necessary to Authenticate the Consumer, respond to the request, or effectuate the Data Rights request.

D. A Controller must not require a Consumer to create a new user account to exercise their Data Rights request, but may require a Consumer to use an existing password-protected account.

E. If a Consumer or Authorized Agent submits a request for an Opt-Out Purpose in a manner that is not one of the Controller's specified Data Rights request methods, or the request is otherwise deficient in a manner unrelated to the Authentication process, the Controller shall either: (1) treat the request as if it had been submitted in accordance with the Controller's specified request methods, or (2) provide the Consumer with information on how to submit the request or remedy any deficiencies in the request.

Rule 4.03 RIGHT TO OPT OUT

A. A Controller shall comply with an opt-out request by:

1. Ceasing to Process the Consumer's Personal Data for the Opt-Out Purpose(s) as soon as feasibly possible, but no later than fifteen (15) days from the date the Controller receives the request.

2. Maintaining a record of the opt-out request and response, in compliance with 4 CCR 9043, Rule 6.11.

B. A Controller must provide an opt-out method, either directly or through a link, clearly and conspicuously in its privacy notice as well as in a clear, conspicuous, and readily accessible location outside the privacy notice.

1. If a link is used, it must take a Consumer directly to the opt-out method and the link text must provide a clear understanding of its purpose, for example "Colorado Opt-Out Rights," "Personal Data Use Opt-Out," or "Your Opt-Out Rights."

2. The opt-out method must:

a. Comply with 4 CCR 904-3, Rule 4.02.

b. Describe the Consumer's right to opt out and provide instructions on how to opt out.

3. The clear, conspicuous, and readily accessible location must be:

a. Positioned in an obvious location of a website or application, such as the header or footer of a Controller's internet homepage, or an application's app store page or download page; and

b. Available to the Consumer at or before the time the Personal Data is Processed for the Opt-Out Purposes.

C. An Authorized Agent may exercise a Consumer's opt-out right, so long as the Authorized Agent's request permits the Controller to Authenticate the identity of the Consumer and the Authorized Agent's authority to act on the Consumer's behalf.

Rule 4.04 RIGHT OF ACCESS

A. A Controller shall comply with an access request by providing the Consumer all the specific pieces of Personal Data it has collected and maintains about the Consumer, including without limitation, any Personal Data that the Controller's Processors obtained in providing services to the Controller.

B. Personal Data provided in response to an access request must be:

1. Understandable to the Controller's target audiences, considering vulnerabilities or unique characteristics of the audience and paying particular attention to vulnerabilities of Children.

2. Provided in the language in which the Consumer interacts with the Controller.

3. Provided in a form that would allow the average Consumer to make an informed decision of whether to exercise deletion, correction, or opt-out rights.

a. For instance, the Personal Data must be provided in a form that is concise, transparent and easily intelligible, and avoids incomprehensible or unexplained internal codes and identifiers.

b. Nothing herein shall prevent a Controller from complying fully with a Consumer's data portability request pursuant to C.R.S. § 6-1-1306(1)(e).

C. A Controller shall not be required to disclose in response to an access request a Consumer's government-issued identification number, financial account number, health insurance or medical identification number, an account password, security questions and answers, or Biometric Data. The Controller shall, however, inform the Consumer with sufficient particularity that it has collected that type of information. For example, a Controller shall respond that it collects "unique Biometric Data including a fingerprint scan" without disclosing the actual fingerprint scan data.

Rule 4.05 RIGHT TO CORRECTION

A. A Controller shall comply with a Consumer's correction request by correcting the Consumer's Personal Data across all data flows and repositories and implementing measures to ensure that the Personal Data remains corrected. The Controller shall also instruct all Processors that maintain the Personal Data at issue to make the necessary corrections in their respective systems and to ensure that the Personal Data remains corrected.

B. If a Consumer submits a request to exercise their right to correct Personal Data and the requested correction to that Personal Data could be made by the Consumer through the Consumer's account settings, a Controller may respond to the **Consumer's request by** providing instructions on how the Consumer may correct the Personal Data so long as:

1. The correction process is not unduly burdensome to the Consumer;

2. The instructions meet all requirements of 4 CCR 904-3, Rule 3.01;

3. The Controller's response is compliant with the timing requirements set forth in C.R.S. § 6-1-1306(2)(a); and

4. The process described in the instructions enable the Consumer to make the specific requested correction.

C. A Controller may decide not to act upon a Consumer's correction request if the Controller determines that the contested Personal Data is more likely than not accurate based on the totality of the circumstances.

1. A Controller may require the Consumer to provide documentation if necessary to determine whether the Personal Data, or the Consumer's requested correction to the Personal Data, is accurate. When requesting documentation, the Controller must provide the Consumer with a meaningful understanding of why the documentation is necessary.

2. Any documentation provided by the Consumer in connection with the Consumer's right to correction shall only be Processed by the Controller in considering the accuracy of the Consumer's Personal Data.

3. The Controller shall implement and maintain reasonable data security measures, consistent with 4 CCR 904-3, Rule 6.09, in Processing any documentation relating to the Consumer's correction request.

4. If the Controller did not receive the Personal Data directly from the Consumer and has no documentation to support the accuracy of the Personal Data, the Consumer's assertion of inaccuracy shall be sufficient to establish that the Personal Data is inaccurate.

Rule 4.06 RIGHT TO DELETION

A. A Controller shall comply with a Consumer's deletion request by:

1. Permanently and completely erasing the Personal Data from its existing systems, except archive or backup systems, or De-Identifying the Personal Data in accordance with C.R.S. § 6-1-1303(11); and

2. Notifying the Controller's Processors and Affiliates to delete the Consumer's Personal Data obtained from the Controller.

B. Notwithstanding 4 CCR 904-3, Rule 4.06(A), a Controller may maintain records of a Consumer's deletion request consistent with 4 CCR 904-3, Rule 6.11 and as needed to effectuate the deletion request.

C. If a Controller or Processor stores any Personal Data on archived or backup systems, it may delay compliance with the Consumer's deletion request with respect to an archived or backup system until that system is restored to an active system or is next accessed or used for a Sale, disclosure, or commercial purpose.

D. If a Consumer submits a deletion request with respect to Personal Data that falls within an exception under C.R.S. § 6-1-1304, the Controller shall delete the Consumer's Personal Data that is not subject to the exception; provide the Consumer with a list of Personal Data that was not deleted along with the applicable exception; and not use the Consumer's Personal Data retained for any other purpose than provided for by the applicable exception.

E. A Controller that has obtained Personal Data about a Consumer from a source other than the Consumer shall comply with a Consumer's deletion request with respect to that Personal Data pursuant to C.R.S. § 6-1-1306(d) by (i) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the Consumer's Personal Data remains deleted from the Consumer's records and not using such retained data for any other purpose, or (ii) opting the Consumer out of the Processing of such Personal Data for any purpose except for those exempted pursuant to the provisions of C.R.S. § 6-1-1304.

Rule 4.07 RIGHT TO DATA PORTABILITY

A. To comply with a data portability request, a Controller must transfer to a Consumer the Personal Data it has collected and maintains about the Consumer through a secure method in a commonly used electronic format that enables the Consumer to have complete access to and full enjoyment of the Personal Data, including, but not limited to, the capacity to save, edit, and transfer the Personal Data to any other person or platform at Consumer's discretion.

B. Pursuant to C.R.S. § 6-1-1306(1)(e), a Controller is not required to provide Personal Data to a Consumer in a manner that would disclose the Controller's trade secrets.

1. Notwithstanding 4 CCR 904-3, Rule 4.07(B), Personal Data or Sensitive Data Inferences created using a trade secret algorithm or other mechanism must be disclosed to comply with a data portability request without disclosing the algorithm or mechanism itself.

Rule 4.08 AUTHENTICATION

A. A Controller shall establish reasonable methods to Authenticate the Consumer submitting a Data Right request and to Authenticate the authority of an Authorized Agent submitting an opt-out request on behalf of a Consumer. To determine if a method is reasonable, the Controller shall consider the Data Rights exercised, the type, sensitivity, value, and volume of Personal Data involved, and the level of possible harm that improper access or use could cause to the Consumer submitting the Data Right request. A Controller should avoid methods that place an unreasonable burden on the Consumer or Authorized Agent submitting a Data Right request.

B. When possible, a Controller shall avoid requesting additional Personal Data to Authenticate a Consumer unless the Controller cannot Authenticate the Consumer from the Personal Data already maintained by the Controller.

C. Personal Data obtained to Authenticate a Consumer may only be used to Authenticate the Consumer submitting the Data Right request or to Authenticate an Authorized Agent's authority, and must be deleted as soon as practical after Processing the Consumer's request, except as required by 4 CCR 904-3, Rule 6.11.

D. A Controller shall implement reasonable security measures, consistent with 4 CCR 904-3, Rule 6.90, to protect Personal Data exchanged to Authenticate a Consumer or to Authenticate an Authorized Agent's authority, considering the type, value, sensitivity, and volume of information exchanged and the level of possible harm improper access or use could cause to the Consumer submitting a Data Right request.

E. A Controller shall not require the Consumer or Authorized Agent to pay a fee for authentication. For example, a Controller may not require a Consumer to provide a notarized affidavit for authentication unless the Controller compensates the Consumer for the cost of notarization.

F. If a Controller cannot Authenticate the Consumer submitting a Data Right request using commercially reasonable efforts, the Controller is not required to comply with the Consumer's request. The Controller shall inform the Consumer that their identity could not be authenticated and may request additional Personal Data if reasonably necessary to Authenticate the Consumer.

Rule 4.09 RESPONDING TO CONSUMER REQUESTS

A. A Controller must respond to a Consumer's Data Right request in compliance with the timing provisions of C.R.S. § 6-1-1306(2)(a)-(b).

B. If a Controller decides not to act on a Consumer's Data Right request, the Controller's response to the Consumer must include the basis for the Controller's decision, including but not limited to (1) any conflict with federal or state law; (2) the relevant exception to the Colorado Privacy Act; (3) the Controller's inability to Authenticate the Consumer's identity; (4) any factual basis for a Controller's good-faith claim that compliance is impossible; or (5) any good-faith, documented belief that the request is fraudulent or abusive.

1. If a Controller has a good-faith claim that complying with the Consumer's request would be impossible, the Controller must explain in its response, in detail, why compliance is impossible.

2. If a Controller has a good-faith, documented belief that a request is fraudulent or abusive, the Controller must explain in its response why it believes the request is fraudulent or abusive.

3. If a Controller denies a Consumer Data Right request based on inability to Authenticate, the Controller must describe in documentation required by 4 C.C.R. 904-3, Rule 6.11 their reasonable efforts to authenticate and why they were unable to do so.

4. A Controller that decides not to act on a Consumer's request must also provide instructions on how to appeal the Controller's decision in accordance with C.R.S. § 6-11306(3).

C. When a Controller complies with a Consumer's Personal Data Right request, the Controller shall also notify all Processors that Process the Consumer's Personal Data of the Consumer's request and the Controller's response.

D. Controllers must maintain all documentation as required by 4 CCR 904-3, Rule 6.11 of these rules.

PART 5 UNIVERSAL OPT-OUT MECHANISM

Rule 5.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in Part 5 is C.R.S. §§ 6-1-108(1), 6-1-1306, and 6-1-1313. The purpose of this rule is to provide technical and other specifications for Universal Opt-Out Mechanisms.

Rule 5.02 RIGHTS EXERCISED

A. Consumers may exercise their right to opt out of the Processing of Personal Data concerning the Consumer for purposes of Targeted Advertising or the Sale of Personal Data through a user-selected Universal Opt-Out Mechanism that meets the technical and other specifications provided in this Rule.

B. The purpose of a Universal Opt-Out Mechanism is to provide Consumers with a simple and easy-to-use method by which Consumers can automatically exercise their opt-out rights with all Controllers they interact with without having to make individualized requests with each Controller.

C. A Universal Opt-Out Mechanism may express a Consumer's choice to opt out of the Processing of Personal Data for all purposes subject to the opt-out right or it may express a Consumer's choice to opt out of the Processing of Personal Data for one specific purpose only. A Universal Opt-Out Mechanism may offer "all purposes" or "specific purposes" options, or both.

Rule 5.03 NOTICE AND CHOICE

A. The platform, developer, or provider that provides a Universal Opt-Out Mechanism shall make clear to the Consumer, whether in its configuration or disclosures to the public, that the mechanism is meant to have the effect of opting the Consumer out of the Processing of Personal Data for specific purposes or all purposes. These notices provided to the Consumer:

1. Shall comply with the requirements for disclosures and communications to Consumers provided in 4 CCR 904-3, Rule 3.01;

2. If applicable, shall state that the Universal Opt-Out Mechanism has been recognized by the Colorado Attorney General;

3. Shall clearly describe the mechanism's limitations, including, for example:

   a. Whether the mechanism will have the effect of opting the Consumer out of the Processing of Personal Data for only one specific Processing purpose; or

   b. Whether the mechanism is unable to opt the Consumer out of Processing through mobile or other applications.

4. Shall not use Dark Patterns as defined in C.R.S. § 6-1-1303(9) and prohibited by 4 CCR 904-3, Rule 7.09; and

5. Need not be tailored only to Colorado or refer to Colorado.

B. A valid Universal Opt-Out Mechanism must represent the Consumer's affirmative, freely given, and unambiguous choice to opt out of the Processing of Personal Data for the purposes listed at C.R.S. § 6-1-1306(1)(a)(IV)(A) and (B).

Rule 5.04 DEFAULT SETTINGS

A. To comply with C.R.S. § 6-1-1313(2), a Universal Opt-Out Mechanism may not be the default setting for a tool that comes pre-installed with a device, such as a browser or operating system.

1. Example: An operating system manufacturer bundles a browser pre-installed with every device shipped with the operating system. The browser sends a Universal Opt-Out mechanism signal by default and never asks the Consumer to enable this setting. The Consumer's decision to use this browser does not represent the Consumer's affirmative, freely given, and unambiguous choice to use the Universal Opt-Out Mechanism because it is a default choice. This is so even if the marketing for the operating system touts its privacy protective features.

2. Example: An operating system manufacturer bundles a browser and apps pre-installed with every device shipped with the operating system. The first time a Consumer runs a browser or app, the operating system asks the Consumer specifically and clearly whether they want to send a Universal Opt-Out Mechanism signal when using the browser or app. No choice is pre-selected, meaning the Consumer is forced to decide. The Consumer's decision to say "yes" and enable the signal represents the Consumer's affirmative, freely given, and unambiguous choice to use the Universal Opt-Out Mechanism.

B. Notwithstanding 4 CCR 904-3, Rule 5.04(A), a Consumer's decision to adopt a tool that does not come pre-installed with a device, such as a browser or operation system, but is marketed prominently as a privacy-protective tool or specifically as a tool designed to exercise a user's rights to opt out of the Processing of Personal Data shall be considered the Consumer's affirmative, freely given, and unambiguous choice to use a Universal Opt-Out Mechanism.

1. Example: A browser manufacturer markets its browser as a "privacy friendly" browser, highlighting that the browser sends a Universal Opt-Out Mechanism signal by default. The browser does not come pre-installed with a device or operating system and must be installed by the Consumer. The Consumer's decision to use this browser represents the Consumer's affirmative, freely given, and unambiguous choice to use the Universal Opt-Out Mechanism. The Consumer need not be given an explicit choice about whether to use the Universal Opt-Out Mechanism in this example.

Rule 5.05 PERSONAL DATA USE LIMITATIONS

A. A platform, developer, or provider providing a Universal Opt-Out Mechanism shall not use, disclose, or retain any Personal Data collected from the Consumer in connection with the Consumer's utilization of the mechanism for any purpose other than sending or Processing the opt-out preference.

B. When Processing a Universal Opt-Out Mechanism, a Controller may not require the collection of additional Personal Data beyond that which is strictly necessary to confirm a Consumer is a resident of Colorado or determine that the mechanism represents a legitimate request to opt out of the Processing of Personal Data as permitted by C.R.S. § 6-1-1306(1)(a)(IV).

C. Notwithstanding 4 CCR 904-3, Rule 5.05(B), a Controller may provide the Consumer with an option to provide additional Personal Data only if it will extend the recognition of the Consumer's use of the Universal Opt-Out Mechanism across platforms, devices, or offline. For example, a Controller may give the Consumer the option to provide their phone number or email address so that the Universal Opt-Out Mechanism or signal can apply to offline Sale of Personal Data or link the Consumer's opt-out choice across devices. Any information provided by the Consumer for this purpose shall not be used, disclosed, or retained for any purpose other than processing the opt-out request.

Rule 5.06 TECHNICAL SPECIFICATION

A. A Universal Opt-Out Mechanism must allow for Consumers to automatically communicate their opt-out choice with multiple Controllers.

1. The Universal Opt-Out Mechanism may communicate a Consumer's opt-out choice by sending an opt-out signal. The signal must be in a format commonly used and recognized by Controllers. An example would be an HTTP header field or JavaScript object.

2. The Universal Opt-Out Mechanism may operate through a means other than by sending an opt-out signal, for example by maintaining a "do not sell" list, so long as Controllers are able to query such a list in an automated manner.

B. The Universal Opt-Out Mechanism must allow Consumers to clearly communicate one or more opt-out rights available under C.R.S. § 6-1-1306(1)(a)(IV).

1. The Universal Opt-Out Mechanism may allow for a Consumer to opt out of Processing for one or more of the Opt-Out Purposes.

2. The Universal Opt-Out Mechanism may allow a Consumer to opt out of one or more Controllers that recognize the mechanism, to opt out of one or more domain, or to opt out of Processing by all Controllers that recognize the mechanism.

C. The Universal Opt-Out Mechanism must store, process, and transmit any Consumer Personal Data using reasonable data security measures, consistent with 4 CCR 904-3, Rule 6.09.

D. A Universal Opt-Out Mechanism must not prevent the Controller's ability to determine:

1. Whether a Consumer is a Resident of the State of Colorado; or

2. That the Universal Opt-Out Mechanism represents a legitimate request to opt out of the Processing of Personal Data.

E. A Universal Opt-Out Mechanism must not unfairly disadvantage any Controller. For example, a Universal Opt-Out Mechanism may not treat different Controllers differently or engage in self-dealing benefiting the creator of the Universal Opt-Out Mechanism over other Controllers.

Rule 5.07 SYSTEM FOR RECOGNIZING UNIVERSAL OPT-OUT MECHANISMS

A. The Colorado Department of Law shall maintain a public list of Universal Opt-Out Mechanisms that have been recognized to meet the standards of this subsection. The initial list shall be released no later than April 1, 2024 and shall be updated periodically.

B. The goal of the public list is to simplify the options facing Controllers, Consumers, and other actors.

C. To be recognized, a Universal Opt-Out Mechanism must at a minimum meet these standards:

1. Comply with all of the technical and other specifications of this section;

2. Be an open system or standard, which is free for adoption by device, operating system, browser, and other manufacturers, Controllers, or Consumers without permission or on fair, reasonable, and non-discriminatory terms; and

3. Not create Consumer or Controller confusion about the similarities and differences between Universal Opt-Out Mechanisms on the public list.

D. The Colorado Department of Law may consider additional factors when determining which Universal Opt-Out Mechanisms to recognize. These include but are not limited to:

1. Commercial adoption by Consumers or Controllers;

2. Ease of use, implementation, and detection by Consumers and Controllers;

3. Whether the Universal Opt-Out Mechanism has been approved by a widely recognized, legitimate standards body after broad multistakeholder participation in the standards-making process.

Rule 5.08 OBLIGATIONS ON CONTROLLERS

A. Effective July 1, 2024,

1. A Controller that receives an opt-out request through a Universal Opt-Out Mechanism shall treat such as a valid request to opt out of the Processing of Personal Data for purposes of Targeted Advertising, Sale of Personal Data, or both, as indicated by the mechanism, for the associated browser or device, and, if known, for the Consumer.

2. After receiving a valid opt-out request through the use of a Universal Opt-Out Mechanism, a Controller shall continue to treat the browser, device, and Consumer as having exercised opt-out rights until the browser, device, or Consumer overrides the opt-out, as specified in 4 CCR 904-3, Rule 5.10.

B. A Controller shall be capable of recognizing any Universal Opt-Out Mechanism recognized under subsection 4 CCR § 904-3, Rule 5.07. For example, in the case of a recognized Universal Opt-Out Mechanism sent as a signal, the Controller must listen for the signal. In the case of a recognized Universal Opt-Out Mechanism utilizing a "do not sell" list, the Controller must query the "do not sell" list.

C. A Controller may also recognize Universal Opt-Out Mechanisms that are not recognized under subsection 4 CCR § 904-3, Rule 5.07.

D. Unless a Controller is Authenticating a Consumer as permitted by C.R.S. § 6-1-1313(2)(f), a Controller may not require a Consumer to login or otherwise Authenticate themself as a condition of recognizing the Consumer's use of the Universal Opt-Out Mechanism.

E. A Controller may display in a conspicuous manner if it has Processed the Consumer's opt-out preference signal. For example, the Controller may display on its website "Opt-Out Preference Signal Honored" when a browser, device, or Consumer utilizing a Universal Opt-Out Mechanism visits the website.

Rule 5.09 CONSENT AFTER UNIVERSAL OPT-OUT

A. A Controller may enable a Consumer to Consent to Processing that the Consumer has opted-out of using a Universal Opt-Out mechanism, so long as the Controller's request for Consent complies with the Consent requirements provided in 4 CCR 904-3, Rule 7.05.

B. A Controller shall not interpret the absence of a Universal Opt-Out Mechanism signal after the Consumer previously utilized a Universal Opt-Out Mechanism as Consent to opt back in.

PART 6 DUTIES OF CONTROLLERS

Rule 6.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in this Part 6 is C.R.S. §§ 6-1-108(1), 6-1-1308, and 6-1-The purpose of the rules in this Part 6 is to provide clarity on the duties of Controllers concerning the Personal Data of Colorado Consumers.

Rule 6.02 PRIVACY NOTICE PRINCIPLES

A. A privacy notice shall provide Consumers with a meaningful understanding and accurate expectations of how their Personal Data will be Processed. It shall also inform Consumers about their rights under the Colorado Privacy Act and provide any information necessary for Consumers to exercise those rights.

B. A Controller is not required to provide a separate Colorado-specific privacy notice or section of a privacy notice as long as the Controller's privacy notice contains all information required in this section and makes clear that Colorado Consumers are entitled to the rights provided by C.R.S. § 6-1-1306.

C. A privacy notice shall comply with all requirements for disclosures and communications to Consumers provided in 4 CCR 904-3, Rule 3.01.

D. A privacy notice must be clear. Information contained in a privacy notice shall be:

1. Concrete and definitive, avoiding abstract or ambivalent terms that may lead to varying interpretations.

2. Clearly labeled, such that Consumers seeking to understand a Controller's Processing activities or how to exercise their Data Rights can easily access the section of the privacy notice containing relevant information.

E. A privacy notice must be easily accessible. A privacy notice must be:

1. Posted online through a conspicuous link using the word "privacy" on the Controller's website homepage or on a mobile application's app store page or download page. A Controller that maintains an application on a mobile or other device shall also include a link to the privacy notice in the application's settings menu.

2. A Controller that does not operate a website shall make the privacy notice conspicuously available to Consumers through a medium regularly used by the Controller to interact with Consumers. For instance, if a Controller interacts with a Consumer offline, an offline version of the privacy notice must be available to the Consumer.

F. A privacy notice must be specific. The level of specificity in a privacy notice should enable a Consumer to understand, in advance or at the time of the Processing, the scope of the Controller's Processing operations, such that a Consumer should not be taken by surprise at a later point about Personal Data that has been collected and the ways in which Personal Data has been Processed.

Rule 6.03 PRIVACY NOTICE CONTENT

A. A privacy notice must include the following information:

1. A comprehensive description of the Controller's online and offline Personal Data Processing practices, including the following information for each Processing purpose:

    a. The Processing purpose described in a level of detail that gives Consumers a meaningful understanding of how their Personal Data is used and why their Personal Data is reasonably necessary for the Processing purpose.

    b. If the Processing purpose includes Targeted Advertising or Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer, the Controller shall list that activity as part of the Processing purpose.

    c. The categories of Personal Data Processed for each of the Controller's Processing purposes, including, but not limited to, whether Sensitive Data or the Personal Data of a Child is Processed. Categories shall be described in a level of detail that provides Consumers a meaningful understanding of the type of Personal Data Processed.

    d. For example, categories of Personal Data described at a sufficiently granular level of detail include, but are not limited to: "real name," "contact information," "government issued identification numbers," "payment information", "Information from Cookies," "data revealing religious affiliation," and "medical data."

    e. Categories of Personal Data that the Controller Sells to or shares with Third Parties, if any, for each Processing purpose.

        Categories of Third Parties to whom the Controller sells, or with whom the Controller shares Personal Data, if any, for each Processing purpose. Categories of Third Parties must be described in a level of detail that gives Consumers a meaningful understanding of what type of entity the Third Party is, and to the extent possible, how the Third Party may Process Personal Data.

        For example, categories of Third Parties described in a sufficiently granular level of detail include, but are not limited to: "analytics companies," "data brokers," "third-party advertisers," "payment processors," "lenders," "other merchants," and "government agencies." For each processing purpose, whether the Personal Data collected is Sold or processed for Targeted Advertising.

2. If a Controller's Processing activity involves the Processing of Personal Data for the purpose of Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer, all disclosures required by 4 CCR 904-3, Rule 9.03.

3. A list of the Data Rights available.

4. A description of the methods through which a Consumer may submit requests to exercise Data Rights, as required by C.R.S. § 6-1-1306(1) and 4 CCR 904-3, Rule 4.02, including:

    a. Instructions on how to use each method.

    b. Instructions on how an Authorized Agent may submit a request to opt out of the Processing of Consumer Personal Data on a Consumer's behalf pursuant to C.R.S. § 6-1-1306(1)(a)(II).

c. A clear and conspicuous method to exercise the right to opt out of the Processing of Personal Data concerning the Consumer pursuant to C.R.S. § 6-1-1306(1)(a)(I), or links to any online method, such as a webform or portal, consistent with 4 CCR 904-3, Rule 4.03.

d. A description of the process the Controller uses to Authenticate the identity of a Consumer exercising a Data Right request or to Authenticate the authority of an Authorized Agent exercising the right to opt out on a Consumer's behalf.

e. Effective July 1, 2024, an explanation of how requests to opt out using Universal Opt-Out Mechanisms will be processed.

5. If a Controller will delete Sensitive Data Inferences within twelve (12) hours pursuant to 4 CCR 904-3, Rule 6.10, a description of the Sensitive Data Inferences subject to this provision and the retention and deletion timeline for such Sensitive Data Inferences.

6. A Controller's contact information.

7. Instructions on how a Consumer may appeal a Controller's action in response to the Consumer's request, as contemplated by C.R.S. § 6-1-1306(3).

8. The date the privacy notice was last updated.

Rule 6.04 CHANGES TO A PRIVACY NOTICE

A. A Controller shall notify Consumers of substantive or material changes to a privacy notice, including, but not limited to, changes to: (1) categories of Personal Data Processed; (2) Processing purposes; (3) a Controller's identity; or (4) methods by which Consumers can exercise their Data Rights request. Changes to a privacy notice shall be communicated to Consumers in a manner by which the Controller regularly interacts with Consumers.

B. Notice of a substantive or material change to a privacy notice must be made 15 calendar days before the change goes into effect.

C. A Controller must obtain Consent from a Consumer pursuant to 4 CCR 904-3, Rules 7.02-7.05 before Processing Personal Data for a secondary use, even if the new purpose is disclosed in the privacy notice.

Rule 6.05 LOYALTY PROGRAMS

A. While a Controller may not increase the cost of or decrease the availability of a product or service based solely on a Consumer's exercise of a Data Right, a Controller is not prohibited from offering Bona Fide Loyalty Program Benefits to a Consumer based on the Consumer's voluntary participation in that Bona Fide Loyalty Program.

B. If a Consumer exercises their right to delete Personal Data such that it is impossible for the Controller to provide a certain Bona Fide Loyalty Program Benefit to the Consumer, the Controller is no longer obligated to provide that Bona Fide Loyalty Benefit to the Consumer. However, the Controller shall provide any available Bona Fide Loyalty Program Benefit for which the deleted Personal Data is not necessary.

C. If a Consumer refuses to Consent to the Processing of Sensitive Data necessary for a personalized Bona Fide Loyalty Program Benefit, the Controller is no longer obligated to provide that personalized Bona Fide Loyalty Program Benefit. However, the Controller shall provide any available, non-personalized Bona Fide Loyalty Program Benefit for which the Sensitive Data is not necessary. A Controller may not condition a Consumer's participation in a Bona Fide Loyalty Program on the Consumer's Consent to Process Sensitive Data unless the Sensitive Data is required for all Bona Fide Loyalty Program Benefits.

D. If a Consumer's decision to exercise a Data Right impacts the Consumer's membership in a Bona Fide Loyalty Program, the Controller shall notify the Consumer of the impact of the Consumer's decision in conformance with 4 CCR 904-3, Rule 3.01 and at least twenty-four (24) hours before discontinuing the Consumer's Bona Fide Loyalty Program Benefit or membership, and must provide a reference or link to the information required by subparagraph E., below.

E. Loyalty Program Disclosures

1. In addition to all other disclosures required by 4 CCR 904-3, Rules 6.03 and 7.03, a Controller maintaining a Bona Fide Loyalty Program must provide the following disclosures as required by 4 CCR 904-3, Rule 6.05(E), as well as in its privacy notice, Bona Fide Loyalty Program terms, and Consent disclosures in requests for Consent to Process Sensitive Data or Personal Data in connection with the Bona Fide Loyalty Program:

    a. The categories of Personal Data or Sensitive Data collected through the Bona Fide Loyalty Program that will be Sold or Processed for Targeted Advertising, if any;

    b. Categories of Third Parties that will receive the Consumer's Personal Data and Sensitive Data, including whether Personal Data will be provided to Data Brokers;

    c. The value of the Bona Fide Loyalty Program Benefits available to the Consumer if the Consumer opts out of the Sale of Personal Data or Processing of Personal Data for Targeted Advertising, and the value of the Bona Fide Loyalty Program Benefits available to the Consumer if the Consumer does not opt out of the Sale of Personal Data or Processing for Targeted Advertising; and

    d. A list of any Bona Fide Loyalty Program Benefits that require the Processing of Personal Data for Sale or Targeted Advertising, and the Third Party receiving the Personal Data and providing each such Bona Fide Loyalty Program Benefit, if applicable.

2. Bona Fide Loyalty Program terms and requests for Consent to Process Sensitive Data or Personal Data in connection with the Bona Fide Loyalty Program shall also include a link to the Controller's privacy notice.

F. Example: A Consumer joins a pharmacy's Bona Fide Loyalty Program that includes both personalized and non-personalized Bona Fide Loyalty Program Benefits. The pharmacy asks the Consumer for Consent to collect Sensitive Data about the Consumer's prescriptions and medical conditions in order to provide personalized Bona Fide Loyalty Program Benefits. When the Consumer refuses Consent, the Controller gives timely notice to the Consumer that it will not provide the personalized Bona Fide Loyalty Program Benefits, but will continue to provide non-personalized Bona Fide Loyalty Program Benefits. Moving forward, the Controller provides only the non-personalized Bona Fide Loyalty Program Benefits following the Consumer's decision to continue to refuse Consent to the collection of Sensitive Data. The Controller is not acting impermissibly because the pharmacy is still providing all available non-

personalized Bona Fide Loyalty Program Benefits and did not condition the Consumer's participation in the Bona Fide Loyalty Program on the Consumers Consent to process Sensitive Data that is not required for personalized Bona Fide Loyalty Program Benefits.

Rule 6.06 PURPOSE SPECIFICATION

A. Controllers shall specify the express purposes for which Personal Data are collected and Processed in both external disclosures to Consumers as well as in any internal documentation required by this Part 6.

B. The express purpose must be described in a sufficiently unambiguous, specific, and clear manner, such that the way Personal Data will be Processed is understood by and predictable to the average Consumer, the Controller, Third Parties, and enforcement authorities.

1. Particular care should be taken to ensure that any specification of the purpose is sufficiently clear to all involved, irrespective of their different cultural or linguistic backgrounds, level of understanding, or special needs.

2. The express purpose must be detailed enough to enable the implementation of necessary data security safeguards and allow for compliance with the law to be assessed.

C. If Personal Data is collected and Processed for more than one purpose, Controllers should specify each unrelated purpose with enough detail to allow Consumers to understand each individual, unrelated purpose.

1. Controllers should avoid identifying one broad purpose to justify numerous Processing activities that are only remotely related.

2. Controllers should avoid specifying one broad purpose to cover potential future Processing activities that are only remotely related.

D. If the Processing purpose has evolved beyond the original express purpose, the Controller must review and update all related disclosures and documentation as necessary.

Rule 6.07 DATA MINIMIZATION

A. To ensure all Personal Data collected is reasonably necessary for the specified purpose, Controllers shall carefully consider each Processing purpose and determine the minimum Personal Data that is necessary, adequate, or relevant for the express purpose or purposes. Such assessment shall be documented according to 4 CCR 904-3, Rule 6.11.

B. Personal Data should only be kept in a form which allows identification of Consumers for as long as is necessary for the express Processing purpose(s). To ensure that the Personal Data are not kept longer than necessary, adequate, or relevant, Controllers shall set specific time limits for erasure or to conduct a periodic review.

1. Any Personal Data determined to no longer be necessary, adequate, or relevant to the express Processing purpose(s) shall be deleted by the Controller and any Processors.

2. Biometric Identifiers or any Personal Data generated from a digital or physical photograph or an audio or video recording held by a Controller shall be reviewed at least once a year to determine

if its storage is still necessary, adequate, or relevant to the express Processing purpose. Controllers must obtain Consent to Process Biometric Identifiers or any Personal Data generated from a digital or physical photograph or an audio or video recording each year after the first year that it is stored.

C. A Controller shall not collect Personal Data other than those disclosed in its required privacy notice. If the Controller intends to collect additional Personal Data the Controller shall revise its privacy notice, and notify Consumers of the change to its privacy notice pursuant to 4 CCR 904-3, Rule 6.04.

Rule 6.08 SECONDARY USE

A. The specified Processing purpose is the purpose disclosed to Consumers before the time the Personal Data is collected from Consumers. Such disclosure shall be included in any required privacy notice or Consent disclosure.

B. Before Processing Personal Data for purposes that are not reasonably necessary to or compatible with specified Processing purpose(s), the Controller must obtain Consent pursuant to C.R.S. § 6-1-1308 and 4 CCR 904-3, Rules 7.02-7.05.

C. If a new Processing purpose is unexpected, unnecessary, unconnected, or would have an unjustified negative impact on the Consumer, the new purpose is not likely to be considered reasonably necessary to or compatible with the original specified purpose. When considering if the new Processing purpose is reasonably necessary to **or** compatible with the original specified purpose, Controllers should consider the following, as applicable:

1. The reasonable expectation of an average Consumer concerning how their Personal Data would be Processed once it was collected;

2. The link between the original specified purpose(s) for which the data was collected and the purpose(s) of further Processing;

3. The relationship between the Consumer and the Controller and the context in which the Personal Data was collected;

4. The type, nature, and amount of the Personal Data subject to the new Processing purpose;

5. The possible consequence or impact to the Consumer of the new Processing purpose;

6. The identity of the entity conducting the new Processing purposes, e.g., the same or different Controller, an Affiliate, a Processor, or a Third Party; and

7. The existence of additional safeguards for the Personal Data, such as encryption or pseudonymization.

D. An assessment of the reasonable necessity or compatibility of any new Processing purpose shall be documented consistent with 4 CCR 904-3, Rule 6.11.

Rule 6.09 DUTY OF CARE

A. Personal Data must be Processed in a manner that ensures appropriate security and confidentiality of the Personal Data, including protection against unauthorized or unlawful access to or use of Personal Data and the equipment used for the Processing and against accidental loss, destruction, or damage, using reasonable technical or organizational measures.

B. Reasonable measures to secure Personal Data include but are not limited to those provided by C.R.S. § 6-1-713.5 and C.R.S. § 24-73-102.

Rule 6.10 DUTY REGARDING SENSITIVE DATA

A. Controllers must obtain Consent to Process Sensitive Data, including Sensitive Data Inferences, consistent with C.R.S. § 6-1-1308(7) and 4 CCR 904-3, Rules 7.02-7.05.

B. Controllers may Process Sensitive Data Inferences from Consumers over the age of thirteen (13) without Consent only if:

1. The Processing purpose of such Personal Data would be obvious to a reasonable Consumer based on the context of the collection and use of the Personal Data, and the relationship between the Controller and Consumer.

2. The Personal Data and any Sensitive Data Inferences are permanently deleted within twelve (12) hours of collection or of the completion of the Processing activity, whichever comes first;

3. The Personal Data and any Sensitive Data Inferences are not transferred, sold, or shared with any Processors, Affiliates, or Third-Parties; and

4. The Personal Data and any Sensitive Data Inferences are not Processed for any purpose other than the express purpose disclosed to the Consumer.

C. If a Controller will delete Sensitive Data Inferences within twelve (12) hours, pursuant to this section, they must (1) include description of the Sensitive Data Inferences subject to this provision and the retention and deletion timeline for such Sensitive Data Inferences in its privacy notice, pursuant to 4 CCR 904-3, Rule 6.03, and (2) include the details of the deletion and verification process in the Controller's Data Protection Assessment, pursuant to 4 CCR 904-3, Rule 8.04.

Rule 6.11 DOCUMENTATION CONCERNING DUTIES OF CONTROLLERS

A. Controllers shall maintain records of all Consumer Data Rights requests made pursuant to C.R.S. 6-1-1306 for at least twenty-four (24) months. Such records shall include, at a minimum, each of the following:

1. The date of request;

2. The Consumer Data Rights request type;

3. The date of the Controller's response;

4. The nature of the Controller's response;

5. The basis for the denial of the request if the request is denied in whole or in part; and

6. The existence and resolution of any Consumer appeal to a denied request.

B. Controllers shall maintain a record of all Data Rights requests made pursuant to C.R.S. § 6-11306 with which the Controller has previously complied. Such records shall be made available at the completion of a merger, acquisition, bankruptcy, or other transaction in which a Third Party assumes control of Personal Data to ensure any new Controller continues to recognize the Consumer's previously exercised Data Rights.

C. Controllers shall maintain a record of any analysis of compliance with 4 CCR 904-3, Rules 6.07, 6.08, and 7.06 for as long as the Processing activity continues, and for at least three (3) years after the conclusion of Processing activity.

D. Required records shall be maintained in a readable format, appropriate to the sophistication and size of the Controller's business.

E. The Controller shall implement and maintain reasonable security procedures and practices, consistent with 4 CCR 904-3, Rule 6.09, in maintaining all required records.

F. Personal Data maintained pursuant to this 4 CCR 904-3, Rule 6.11, where that information is not used for any other purpose, shall not be subject to Data Rights requests.

G. Personal Data maintained for required documentation shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the Colorado Privacy Act, § 6-1-1301, *et seq*., and these rules. Personal Data maintained for required documentation shall not be shared with any Third Party except as necessary to comply with a legal obligation or as part of a merger, acquisition, bankruptcy, or other transaction in which a Third Party assumes control of Personal Data.

H. Other than as required by this subsection and 4 CCR 904-3, Rule 4.06, a Controller is not required to retain Personal Data solely for the purpose of fulfilling a Data Rights request made under the Colorado Privacy Act, § 6-1-1301, *et seq*.

PART 7 CONSENT

Rule 7.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in this Part 7 is C.R.S. §§ 6-1-108(1), 6-1-1303(5), 6-1-1306, 6-1-1308 and 6-1-1313. The purpose of these rules in this Part 7 is to provide clarity on the requirements to obtain Consent, including the prohibition against obtaining agreement through the use of Dark Patterns.

Rule 7.02 REQUIRED CONSENT

A. Pursuant to C.R.S. §§ 6-1-1303(5), 6-1-1306(1)(a)(IV)(C), 6-1-1308(4), and 6-1-1308(7), a Controller must obtain valid Consumer Consent prior to:

1. Processing a Consumer's Sensitive Data;

2. Processing Personal Data concerning a known Child, in which case the Child's parent or lawful guardian must provide Consent;

3. Selling a Consumer's Personal Data, Processing a Consumer's Personal Data for Targeted Advertising, or Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer after the Consumer has exercised the right to opt out of the Processing for those purposes; and

4. Processing Personal Data for purposes that are not reasonably necessary to, or compatible with, the original specified purposes for which the Personal Data are Processed.

B. Controllers may rely upon valid consent obtained prior to July 1, 2023 to continue to Process a Consumer's previously collected Personal Data, including Sensitive Data collected before July 1, 2023. Consent obtained before July 1, 2023 shall be considered valid only if it would comply with the requirements set forth in C.R.S. §§ 6-1-1303(5), 6-1-1306(1)(a)(IV)(C), 6-1-1308(4), and 6-11308(7) and Part 7 of these rules.

1. If a Controller has collected Sensitive Data prior to July 1, 2023 and has not also previously obtained valid consent to Process such Sensitive Data, the Controller shall obtain consent as required by January 1, 2023 to continue to Process the Sensitive Data.

C. Notwithstanding the above, a Controller Processing Sensitive Data Inferences is not required to obtain Consent for the Processing activity if the processing falls within the requirements of 4 CCR 904-3, Rule 6.10.

Rule 7.03 REQUIREMENTS FOR VALID CONSENT

A. To be valid, a Consent must meet each of the following elements: (1) it must be obtained through the Consumer's clear, affirmative action; (2) it must be freely given by the Consumer; (3) it must be specific; (4) it must be informed; and (5) it must reflect the Consumer's unambiguous agreement.

B. Consent must be obtained through the Consumer's clear, affirmative action. For purposes of obtaining valid Consent:

1. A "clear, affirmative action" means a Consumer's Consent is communicated through either (a) deliberate and clear conduct, or (b) a statement that clearly indicates their acceptance of the proposed Processing of their Personal Data.

2. A blanketed acceptance of general terms and conditions, silence, inactivity or in action, pre-ticked boxes, and other negative option opt-out constructions that require intervention from the Consumer to prevent agreement are not clear affirmative actions for the purposes of valid Consent.

C. Consent must be freely given. For purposes of obtaining valid Consent:

1. Consumers may refuse Consent without detriment and withdraw Consent easily at any time.

2. Consent is not freely given when:

a. It is bundled with other terms and conditions;

b. The performance of a contract is dependent on Consent to Process Personal Data that is not necessary to provide the goods or services contemplated by the contract; or

c. The Controller denies goods, services, discounts, or promotions to a Consumer who chooses not to provide Consent, unless:

i. The Personal Data is necessary to the provision of those goods, services, discounts, or promotions, consistent with 4 CCR 904-3, Rule 6.05; or

ii. The Consent is otherwise required in connection with a Consumer's voluntary participation in a Bona Fide Loyalty Program, consistent with the requirements in 4 CCR 904-3, Rule 6.05.

3. Example: An online dating application asks users for information about their sexual orientation to provide a more targeted service. The application's terms and conditions also tell users that the application will share the collected Personal Data with similar applications for advertising purposes. Consent is required because Personal Data revealing sexual orientation is Sensitive Data. Since users cannot accept the required terms and conditions without the opportunity to separately provide or withhold Consent for sharing with similar applications, the Consent is not freely given.

D. Consent must be specific.

1. When Controllers request Consent to Process Personal Data for more than one unrelated or incompatible Processing purpose, Consumers must have the ability to separately Consent to each specific purpose.

2. Consent to Process Personal Data for one purpose does not constitute valid Consent to Process Personal Data for other purposes.

3. Consent to Sell or share Sensitive Data or Personal Data with certain parties does not constitute valid Consent to Sell or share Sensitive Data or Personal Data, when required, with other parties.

4. Example: A cosmetic retailer asks a customer for Consent to use Sensitive Data revealing the customer's racial origin in order to provide targeted offers to the customer and to share the customer's racial origin information with commercial partners. This Consent is not specific as there is no opportunity to provide separate Consent for the two separate Processing purposes. Therefore, Consent in this example would not be valid.

5. Example: In the example above, the Controller requests Consent only to share Sensitive Data revealing the customer's racial origin with commercial partners. The Controller lists "Fashion Co. #1" and "Make Up Co. #1" as commercial partners who will receive Sensitive Data. Consent would be deemed valid for only these two Third Parties because their identity was provided to the Consumer at the time that his or her Consent was collected. Consent would not be deemed valid for sharing with another Third Party whose identity has not been provided.

E. Consent must be informed.

1. A request for Consent must contain the following disclosures:

a. The Controller's identity;

b. The reason that Consent is required;

c. The Processing purpose for which Consent is sought;

d. The categories of Personal Data that the Controller shall Process to effectuate the Processing purpose;

e. Categories of all parties who will have access to the Personal Data, and names of all Third Parties and Affiliates receiving the Sensitive Data through Sale or sharing. Names of Processors, as defined in C.R.S. § 6-1-1306(19) are not required; and

f. A description of the Consumer's right to withdraw Consent for the identified Processing purpose at any time in accordance with 4 CCR 904-3, Rule 7.07 and details of how and where to do so.

g. Any disclosures required by 4 CCR 904-3, Rules 6.05 and 9.05.

F. Consent may not be obtained using Dark Patterns as defined in C.R.S § 6-1-1309(9) and prohibited by 4 CCR 904-3, Rule 7.09. Pursuant to C.R.S. § 6-1-1303(5)(c) and 4 CCR 904-3, Rule 7.09, any agreement obtained through Dark Patterns is not valid Consent.

Rule 7.04 REQUESTS FOR CONSENT

A. Controllers shall provide a simple mechanism to enable a Consumer to provide Consent when required, including Consent to Processing purposes from which the Consumer has previously opted out. Such a mechanism should be easy for a reasonable Consumer to locate and should comply with the other requirements set forth in Part 7 of these rules.

B. Requests for Consent shall be prominent, concise, and separate and distinct from other terms and conditions, and shall comply with all requirements for disclosures and communications to Consumers set forth in 4 CCR 904-3, Rule 3.01.

C. A Consent request method may provide the Consumer with a link to a webpage containing the Consent disclosures required by 4 CCR 904-3, Rule 7.03, provided the request method clearly states the title and section of the relevant disclosures. If technically feasible, the request method must also link the Consumer directly to the relevant section of the disclosure.

D. Example: A mobile application requests Consent to collect health information to provide diet and fitness advice. The Consent request provides a link to the application's privacy notice which contains the required Consent disclosures. However, the Consent request does not direct or bring the Consumer to the relevant section of the privacy notice. Consent is not valid because the Consent request does not clearly indicate the title and section where the Consumer can find the required disclosures and did not link the Consumer directly to the relevant section of the privacy notice.

E. Example: Acme Toy Store collects customer email addresses in order to send customers information about product recalls and maintains those email addresses in a recall email distribution list. Acme Toy Store wants to use the recall email distribution list to send those customers promotional materials. Acme Toy Store must obtain customer consent prior to using the recall email distribution list to provide

promotional materials because providing promotional materials is not necessary to or compatible with providing product recall information. Acme Toy Store emails the recall distribution list attaching a revised privacy notice disclosing the new promotional purposes and asks customers to Consent to the new privacy notice, but does not state the new purpose in the email, and does not direct customers to the section of the privacy notice disclosing the secondary purpose. Consent is not valid because the email did not contain the required Consent disclosures or direct the customers to a document containing the required Consent disclosures.

1. Example: Under the same circumstances, Acme Toy Store emails the recall email distribution list informing those customers that Consent is required for the Acme Toy Store to Process email addresses for a secondary purpose, explaining that the secondary purpose is to provide customers with promotional materials, providing all other required disclosures and including a mechanism that enables the customers to provide Consent and to revoke Consent through the same user interface. Consent is valid because the email contained all required Consent disclosures in an acceptable form.

2. Example: Under the same circumstances, Acme Toy Store emails the product recall email distribution list informing those customers that it would like to use their email addresses for a secondary purpose as contemplated in section B.2.e. of its privacy notice and requests the customers' Consent to do so. It then provides a link directly to section B.2.e. of its privacy notice which explains that Acme Toy Store uses customer email addresses to send information about Acme Toy Store's sales and promotions, in addition to all other disclosures. The email provides a Consent mechanism that enables the customers to provide or revoke consent through the same user interface. Consent is valid because the email and linked page together contained all required disclosures, the email provided the specific section of the relevant disclosures, and the link brought the customers directly to the relevant disclosures.

Rule 7.05 CONSENT AFTER OPT-OUT

A. The Consumer's decision to Consent to Processing activities from which the Consumer has previously opted-out using either a Universal Opt-Out Mechanism or directly with a particular Controller is subject to the requirements for Consent under 4 CCR 904-3, Rules 7.03 and 7.04.

B. If a Controller wishes to proactively obtain Consent to Process Personal Data for an Opt-Out Purpose after the Consumer has opted out of Processing for that Purpose, a Controller shall provide a link or similar mechanism on its website or application that enables the Consumer to provide Consent. The link or similar mechanism must:

1. Have a similar look, feel, and size relative to other links on the same web page or application, and not be presented through pop-up windows, pop-up banners, or other web interface displays that degrade or obstruct the Consumer's experience on the Controller's web page or application; and

2. Meet all other requirements for a valid Consent under this Part 7.

C. If a Controller conspicuously displays the status of the Consumer's opt-out choice on the website pursuant to 4 CCR 904-3, Rule 5.08(E), the link to provide Consent may appear beside or in conjunction with the Consumer's opt-out status.

D. If a Consumer has opted-out of the Processing of Personal Data for the Opt-Out Purposes, and then initiates a transaction or attempts to use a product or service inconsistent with the request to opt-out,

such as signing up for a Bona Fide Loyalty Program that also involves the Sale of Personal Data, the Controller may request the Consumer's Consent to Process the Consumer's Personal Data for that purpose, so long as the request for Consent complies with all provisions of 4 CCR 904-3, Rules 7.03 and 7.04.

E. Example: A Consumer opts out of the use of Personal Data for Sale or Targeted Advertising using a Universal Opt-Out Mechanism. The Consumer visits the website of a fashion retailer that routinely shares Consumer Personal Data for Targeted Advertising. The fashion retailer must obtain the Consumer's consent because the Consumer has already opted out of Processing for that purpose. The fashion retailer's website displays a pop-up banner seeking Consent to share the Consumer's Personal Data for Targeted Advertising. This is not a valid request for Consumer Consent because the request is made through a pop-up banner that degrades or obstructs the Consumer's experience on the Controller's web page or application.

F. Example: A Consumer opts out of the use of Personal Data for Sale or Targeted Advertising using a Universal Opt-Out Mechanism. The Consumer visits a fashion retailer's website. The fashion retailer's homepage contains a message at the top of the webpage that states "you have opted out of targeted advertising" next to a link that states "Opt-in to Data Use". The linked webpage also meets all requirements of 4 CCR 904-3, Rules 7.03 and 7.04. Consent pursuant to this request is valid.

Rule 7.06 CONSENT FOR CHILDREN

A. If a Controller operates a website or business directed to Children or has actual knowledge that it is collecting or maintaining Personal Data from a Child, the Controller shall take commercially reasonable steps to verify a Consumer's age before Processing that Consumer's Personal Data.

B. When a Controller engages in Processing activities involving the collection and Processing of Personal Data from a known Child, the Controller must obtain Consent from the parent or lawful guardian of that Child before collecting or Processing the Child's Personal Data.

C. A Controller Processing the Personal Data of a Child must make reasonable efforts to obtain verifiable parental Consent, taking into consideration available technology. Any method to obtain verifiable parental Consent must be reasonably calculated, in light of available technology, to ensure that the person providing Consent is the Child's parent.

D. Reasonably calculated methods for determining that a person Consenting to the Processing of a Child's Personal Data is the parent or lawful guardian of that Child include, but are not limited to:

1. Providing a Consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan.

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

3. Having a parent or guardian call a toll-free telephone number staffed by trained personnel.

4. Having a parent or guardian connect to trained personnel via videoconference.

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

D. Any Personal Data collected for purposes of verifying a person's age or the identity of a parent or legal guardian may not be used for any reason other than Processing these verifications.

F. Parental verification and Consent pursuant to this section must be documented as required by 4 CCR 904-3, Rule 6.11.

Rule 7.07 REFUSING OR WITHDRAWING CONSENT

A. A Consumer shall be able to refuse or revoke Consent as easily and within the same number of steps as Consent is affirmatively provided.

B. If Consent is obtained through an electronic interface, the Consumer shall be able to refuse or withdraw Consent through the same electronic interface.

C. When using an electronic interface and when feasible based on the Consumer's relationship with the Controller, a Controller should allow Consumers to track what Processing activities they have Consented to or opted out of.

D. There shall be no detriment to a Consumer for refusing or withdrawing Consent, consistent with C.R.S. § 6-1-1308(1)(c)(II), and 4 CCR 904-3, Rule 6.05.

E. If a Consumer withdraws Consent for a Processing activity, the Controller shall cease that Processing activity and provide the Consumer instructions on how to exercise the Right to Deletion or provide a link to exercise the Right to Deletion.

1. If the Personal Data subject to the withdrawal of Consent is Sensitive Data, the Controller shall, pursuant to C.R.S. § 6-1-1308(3) and 4 CCR 904-3, Rule 6.07, delete or otherwise render permanently anonymized or inaccessible the Sensitive Data collected solely for the purpose of that Processing activity and not reasonably necessary in relation to another specified purpose for which the Controller has obtained and continues to have valid Consent.

Rule 7.08 REFRESHING CONSENT

A. A Controller that has obtained Consent from a Consumer must refresh Consent in compliance with all requirements of this Part 7 at regular intervals based on the context and scope of the original Consent, sensitivity of the Personal Data collected, and reasonable expectations of the Consumer.

B. If a Processing purpose materially evolves such that the new purpose becomes a secondary use pursuant to C.R.S. § 6-1-1308(4), the Consumer's original Consent is no longer valid, and the Controller must obtain new Consent pursuant to Part 7 of these rules.

C. For Processing of Sensitive Data, Consent must be refreshed at least annually.

Rule 7.09 USER INTERFACE DESIGN, CHOICE ARCHITECTURE, AND DARK PATTERNS

A. Controllers shall not use an interface design or choice architecture that has the substantial effect of subverting or impairing user autonomy, decision making or choice, or unfairly, fraudulently, or deceptively manipulating or coercing a Consumer into providing Consent.

B. The following principles shall be considered when designing a user interface or a choice architecture:

1. Consent choice options should be presented to Consumers in a symmetrical way that does not impose unequal weight or focus on one available choice over another.

    a. Example: One choice should not be presented with less prominent size, font, or styling than the other choice. Presenting an “I accept” button in a larger size than the “I do not accept” button would not be considered equal or symmetrical. Presenting an “I do not accept” button in a greyed-out color while the “I accept” button is presented in a bright or obvious color would not be considered equal or symmetrical.

    b. Example: If multiple choices are offered to a Consumer, it should be equally easy to accept or reject all options. Presenting the option to “accept all” when offering a Consumer the choice to Consent to the use of Sensitive Data for multiple purposes without an option to “reject all” would not be considered equal or symmetrical.

2. Consent choice options should avoid the use of emotionally manipulative language or visuals to coerce or steer Consumer choice.

    a. Example: One choice should not be presented in a way that creates unnecessary guilt or shames the user into selecting a specific choice. Presenting the choices “I accept, I want to help endangered species” vs “No, I don’t care about animals” could be considered emotionally manipulative.

    b. Example: The explanation of the choice to Consumers should not include gratuitous information to emotionally manipulate Consumers. Explaining that a mobile application “helps save lives” when asking for Consent to collect Sensitive Data for Targeted Advertising may be considered emotionally manipulative if the Targeted Advertising is not critical to the lifesaving functionality of the application.

3. A Consumer’s silence or failure to take an affirmative action should not be interpreted as acceptance or Consent.

    a. Example: A Consumer closing a pop-up window which requests Consent without first affirmatively selecting the equivalent of an “I accept” button should not be interpreted as Consent.

    b. Example: A Consumer navigating forward on a webpage after a Consent choice has been presented without selecting the equivalent of an “I accept” button should not be interpreted as affirmative Consent.

    c. Example: A Consumer continuing to use a Smart TV without replying “I accept” or “I consent” in reply to a verbal request for Consent should not be interpreted as affirmative Consent.

4. Consent choice options should not be presented with a preselected or default option.

    a. Example: Checkboxes or radial buttons should not be selected automatically when presented to a Consumer.

5. A Consumer should be able to select either Consent choice option within the same number of steps.

    a. Example: Consumers should be presented with all choices at the same time. Presenting an "I accept" button next to a "Learn More" button which requires Consumers to take an extra step before they are given the option of an "I do not accept" button could be considered an unnecessary restriction.

    b. Example: Describing the choice before Consumers and placing both the "I accept" and "I do not accept" buttons after a "select preferences" button would not be considered an unnecessary restriction.

    6. A Consumer's expected interaction with a website, application, or product should not be unnecessarily interrupted or intruded upon to request Consent.

    a. Example: Consumers should not be interrupted multiple times in one visit to a website to Consent if they have declined the Consent choice offered when they arrived at the page.

    b. Example: Consumers should not be redirected away from the content or service they are attempting to interact with because they declined the Consent choice offered.

    c. Example: Consumers should not be forced to navigate through multiple pop-ups which cover or otherwise disrupt the content or service they are attempting to interact with because they declined the Consent choice offered.

7. Consent choice options should not include misleading statements, omissions, affirmative misstatements, or intentionally confusing language to obtain Consent.

    a. Example: Choices should not be driven by a false sense of urgency. A countdown clock displayed next to a Consent choice option which states "time is running out to Consent to this data use and receive a limited discount" where the discount is not actually limited by time or availability would be considered creating a false sense of urgency.

    b. Example: Choices should avoid the use of double negatives when describing Consent choice options to Consumers.

    c. Example: Consent choice options should not be presented with confusing or unexpected syntax. "Please do not check this box if you wish to Consent to this data use" would be considered confusing syntax.

    d. Example: The language used for choice options should logically follow the question presented to the Consumer. Offering the options of "Yes" or "No" to the question "Do you wish to provide or decline Consent for the described purposes" would be considered an illogical choice option. The choice options "provide" and "decline" would be considered to logically follow the same question.

8. The vulnerabilities or unique characteristics of the target audience of a product, service, or website should be considered when deciding how to present Consent choice options.

   a. Example: A website or service that primarily interacts with Consumers under the age of 18 should consider the simplicity of the language used to explain the choice options or the way in which cartoon imagery or endorsements might unduly influence their choice.

   b. Example: A website or service that primarily interacts with the elderly should consider font size and space between buttons to ensure readability and ease of interaction with design elements.

9. User interface design and Consent choice architecture should operate in a substantially similar manner when accessed through digital accessibility tools.

   a. Example: If it takes two clicks for a Consumer to Consent through a website, it should take no more than two actions for a Consumer using a digital accessibility tool to complete the same Consent process.

C. The use of Dark Patterns, as defined in C.R.S. § 6-1-1303(9), is prohibited.

D. Consent obtained in violation of this part 4 CCR 904-3, Rule 7.09 may be considered a Dark Pattern. Any agreement obtained through Dark Patterns does not constitute valid Consent in compliance with C.R.S. §§ 6-1-1303, 6-1-1306, and 6-1-1308.

E. The fact that a design or practice is commonly used is not, alone, enough to demonstrate that any particular design or practice is not a Dark Pattern.

F. In addition to the principles included in this part 4 CCR 904-3, Rule 7.09, Controllers may consider statutes, administrative rules, and administrative guidance concerning Dark Patterns from other jurisdictions when evaluating the appropriateness of their proposed choice architecture or system design.

PART 8 DATA PROTECTION ASSESSMENTS

Rule 8.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in this Part 8 is C.R.S. §§ 6-1-108(1), 6-1-1309, and 6-11313. The purpose of the rules in this Part 8 is to provide clarity on the requirements and timing of data protection assessments.

Rule 8.02 SCOPE

A. A data protection assessment shall be a genuine, thoughtful analysis that: 1) identifies and describes all risks posed by Processing that presents a heightened risk of harm to a Consumer; 2) documents measures considered and taken to address and offset those risks, including those duties required by C.R.S. § 6-1-1308; 3) contemplates the benefits of the Processing; and 4) demonstrates that the benefits of the Processing outweigh the risks offset by safeguards in place.

B. If a Controller conducts a data protection assessment for the purpose of complying with another jurisdiction's law or regulation, the assessment shall satisfy the requirements established in this section

if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

C. The depth, level of detail, and scope of data protection assessments should be proportionate to the size of the Controller, amount and sensitivity of Personal Data Processed, and Personal Data Processing activities subject to the assessment.

D. A "comparable set of Processing operations" that can be addressed by a single data protection assessment pursuant to C.R.S. § 6-1-1309(5) is a set of Processing operations using similar methods to collect the same categories of Personal Data for the same purposes.

1. Example: The ACME Toy Store chain is considering using in-store paper forms to collect names, mailing addresses, and birthdays from Children that visit their stores, and using that information to mail a coupon and list of age-appropriate toys to each child during the Child's birth month and every November. ACME uses the same Processors and Processing systems for each category of mailings across all stores. ACME must conduct and document a data protection assessment because it is Processing Personal Data from known Children, which is Sensitive Data. ACME can use the same data protection assessment for Processing the Personal Data for the birthday mailing and November mailing across all stores because in each case it is collecting the same categories of Personal Data in the same way for the purpose of sending coupons and age-appropriate toy lists to Children.

Rule 8.03 STAKEHOLDER INVOLVEMENT

A. A data protection assessment should involve all relevant internal actors from across the Controller's organizational structure, and where needed, relevant external parties, to identify, assess and address the data protection risks.

Rule 8.04 DATA PROTECTION ASSESSMENT CONTENT

A. At a minimum, a data protection assessment must describe each of the following:

1. The Processing activity;

2. The specific purpose of the Processing activity;

3. The specific types of Personal Data to be Processed as well as the sources and amount of Personal Data collected, how long the Personal Data will be maintained, and whether it includes Sensitive Data, including Personal Data from a known Child as described in C.R.S. § 6-1-1303(24);

4. How the Personal Data to be Processed is adequate, relevant, and limited to what is reasonably necessary in relation to the specified purpose;

5. Operational details for the Processing, including planned processes for Personal Data collection, use, storage, retention, and sharing, and the technology or Processors to be used;

6. Names and categories of Personal Data recipients, including Third Parties, Affiliates, and Processors that will have access to the Personal Data;

7. The relationship between the Controller and the Consumer(s) whose Personal Data will be Processed;

8. The expectations of the Consumer(s) concerning how their Personal Data will be used, including expectations based on privacy notices, Consent disclosures and unique vulnerabilities;

9. Procedural safeguards to be afforded to the Consumer when Personal Data is obtained, including:

    a. Whether and how the Controller will request Consent, if required, in accordance with Part 7 of these rules;

    b. Whether and how the Controller will provide Consumers the opportunity to opt out of Processing, if required, in accordance with 4 CCR 904-3, Rule 4.03 and Part 5 of these rules; and

    c. Whether and how the Controller will review web interfaces to be used in Consent requests for Dark Patterns.

10. Alternative Processing activities considered to achieve the same purpose;

11. The sources and nature of risks to individual Consumers and broader Consumer groups posed by the Processing activity. The source and nature of the risks may differ based on the processing activity and type of Personal Data processed. Issues that a Controller may consider in a data protection assessment include, for example:

    a. Constitutional harms, such as speech harms or associational harms;

    b. Intellectual privacy harms, such as the creation of negative inferences about an individual based on what an individual reads, learns, or debates;

    c. Data security harms, such as unauthorized access or adversarial use;

    d. Discrimination harms, such as a violation of federal antidiscrimination laws or antidiscrimination laws of any state or political subdivision thereof, or unlawful disparate impact;

    e. Unfair, unconscionable, or deceptive treatment;

    f. A negative outcome or decision with respect to an individual's eligibility for a right, privilege, or benefit related to financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services;

    g. Financial injury or economic harm;

    h. Physical injury, harassment, or threat to an individual or property;

    i. Privacy harms, such as physical or other intrusion upon the solitude or seclusion or the private affairs or concerns of Consumers, stigmatization or reputational injury;

j. Psychological harm, including anxiety, embarrassment, fear, and other mental trauma; or

k. Other detrimental or negative consequences that affect an individual's private life, privacy affairs, private family matters or similar concerns, including actions and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that Personal Data or other data will not be collected, observed, or used.

12. Measures and safeguards a Controller will put into place to mitigate risks and comply with C.R.S. § 6-1-1308, which may include, but are not limited to:

a. Measures to secure Personal Data during storage, use, and transfer, including any relevant data security frameworks used;

b. Measures to limit the categories and amount of Personal Data to be Processed;

c. The use of De-identified Data;

d. Measures taken to prevent the Processing activity from leading to unlawful discrimination;

e. Contractual agreements in place to ensure that Personal Data in the possession of a Processor or other Third Party remains secure; or

f. Any other practices, policies, or trainings intended to mitigate Processing risks.

13. If a Controller is Processing Personal Data for Profiling as contemplated in C.R.S. § 6-1-1309(2)(a), a data protection assessment of that Processing activity must also comply with 4 CCR 904-3, Rule 9.06;

14. If a Controller is Processing Sensitive Data pursuant to the exception in section 4 CCR 904-3, Rule 6.10, the details of the process implemented to ensure that Personal Data and Sensitive Data Inferences are not transferred and are deleted within twelve (12) hours of the Personal Data Processing activity subject to the exception, as well as the auditing procedure for this process;

15. The benefits of the Processing that may flow to the Controller, Consumer, and other expected stakeholders, and how the benefits outweigh the risks, as mitigated by safeguards, and justify the Processing activity;

16. Relevant internal actors and external parties contributing to the data protection assessment;

17. The data protection assessment review process, including whether any internal or external audit was conducted, and if so, the name of the auditor, the names and positions of individuals involved in the review process, and the details of the audit process; and

18. Dates the data protection assessment was reviewed and approved, and names, positions, and signatures of the individuals responsible for the review and approval.

Rule 8.05 TIMING

A. A Controller shall conduct and document a data protection assessment before initiating a data Processing activity that Presents a Heightened Risk of Harm to a Consumer, as defined at C.R.S. § 6-1-1309(2).

B. A Controller shall review and update the data protection assessment periodically throughout the Processing activity's lifecycle in order to: 1) monitor for harm caused by the Processing and adjust safeguards accordingly; and 2) ensure that data protection and privacy are considered as the Controller makes new decisions with respect to the Processing.

C. Data protection assessments containing Processing for Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer shall be reviewed and updated at least annually, and include an updated evaluation for fairness and disparate impact and the results of any such evaluation.

D. A new data Processing activity is generated when existing Processing activities are modified in a way that materially changes the level of risk presented. When a new data Processing activity is generated, a data protection assessment must reflect changes to the pre-existing activity and additional considerations and safeguards to offset the new risk level.

1. Modifications that may materially change the level of risk of a Processing activity may include, without limitation, changes to any of the following:

a. The way that existing systems or Processes handle Personal Data;

b. Processing purpose;

c. Personal data Processed or sources of Personal Data;

d. Method of collection of Personal Data;

e. Personal Data recipients;

f. Processor roles or Processors;

g. Algorithm applied or algorithmic result; or

h. Software or other systems used for Processing

E. Data protection assessments, including prior versions which have been revised when a new data Processing activity is generated, shall be stored for as long as the Processing activity continues, and for at least three (3) years after the conclusion of the Processing activity. Data protection assessments shall be held in an electronic, transferable form.

F. Data protection assessments shall be required for activities conducted after July 1, 2023 and are not retroactive.

Rule 8.06 ATTORNEY GENERAL REQUESTS

A. A Controller shall make the data protection assessment available to the Attorney General within thirty (30) days of the Attorney General's request.

PART 9 PROFILING

Rule 9.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in this Part 9 is C.R.S. §§ 6-1-108(1), 6-1-1306, 6-1-1309, and 6-1-1313. The purpose of the rules in this Part 9 is to provide clarity on the duties and rights related to Profiling.

Rule 9.02 SCOPE

A. Controllers have an affirmative obligation to provide clear, understandable, and transparent information to Consumers about how their Personal Data is used, including for Profiling, pursuant to C.R.S. § 6-1-1302(1)(c)(II)(B).

B. Consumers have the right to opt out of Profiling when the Profiling is done in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer, pursuant to C.R.S. §§ 6-1-1306(1)(a)(I).

C. Controllers must conduct and document a data protection assessment compliant with C.R.S. § 61-1309 and Part 8 of these rules before Processing Personal Data for Profiling as contemplated in C.R.S. §§ 6-1-1303(10) and 6-1-1309(1)(a)(I).

D. The Automated Processing used in Profiling includes Solely Automated Processing, Human Reviewed Automated Processing, and Human Involved Automated Processing, as defined at 4 CCR 904-3, Rule 2.02.

Rule 9.03 PROFILING OPT-OUT TRANSPARENCY

A. To ensure that Consumers understand how their Personal Data may be used for Profiling in furtherance of Decisions that Produce Legal or Other Similarly Significant Effects Concerning a Consumer, Controllers that Process Personal Data for Profiling covered by C.R.S. §§ 6-11303(10) and 6-1-1306(1)(a)(I) shall provide clear, understandable, and transparent information to Consumers in the required privacy notice, including at a minimum:

1. What decision is subject to Profiling;

2. The categories of Personal Data that were or will be Processed as part of the Profiling in Furtherance of Decisions that Produce Legal or Other Similarly Significant Effects;

3. A plain language explanation of the logic used in the Profiling process;

4. Why Profiling is relevant to the ultimate decision;

5. If the Profiling is used to serve ads related to housing, employment, or financial or lending services;

6. If the system has been evaluated for accuracy, fairness, or bias, including the impact of the use of Sensitive Data, and the outcome of any such evaluation;

7. The benefits and potential consequences of the decision concerning the Consumer; and

8. Information about how a Consumer may exercise the right to opt out of the Processing of Personal Data concerning the Consumer for Profiling in Furtherance of Decisions that Produce Legal or Other Similarly Significant Effects.

B. Notwithstanding the requirements in 4 CCR 904-3, Rule 9.03(A), nothing in 4 CCR 904-3, Rule 9.03 shall be construed as requiring the Controller to provide information to a Consumer in a manner that would disclose the Controller's trade secrets.

Rule 9.04 OPTING OUT OF PROFILING IN FURTHERANCE OF DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS CONCERNING A CONSUMER

A. Consumers have the right to opt out of Profiling in furtherance of Decisions that Produce Legal or other Similarly Significant Effects Concerning a Consumer through the method specified by the Controller in the required privacy notice, pursuant to C.R.S. § 6-1-1306(1) and 4 CCR 904-3, Rule 4.03.

B. Requests to opt out of Profiling in furtherance of Decisions that Produce Legal or other Similarly Significant Effects Concerning a Consumer based on Solely Automated Processing or Human Reviewed Automated Processing shall be honored pursuant to C.R.S. § 6-1-1306(2).

C. A Controller may not take action on a request to opt out of Profiling in furtherance of Decisions that Produce Legal or other Similarly Significant Effects Concerning a Consumer if the Profiling used is based on Human Involved Automated Processing. If a Controller does not take action based on this reason, the Controller shall inform the Consumer pursuant to C.R.S. § 6-11306(2)(b) and include the following information:

1. The decision subject to the Profiling;

2. The specific pieces of Personal Data that were or will be used as part of the Profiling used in the decision-making process;

3. A non-technical, plain language explanation of the logic used in the Profiling process, or a link to such information if it is included in the Controller's privacy notice;

4. A non-technical, plain language explanation of the role of meaningful human involvement in Profiling and the decision-making process;

5. Why the Profiling is relevant to the decision-making process;

6. The benefits and potential consequences of the decision based on the Profiling; and

7. An explanation of how Consumers can correct or delete the Personal Data used in the Profiling used in the decision-making process.

D. In order to ensure that Consumers have an opportunity to exercise their right to opt out of Profiling in furtherance of Decisions that Produce Legal or Other Similarly Significant Effects Concerning a

Consumer, Controllers that Process Personal Data for Profiling covered by C.R.S. §§ 6-1-1303(10) and 6-1-1306(1)(a)(I) shall provide a method to exercise the right to opt out of Profiling in furtherance of Decision that Produce Legal or Other similarly Significant Effects Concerning a Consumer clearly and conspicuously in any required privacy notice and in a clear, conspicuous, and readily accessible location outside of the privacy notice.

Rule 9.05 CONSENT FOR PROFILING IN FURTHERANCE OF DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS CONCERNING A CONSUMER

A. When a Consumer has opted out of Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer as defined by C.R.S. § 6-1-1303(10), the Controller may request that a Consumer provide Consent after opting out subject to 4 CCR 9043, Rule 7.05.

B. If a Controller decides to begin Processing Personal Data for Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer and such Processing is not reasonably necessary to or compatible with the original specified purposes for which the Personal Data was Processed, the Controller shall request the Consumer provide Consent subject to C.R.S. § 6-1-1308(4) and Part 7 of these rules.

C. Any request for Consent to Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer must include meaningful information about the Profiling that allows a Consumer to make an informed, freely given, and specific choice, including, at a minimum:

1. The decision subject to the Profiling;

2. The categories of Personal Data used in the Profiling;

3. A plain language explanation of the logic used in the Profiling, or a link to such information if it is included in the Controller's privacy notice;

4. How Profiling is used in the decision-making process, including if the decision is based on Solely Automated Processing, Human Reviewed Automated Processing, or Human Involved Automated Processing;

5. Why the Profiling is relevant to the decision-making process;

6. Potential benefits and consequences of the decision based on the Profiling; and

7. A link to where Consumers can find any additional information about the Profiling and decision-making process and their associated rights.

D. Notwithstanding the requirements in 4 CCR 904-3, Rule 9.05(C), nothing in 4 CCR 904-3, Rule 9.03 shall be constructed as requiring the Controller to provide information to a Consumer in a manner that would disclose the Controller's trade secrets.

Rule 9.06 DATA PROTECTION ASSESSMENTS FOR PROFILING

A. Controllers must conduct and document a data protection assessment compliant with C.R.S. § 61-1309 and 4 CCR 904-3. Rules 8.01-8.05 before Processing Personal Data for Profiling if the Profiling presents a reasonably foreseeable risk of:

1. Unfair or deceptive treatment of, or unlawful disparate impact on Consumers;

2. Financial or physical injury to Consumers;

3. A physical or other intrusion upon the solitude or seclusion, or private affairs or concerns, of Consumers if the intrusion would be offensive to a reasonable person; or

4. Other substantial injury to Consumers.

B. Profiling under C.R.S. § 6-1-1309(2)(a) and covered by required data protection assessment includes Profiling using Solely Automated Processing, Human Reviewed Automated Processing, and Human Involved Automated Processing.

C. "Unfair or deceptive treatment" as used in this 4 CCR 904-3, Rule 9.06 includes conduct or activity which violates state or federal laws that prohibit unfair and deceptive commercial practices.

D. "Unlawful disparate impact" as used in this 4 CCR 904-3, Rule 9.06 includes conduct or activity which violates state or federal laws that prohibit unlawful discrimination against Consumers.

E. "Other substantial injury" to Consumers as used in this 4 CCR 904-3, Rule 9.06 includes but is not limited to a small harm to a large number of Consumers.

F. If a Controller is Processing Personal Data for Profiling under C.R.S. § 6-1-1309(2)(a), a data protection assessment of that Processing activity must include the elements listed at 4 CCR 9043, Rule 8.04 as well as each of the following:

1. The specific types of Personal Data that were or will be used in the Profiling or decision-making process;

2. The decision to be made using the automated decision-making system;

3. The benefits of Automated Processing over manual Processing for the stated purpose;

4. A plain language explanation of why the Profiling directly and reasonably relates to the Controller's goods and services;

5. An explanation of the training data and logic used to create the Profiling system, including any statistics used in the analysis;

6. If the Profiling is conducted by Third Party software purchased by the Controller, the name of the software and copies of any internal or external evaluations of the accuracy and reliability of the software;

7. A plain language description of the outputs secured from the Profiling process;

8. A plain language description of how the outputs from the Profiling process are or will be used, including whether and how they are used to make a decision to provide or deny or substantially contribute to the provision or denial of financial or lending services, housing, insurance, education, enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services.

9. If there is human involvement in the Profiling process, the degree and details of any human involvement;

10. How the Profiling system is evaluated for fairness and disparate impact, and the results of any such evaluation;

11. Safeguards used to reduce the risk of harms identified; and

12. Safeguards for any data sets produced by or derived from the Profiling.

PART 10 MATERIALS INCORPORATED BY REFERENCE

Rule 10.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in this Part 10 is C.R.S. §§ 6-1-108(1) and 6-1-1313. The purpose of the rules in this Part 10 is to incorporate by reference the guidelines that are referred to in 4 CCR 904-3, Rule 3.01(A)(2).

Rule 10.02 WEB CONTENT ACCESSIBILITY GUIDELINES

A. The Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, are hereby incorporated into 4 CCR 904-3, Rule 3.01(A)(2) by reference pursuant to C.R.S. § 24-4-103(12.5), and do not include any later amendments.

B. Copies of the Web Content Accessibility Guidelines that are incorporated by reference into these rules may be obtained by sending a written request to the following address by U.S. mail:

Colorado Department of Law
Ralph L. Carr Judicial Center
1300 Broadway, 9th Floor
Denver, CO 80203

C. The Web Content Accessibility Guidelines published by the World Wide Web Consortium incorporated by reference into these rules are available at no cost in an electronic form online at https://www.w3.org/TR/WCAG21/.

D. The Colorado Department of Law also maintains a copy of the Web Content Accessibility Guidelines that are incorporated by reference into these rules that is available for public inspection at the Colorado Department of Law's office during regular business hours.

KILPATRICK TOWNSEND

Connecticut Act Concerning Personal Data Privacy and Online Monitoring

On May 10, 2022, the Connecticut Act Concerning Personal Data Privacy and Online Monitoring ("CTDPA") was signed into law, making the CTDPA the fifth comprehensive data privacy law passed in the United States.

The CTDPA will take effect on July 1, 2023. The full text of the CTDPA is provided below.

Please see the Comprehensive Data Privacy Law Quick Reference Guide for a high-level comparison of the requirements of the CTDPA compared to other comprehensive data privacy laws.

CTDPA Official Text:

Substitute Senate Bill No. 6

Public Act No. 22-15

AN ACT CONCERNING PERSONAL DATA PRIVACY AND ONLINE MONITORING.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. (NEW) (*Effective July 1, 2023*) As used in this section and sections 2 to 11, inclusive, of this act, unless the context otherwise requires:

(1) "Affiliate" means a legal entity that shares common branding with another legal entity or controls, is controlled by or is under common control with another legal entity. For the purposes of this subdivision, "control" or "controlled" means (A) ownership of, or the power to vote, more than fifty per cent of the outstanding shares of any class of voting security of a company, (B) control in any manner over the election of a majority of the directors or of individuals exercising similar functions, or (C) the power to exercise controlling influence over the management of a company.

(2) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights afforded under subdivisions (1) to (4), inclusive, of subsection (a) of section 4 of this act is being made by, or on behalf of, the consumer who is entitled to exercise such consumer rights with respect to the personal data at issue.

(3) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include (A) a digital or physical photograph, (B) an audio or video recording, or (C) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

(4) "Business associate" has the same meaning as provided in HIPAA.

(5) "Child" has the same meaning as provided in COPPA.

(6) "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. "Consent" does not include (A) acceptance of a general or broad terms of use or similar document that contains

descriptions of personal data processing along with other, unrelated information, (B) hovering over, muting, pausing or closing a given piece of content, or (C) agreement obtained through the use of dark patterns.

(7) "Consumer" means an individual who is a resident of this state. "Consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency.

(8) "Controller" means an individual who, or legal entity that, alone or jointly with others determines the purpose and means of processing personal data.

(9) "COPPA" means the Children's Online Privacy Protection Act of 1998, 15 USC 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to said act, as said act and such regulations, rules, guidance and exemptions may be amended from time to time.

(10) "Covered entity" has the same meaning as provided in HIPAA.

(11) "Dark pattern" (A) means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and (B) includes, but is not limited to, any practice the Federal Trade Commission refers to as a "dark pattern".

(12) "Decisions that produce legal or similarly significant effects concerning the consumer" means decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services.

(13) "De-identified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data (A) takes reasonable measures to ensure that such data cannot be associated with an individual, (B) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data, and (C) contractually obligates any recipients of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this subdivision.

(14) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq., as amended from time to time.

(15) "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly.

(16) "Institution of higher education" means any individual who, or school, board, association, limited liability company or corporation that, is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees.

(17) "Nonprofit organization" means any organization that is exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent corresponding internal revenue code of the United States, as amended from time to time.

(18) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include de-identified data or publicly available information.

(19) “Precise geolocation data” means information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of one thousand seven hundred fifty feet. “Precise geolocation data” does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(20) “Process” or “processing” means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion or modification of personal data.

(21) “Processor” means an individual who, or legal entity that, processes personal data on behalf of a controller.

(22) “Profiling” means any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual’s economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

(23) “Protected health information” has the same meaning as provided in HIPAA.

(24) “Pseudonymous data” means personal data that cannot be attributed to a specific individual without the use of additional information, provided such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

(25) “Publicly available information” means information that (A) is lawfully made available through federal, state or municipal government records or widely distributed media, and (B) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.

(26) “Sale of personal data” means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. “Sale of personal data” does not include (A) the disclosure of personal data to a processor that processes the personal data on behalf of the controller, (B) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer, (C) the disclosure or transfer of personal data to an affiliate of the controller, (D) the disclosure of personal data where the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party, (E) the disclosure of personal data that the consumer (i) intentionally made available to the general public via a channel of mass media, and (ii) did not restrict to a specific audience, or (F) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction, or a proposed merger, acquisition, bankruptcy or other transaction, in which the third party assumes control of all or part of the controller’s assets.

(27) “Sensitive data” means personal data that includes (A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status, (B) the processing of genetic or biometric data for the purpose of uniquely identifying an individual, (C) personal data collected from a known child, or (D) precise geolocation data.

(28) “Targeted advertising” means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer’s activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer’s preferences or interests. “Targeted advertising” does not include (A) advertisements based on activities within a controller’s own Internet web sites or online applications, (B) advertisements based on the context of a consumer’s current search query, visit to an Internet web site or online application, (C) advertisements directed to a consumer in response to the consumer’s

request for information or feedback, or (D) processing personal data solely to measure or report advertising frequency, performance or reach.

(29) "Third party" means an individual or legal entity, such as a public authority, agency or body, other than the consumer, controller or processor or an affiliate of the processor or the controller.

(30) "Trade secret" has the same meaning as provided in section 35-51 of the general statutes.

Sec. 2. (NEW) (*Effective July 1, 2023*) The provisions of sections 1 to 11, inclusive, of this act apply to persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and that during the preceding calendar year: (1) Controlled or processed the personal data of not less than one hundred thousand consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or (2) controlled or processed the personal data of not less than twenty-five thousand consumers and derived more than twenty-five per cent of their gross revenue from the sale of personal data.

Sec. 3. (NEW) (*Effective July 1, 2023*) (a) The provisions of sections 1 to 11, inclusive, of this act do not apply to any: (1) Body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state; (2) nonprofit organization; (3) institution of higher education; (4) national securities association that is registered under 15 USC 78o-3 of the Securities Exchange Act of 1934, as amended from time to time; (5) financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.; or (6) covered entity or business associate, as defined in 45 CFR 160.103.

(b) The following information and data is exempt from the provisions of sections 1 to 11, inclusive, of this act: (1) Protected health information under HIPAA; (2) patient-identifying information for purposes of 42 USC 290dd-2; (3) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR 46; (4) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use; (5) the protection of human subjects under 21 CFR Parts 6, 50 and 56, or personal data used or shared in research, as defined in 45 CFR 164.501, that is conducted in accordance with the standards set forth in this subdivision and subdivisions (3) and (4) of this subsection, or other research conducted in accordance with applicable law; (6) information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq.; (7) patient safety work product for purposes of section 19a-127o of the general statutes and the Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as amended from time to time; (8) information derived from any of the health care related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA; (9) information originating from and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this subsection that is maintained by a covered entity or business associate, program or qualified service organization, as specified in 42 USC 290dd-2, as amended from time to time; (10) information used for public health activities and purposes as authorized by HIPAA, community health activities and population health activities; (11) the collection, maintenance, disclosure, sale, communication or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time; (12) personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended from time to time; (13) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC 1232g et seq., as amended from time to time; (14) personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 USC 2001 et seq., as

amended from time to time; (15) data processed or maintained (A) in the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor or third party, to the extent that the data is collected and used within the context of that role, (B) as the emergency contact information of an individual under sections 1 to 11, inclusive, of this act used for emergency contact purposes, or (C) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under subdivision (1) of this subsection and used for the purposes of administering such benefits; and (16) personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the Airline Deregulation Act, 49 USC 40101 et seq., as amended from time to time, by an air carrier subject to said act, to the extent sections 1 to 11, inclusive, of this act are preempted by the Airline Deregulation Act, 49 USC 41713, as amended from time to time.

(c) Controllers and processors that comply with the verifiable parental consent requirements of COPPA shall be deemed compliant with any obligation to obtain parental consent pursuant to sections 1 to 11, inclusive, of this act.

Sec. 4. (NEW) (*Effective July 1, 2023*) (a) A consumer shall have the right to: (1) Confirm whether or not a controller is processing the consumer's personal data and access such personal data, unless such confirmation or access would require the controller to reveal a trade secret; (2) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data; (3) delete personal data provided by, or obtained about, the consumer; (4) obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means, provided such controller shall not be required to reveal any trade secret; and (5) opt out of the processing of the personal data for purposes of (A) targeted advertising, (B) the sale of personal data, except as provided in subsection (b) of section 6 of this act, or (C) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

(b) A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with section 5 of this act to exercise the rights of such consumer to opt out of the processing of such consumer's personal data for purposes of subdivision (5) of subsection (a) of this section on behalf of the consumer. In the case of processing personal data of a known child, the parent or legal guardian may exercise such consumer rights on the child's behalf. In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the consumer may exercise such rights on the consumer's behalf.

(c) Except as otherwise provided in sections 1 to 11, inclusive, of this act, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to said sections as follows:

(1) A controller shall respond to the consumer without undue delay, but not later than forty-five days after receipt of the request. The controller may extend the response period by forty-five additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of any such extension within the initial forty-five-day response period and of the reason for the extension.

(2) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than forty-five days after receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision.

(3) Information provided in response to a consumer request shall be provided by a controller, free of charge, once per consumer during any twelve-month period. If requests from a consumer are manifestly unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

(4) If a controller is unable to authenticate a request to exercise any of the rights afforded under subdivisions (1) to (4), inclusive, of subsection (a) of this section using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise such right or rights until such consumer provides additional information reasonably necessary to authenticate such consumer and such consumer's request to exercise such right or rights. A controller shall not be required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that such request is fraudulent. If a controller denies an opt-out request because the controller believes such request is fraudulent, the controller shall send a notice to the person who made such request disclosing that such controller believes such request is fraudulent, why such controller believes such request is fraudulent and that such controller shall not comply with such request.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete such data pursuant to subdivision (3) of subsection (a) of this section by (A) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the controller's records and not using such retained data for any other purpose pursuant to the provisions of sections 1 to 11, inclusive, of this act, or (B) opting the consumer out of the processing of such personal data for any purpose except for those exempted pursuant to the provisions of sections 1 to 11, inclusive, of this act.

(d) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Not later than sixty days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

Sec. 5. (NEW) (*Effective July 1, 2023*) A consumer may designate another person to serve as the consumer's authorized agent, and act on such consumer's behalf, to opt out of the processing of such consumer's personal data for one or more of the purposes specified in subdivision (5) of subsection (a) of section 4 of this act. The consumer may designate such authorized agent by way of, among other things, a technology, including, but not limited to, an Internet link or a browser setting, browser extension or global device setting, indicating such consumer's intent to opt out of such processing. A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on such consumer's behalf.

Sec. 6. (NEW) (*Effective July 1, 2023*) (a) A controller shall: (1) Limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer; (2) except as otherwise provided in sections 1 to 11, inclusive, of this act, not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent; (3) establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the

volume and nature of the personal data at issue; (4) not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with COPPA; (5) not process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers; (6) provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of such consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request; and (7) not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a controller has actual knowledge, and wilfully disregards, that the consumer is at least thirteen years of age but younger than sixteen years of age. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in sections 1 to 11, inclusive, of this act, including denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods or services to the consumer.

(b) Nothing in subsection (a) of this section shall be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts or club card program.

(c) A controller shall provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes: (1) The categories of personal data processed by the controller; (2) the purpose for processing personal data; (3) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request; (4) the categories of personal data that the controller shares with third parties, if any; (5) the categories of third parties, if any, with which the controller shares personal data; and (6) an active electronic mail address or other online mechanism that the consumer may use to contact the controller.

(d) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing.

(e) (1) A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to sections 1 to 11, inclusive, of this act. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests and the ability of the controller to verify the identity of the consumer making the request. A controller shall not require a consumer to create a new account in order to exercise consumer rights, but may require a consumer to use an existing account. Any such means shall include:

(A) (i) Providing a clear and conspicuous link on the controller's Internet web site to an Internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or sale of the consumer's personal data; and (ii) Not later than January 1, 2025, allowing a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent, with such consumer's consent, by a platform, technology or mechanism to the controller indicating such consumer's intent to opt out of any such processing or sale. Such platform, technology or mechanism shall:

(I) Not unfairly disadvantage another controller;

(II) Not make use of a default setting, but, rather, require the consumer to make an affirmative, freely given and unambiguous choice to opt out of any processing of such consumer's personal data pursuant to sections 1 to 11, inclusive, of this act;

(III) Be consumer-friendly and easy to use by the average consumer;

(IV) Be as consistent as possible with any other similar platform, technology or mechanism required by any federal or state law or regulation; and

(V) Enable the controller to accurately determine whether the consumer is a resident of this state and whether the consumer has made a legitimate request to opt out of any sale of such consumer's personal data or targeted advertising.

(B) If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent in accordance with the provisions of subparagraph (A) of this subdivision conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts or club card program, the controller shall comply with such consumer's opt-out preference signal but may notify such consumer of such conflict and provide to such consumer the choice to confirm such controller-specific privacy setting or participation in such program.

(2) If a controller responds to consumer opt-out requests received pursuant to subparagraph (A) of subdivision (1) of this subsection by informing the consumer of a charge for the use of any product or service, the controller shall present the terms of any financial incentive offered pursuant to subsection (b) of this section for the retention, use, sale or sharing of the consumer's personal data.

Sec. 7. (NEW) (*Effective July 1, 2023*) (a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under sections 1 to 11, inclusive, of this act. Such assistance shall include: (1) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests; (2) taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security, as defined in section 36a-701b of the general statutes, of the system of the processor, in order to meet the controller's obligations; and (3) providing necessary information to enable the controller to conduct and document data protection assessments.

(b) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The contract shall also require that the processor: (1) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data; (2) at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law; (3) upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in sections 1 to 11, inclusive, of this act; (4) after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and (5) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an

assessment of the processor's policies and technical and organizational measures in support of the obligations under sections 1 to 11, inclusive, of this act, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.

(c) Nothing in this section shall be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of such controller's or processor's role in the processing relationship, as described in sections 1 to 11, inclusive, of this act.

(d) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in such person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to such processing and may be subject to an enforcement action under section 11 of this act.

Sec. 8. (NEW) (*Effective July 1, 2023*) (a) A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes: (1) The processing of personal data for the purposes of targeted advertising; (2) the sale of personal data; (3) the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of (A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers, (B) financial, physical or reputational injury to consumers, (C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or (D) other substantial injury to consumers; and (4) the processing of sensitive data.

(b) Data protection assessments conducted pursuant to subsection (a) of this section shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The controller shall factor into any such data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(c) The Attorney General may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in sections 1 to 11, inclusive, of this act. Data protection assessments shall be confidential and shall be exempt from disclosure under the Freedom of Information Act, as defined in section 1-200 of the general statutes. To the extent any information contained in a data protection assessment disclosed to the Attorney General includes information subject to attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

(d) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(e) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment shall be deemed to satisfy the requirements established in this

section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

(f) Data protection assessment requirements shall apply to processing activities created or generated after July 1, 2023, and are not retroactive.

Sec. 9. (NEW) (*Effective July 1, 2023*) (a) Any controller in possession of de-identified data shall: (1) Take reasonable measures to ensure that the data cannot be associated with an individual; (2) publicly commit to maintaining and using de-identified data without attempting to reidentify the data; and (3) contractually obligate any recipients of the de-identified data to comply with all provisions of sections 1 to 11, inclusive, of this act.

(b) Nothing in sections 1 to 11, inclusive, of this act shall be construed to: (1) Require a controller or processor to re-identify de-identified data or pseudonymous data; or (2) maintain data in identifiable form, or collect, obtain, retain or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

(c) Nothing in sections 1 to 11, inclusive, of this act shall be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller: (1) Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data; (2) does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and (3) does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

(d) The rights afforded under subdivisions (1) to (4), inclusive, of subsection (a) of section 4 of this act shall not apply to pseudonymous data in cases where the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

(e) A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

Sec. 10. (NEW) (*Effective July 1, 2023*) (a) Nothing in sections 1 to 11, inclusive, of this act shall be construed to restrict a controller's or processor's ability to: (1) Comply with federal, state or municipal ordinances or regulations; (2) comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, municipal or other governmental authorities; (3) cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state or municipal ordinances or regulations; (4) investigate, establish, exercise, prepare for or defend legal claims; (5) provide a product or service specifically requested by a consumer; (6) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty; (7) take steps at the request of a consumer prior to entering into a contract; (8) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual, and where the processing cannot be manifestly based on another legal basis; (9) prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action; (10) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that determine, (A) whether the deletion of the information is likely to provide

substantial benefits that do not exclusively accrue to the controller, (B) the expected benefits of the research outweigh the privacy risks, and (C) whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification; (11) assist another controller, processor or third party with any of the obligations under sections 1 to 11, inclusive, of this act; or (12) process personal data for reasons of public interest in the area of public health, community health or population health, but solely to the extent that such processing is (A) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed, and (B) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law.

(b) The obligations imposed on controllers or processors under sections 1 to 11, inclusive, of this act shall not restrict a controller's or processor's ability to collect, use or retain data for internal use to: (1) Conduct internal research to develop, improve or repair products, services or technology; (2) effectuate a product recall; (3) identify and repair technical errors that impair existing or intended functionality; or (4) perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(c) The obligations imposed on controllers or processors under sections 1 to 11, inclusive, of this act shall not apply where compliance by the controller or processor with said sections would violate an evidentiary privilege under the laws of this state. Nothing in sections 1 to 11, inclusive, of this act shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the state as part of a privileged communication.

(d) A controller or processor that discloses personal data to a processor or third-party controller in accordance with sections 1 to 11, inclusive, of this act shall not be deemed to have violated said sections if the processor or third-party controller that receives and processes such personal data violates said sections, provided, at the time the disclosing controller or processor disclosed such personal data, the disclosing controller or processor did not have actual knowledge that the receiving processor or third-party controller would violate said sections. A third-party controller or processor receiving personal data from a controller or processor in compliance with sections 1 to 11, inclusive, of this act is likewise not in violation of said sections for the transgressions of the controller or processor from which such third-party controller or processor receives such personal data.

(e) Nothing in sections 1 to 11, inclusive, of this act shall be construed to: (1) Impose any obligation on a controller or processor that adversely affects the rights or freedoms of any person, including, but not limited to, the rights of any person (A) to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution, or (B) under section 52-146t of the general statutes; or (2) apply to any person's processing of personal data in the course of such person's purely personal or household activities.

(f) Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is: (1) Reasonably necessary and proportionate to the purposes listed in this section; and (2) adequate, relevant and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used or retained pursuant to subsection (b) of this section shall, where applicable, take into account the nature and purpose or purposes of such collection, use or retention. Such data shall be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use or retention of personal data.

(g) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsection (f) of this section.

(h) Processing personal data for the purposes expressly identified in this section shall not solely make a legal entity a controller with respect to such processing.

Sec. 11. (NEW) (*Effective July 1, 2023*) (a) The Attorney General shall have exclusive authority to enforce violations of sections 1 to 10, inclusive, of this act.

(b) During the period beginning on July 1, 2023, and ending on December 31, 2024, the Attorney General shall, prior to initiating any action for a violation of any provision of sections 1 to 10, inclusive, of this act, issue a notice of violation to the controller if the Attorney General determines that a cure is possible. If the controller fails to cure such violation within sixty days of receipt of the notice of violation, the Attorney General may bring an action pursuant to this section. Not later than February 1, 2024, the Attorney General shall submit a report, in accordance with section 11-4a of the general statutes, to the joint standing committee of the General Assembly having cognizance of matters relating to general law disclosing: (1) The number of notices of violation the Attorney General has issued; (2) the nature of each violation; (3) the number of violations that were cured during the sixty-day cure period; and (4) any other matter the Attorney General deems relevant for the purposes of such report.

(c) Beginning on January 1, 2025, the Attorney General may, in determining whether to grant a controller or processor the opportunity to cure an alleged violation described in subsection (b) of this section, consider: (1) The number of violations; (2) the size and complexity of the controller or processor; (3) the nature and extent of the controller's or processor's processing activities; (4) the substantial likelihood of injury to the public; (5) the safety of persons or property; and (6) whether such alleged violation was likely caused by human or technical error.

(d) Nothing in sections 1 to 10, inclusive, of this act shall be construed as providing the basis for, or be subject to, a private right of action for violations of said sections or any other law.

(e) A violation of the requirements of sections 1 to 10, inclusive, of this act shall constitute an unfair trade practice for purposes of section 42-110b of the general statutes and shall be enforced solely by the Attorney General, provided the provisions of section 42-110g of the general statutes shall not apply to such violation.

Sec. 12. (*Effective from passage*) (a) Not later than September 1, 2022, the chairpersons of the joint standing committee of the General Assembly having cognizance of matters relating to general law shall convene a task force to study:

(1) Information sharing among health care providers and social care providers and make recommendations to eliminate health disparities and inequities across sectors, as described in subsection (a) of section 19a-133b of the general statutes;

(2) Algorithmic decision-making and make recommendations concerning the proper use of data to reduce bias in such decision-making;

(3) Possible legislation that would require an operator, as defined in the Children's Online Privacy Protection Act, 15 USC 6501 et seq., as amended from time to time, to, upon a parent's request, delete the account of a child and cease to collect, use or maintain, in retrievable form, the child's personal data on the operator's Internet web

site or online service directed to children, and provide parents with an accessible, reasonable and verifiable means to make such a request;

(4) Any means available to verify the age of a child who creates a social media account;

(5) Issues concerning data colocation, including, but not limited to, the impact that the provisions of sections 1 to 11, inclusive, of this act have on third parties that provide data storage and colocation services;

(6) Possible legislation that would expand the provisions of sections 1 to 11, inclusive, of this act to include additional persons or groups; and

(7) Other topics concerning data privacy.

(b) The chairpersons of the joint standing committee of the General Assembly having cognizance of matters relating to general law shall serve as the chairpersons of the task force, and shall jointly appoint the members of the task force. Such members shall include, but need not be limited to:

(1) Representatives from business, academia, consumer advocacy groups, small and large companies and the office of the Attorney General; and

(2) Attorneys with experience in privacy law.

(c) The administrative staff of the joint standing committee of the General Assembly having cognizance of matters relating to general law shall serve as administrative staff of the task force.

(d) Not later than January 1, 2023, the task force shall submit a report on its findings and recommendations to the joint standing committee of the General Assembly having cognizance of matters relating to general law, in accordance with the provisions of section 11-4a of the general statutes. The task force shall terminate on the date that it submits such report or January 1, 2023, whichever is later.

Approved May 10, 2022

KILPATRICK TOWNSEND

Illinois Biometric Information Privacy Act

Although not a comprehensive data privacy law, the Illinois Biometric Information Privacy Act ("BIPA") was the first United States law to comprehensively regulate biometric information. BIPA is unique to other biometrics laws in that it provides for a private right of action.

BIPA has been in effect since 2008. The full text of BIPA is accessible at https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

Please see the Biometrics Law Quick Reference Guide for a high-level comparison of the requirements of BIPA compared to other comprehensive biometrics laws.

KILPATRICK TOWNSEND

Nevada Senate Bill No. 260

The Nevada legislature updated (through SB 260) a law permitting consumers to opt-out of the sale of the consumer's personal information to profoundly expand the scope of (1) sales of which consumers may opt-out and (2) types of entities subject to the law.

Nevada consumers no longer have only the right to opt-out of sales to data brokers. As revised by SB 260 Nevada law broadly defines "sales" to include exchanges of information for monetary consideration to any third party.

Data brokers, in addition to website operators, must now field opt-outs under Nevada's updated law. As originally enacted, the law applied only to operators of commercial websites and online services. As of October 2021 (when SB 260 took effect), data brokers must also comply with the law. (Unlike California and Vermont law, however, Nevada law does not create a data broker registry).

Exceptions abound under the Nevada law and SB 260 preserves and expands upon those exceptions. Given the expanded scope of sales, companies may need to rely on such exceptions more substantially than they have been since 2019. A few of the key exceptions added by SB 260 ensure that the law does **not** apply to:

- Consumer reporting agencies and any agencies and entities subject to the Gramm-Leach Bliley Act;
- Any personally identifiable information subject to the Fair Credit Reporting Act or Gramm-Leach-Bliley Act;
- Entities that collect, maintain, or sell personally identifiable information for fraud prevention purposes; and
- Any organization that does not collect, maintain, or sell covered information.

Given that Nevada's privacy law also applies to traditional selling, organizations should reassess their compliance positions under the law. Fortunately, organizations that find themselves subject to the law probably also sell personal information under the CCPA, so compliance may be as simple as expanding CCPA opt-out rights to Nevadans.

The full text of SB 260 is accessible at https://www.leg.state.nv.us/App/NELIS/REL/81st2021/Bill/7805/Text.

KILPATRICK TOWNSEND

Texas Capture or Use of Biometric Identifier Act

Although not a comprehensive data privacy law, the Texas Capture or Use of Biometric Identifier Act ("CUBI") is the second United States law to comprehensively regulate biometrics.

CUBI has been in effect since 2009. The full text of CUBI is accessible at https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.HTM.

Please see the Biometrics Law Quick Reference Guide for a high-level comparison of the requirements of CUBI compared to other comprehensive biometrics laws.

KILPATRICK TOWNSEND

Utah Consumer Privacy Act

On March 24, 2022, the Utah Consumer Privacy Act ("UCPA") was signed into law, making the UCPA the fourth comprehensive data privacy law passed in the United States.

The UCPA will take effect on December 31, 2023. The full text of the UCPA is provided below.

Please see the Comprehensive Data Privacy Law Quick Reference Guide for a high-level comparison of the requirements of the UCPA compared to other comprehensive data privacy laws.

UCPA Official Text:

Enrolled Copy **S.B. 227**

CONSUMER PRIVACY ACT

2022 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Kirk A. Cullimore

House Sponsor: Brady Brammer

LONG TITLE

General Description:

This bill enacts the Utah Consumer Privacy Act.

Highlighted Provisions:

This bill:

< defines terms;

< provides consumers the right to:

• access and delete certain personal data maintained by certain businesses; and

• opt out of the collection and use of personal data for certain purposes;

< requires certain businesses that control and process consumers' personal data to:

• safeguard consumers' personal data;

• provide clear information to consumers regarding how the consumers' personal data are used; and

• accept and comply with a consumer's request to exercise the consumer's rights under this bill;

< creates a right for a consumer to know what personal data a business collects, how

the business uses the personal data, and whether the business sells the personal data;

< upon request and subject to exceptions, requires a business to delete a consumer's personal data or stop selling the consumer's personal data;

< allows the Division of Consumer Protection to accept and investigate consumer complaints regarding the processing of personal data;

< authorizes the Office of the Attorney General to take enforcement action and impose penalties; and

< makes technical changes.

Money Appropriated in this Bill:

None

Other Special Clauses:

This bill provides a special effective date.

Utah Code Sections Affected:

AMENDS:

13-2-1, as last amended by Laws of Utah 2021, Chapter 266

ENACTS:

13-61-101, Utah Code Annotated 1953

13-61-102, Utah Code Annotated 1953

13-61-103, Utah Code Annotated 1953

13-61-201, Utah Code Annotated 1953

13-61-202, Utah Code Annotated 1953

13-61-203, Utah Code Annotated 1953

13-61-301, Utah Code Annotated 1953

13-61-302, Utah Code Annotated 1953

13-61-303, Utah Code Annotated 1953

13-61-304, Utah Code Annotated 1953

13-61-305, Utah Code Annotated 1953

13-61-401, Utah Code Annotated 1953

13-61-402, Utah Code Annotated 1953

13-61-403, Utah Code Annotated 1953

13-61-404, Utah Code Annotated 1953

Be it enacted by the Legislature of the state of Utah:

Section 1. Section **13-2-1** is amended to read:

13-2-1. Consumer protection division established -- Functions.

(1) There is established within the Department of Commerce the Division of Consumer Protection.

(2) The division shall administer and enforce the following:

(a) Chapter 5, Unfair Practices Act;

(b) Chapter 10a, Music Licensing Practices Act;

(c) Chapter 11, Utah Consumer Sales Practices Act;

(d) Chapter 15, Business Opportunity Disclosure Act;

(e) Chapter 20, New Motor Vehicle Warranties Act;

(f) Chapter 21, Credit Services Organizations Act;

(g) Chapter 22, Charitable Solicitations Act;

(h) Chapter 23, Health Spa Services Protection Act;

(i) Chapter 25a, Telephone and Facsimile Solicitation Act;

(j) Chapter 26, Telephone Fraud Prevention Act;

(k) Chapter 28, Prize Notices Regulation Act;

(l) Chapter 32a, Pawnshop and Secondhand Merchandise Transaction Information Act;

(m) Chapter 34, Utah Postsecondary Proprietary School Act;

(n) Chapter 34a, Utah Postsecondary School State Authorization Act;

(o) Chapter 41, Price Controls During Emergencies Act;

(p) Chapter 42, Uniform Debt-Management Services Act;

(q) Chapter 49, Immigration Consultants Registration Act;

(r) Chapter 51, Transportation Network Company Registration Act;

(s) Chapter 52, Residential Solar Energy Disclosure Act;

(t) Chapter 53, Residential, Vocational and Life Skills Program Act;

(u) Chapter 54, Ticket Website Sales Act;

(v) Chapter 56, Ticket Transferability Act; [and]

(w) Chapter 57, Maintenance Funding Practices Act[.]; and

(x) Chapter 61, Utah Consumer Privacy Act.

Section 2. Section 13-61-101 is enacted to read:

CHAPTER 61. UTAH CONSUMER PRIVACY ACT

Part 1. General Provisions

13-61-101. Definitions.

As used in this chapter:

(1) "Account" means the Consumer Privacy Restricted Account established in Section 13-61-403.

(2) "Affiliate" means an entity that:

(a) controls, is controlled by, or is under common control with another entity; or

(b) shares common branding with another entity.

(3) "Aggregated data" means information that relates to a group or category of consumers:

(a) from which individual consumer identities have been removed; and

(b) that is not linked or reasonably linkable to any consumer.

(4) "Air carrier" means the same as that term is defined in 49 U.S.C. Sec. 40102.

(5) "Authenticate" means to use reasonable means to determine that a consumer's request to exercise the rights described in Section 13-61-201 is made by the consumer who is entitled to exercise those rights.

(6) (a) "Biometric data" means data generated by automatic measurements of an individual's unique biological characteristics.

(b) "Biometric data" includes data described in Subsection (6)(a) that are generated by automatic measurements of an individual's fingerprint, voiceprint, eye retinas, irises, or any other unique biological pattern or characteristic that is used to identify a specific individual.

(c) "Biometric data" does not include:

(i) a physical or digital photograph;

(ii) a video or audio recording;

(iii) data generated from an item described in Subsection (6)(c)(i) or (ii);

(iv) information captured from a patient in a health care setting; or

(v) information collected, used, or stored for treatment, payment, or health care operations as those terms are defined in 45 C.F.R. Parts 160, 162, and 164.

(7) "Business associate" means the same as that term is defined in 45 C.F.R. Sec. 160.103.

(8) "Child" means an individual younger than 13 years old.

(9) "Consent" means an affirmative act by a consumer that unambiguously indicates the consumer's voluntary and informed agreement to allow a person to process personal data related to the consumer.

(10) (a) "Consumer" means an individual who is a resident of the state acting in an individual or household context.

(b) "Consumer" does not include an individual acting in an employment or commercial context.

(11) "Control" or "controlled" as used in Subsection (2) means:

(a) ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting securities of an entity;

(b) control in any manner over the election of a majority of the directors or of the individuals exercising similar functions; or

(c) the power to exercise controlling influence of the management of an entity.

(12) "Controller" means a person doing business in the state who determines the purposes for which and the means by which personal data are processed, regardless of whether the person makes the determination alone or with others.

(13) "Covered entity" means the same as that term is defined in 45 C.F.R. Sec. 160.103.

(14) "Deidentified data" means data that:

(a) cannot reasonably be linked to an identified individual or an identifiable individual; and

(b) are possessed by a controller who:

(i) takes reasonable measures to ensure that a person cannot associate the data with an individual;

(ii) publicly commits to maintain and use the data only in deidentified form and not attempt to reidentify the data; and

(iii) contractually obligates any recipients of the data to comply with the requirements described in Subsections (14)(b)(i) and (ii).

(15) "Director" means the director of the Division of Consumer Protection.

(16) "Division" means the Division of Consumer Protection created in Section 13-2-1.

(17) "Governmental entity" means the same as that term is defined in Section 63G-2-103.

(18) "Health care facility" means the same as that term is defined in Section 26-21-2.

(19) "Health care provider" means the same as that term is defined in Section 26-21-2.

(20) "Identifiable individual" means an individual who can be readily identified, directly or indirectly.

(21) "Institution of higher education" means a public or private institution of higher education.

(22) "Local political subdivision" means the same as that term is defined in Section 11-14-102.

(23) "Nonprofit corporation" means:

(a) the same as that term is defined in Section 16-6a-102; or

(b) a foreign nonprofit corporation as defined in Section 16-6a-102.

(24) (a) "Personal data" means information that is linked or reasonably linkable to an identified individual or an identifiable individual.

(b) "Personal data" does not include deidentified data, aggregated data, or publicly available information.

(25) "Process" means an operation or set of operations performed on personal data, including collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(26) "Processor" means a person who processes personal data on behalf of a controller.

(27) "Protected health information" means the same as that term is defined in 45 C.F.R. Sec. 160.103.

(28) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, if the additional information is:

(a) kept separate from the consumer's personal data; and

(b) subject to appropriate technical and organizational measures to ensure that the personal data are not attributable to an identified individual or an identifiable individual.

(29) "Publicly available information" means information that a person:

(a) lawfully obtains from a record of a governmental entity;

(b) reasonably believes a consumer or widely distributed media has lawfully made available to the general public; or

(c) if the consumer has not restricted the information to a specific audience, obtains from a person to whom the consumer disclosed the information.

(30) "Right" means a consumer right described in Section 13-61-201.

(31) (a) "Sale," "sell," or "sold" means the exchange of personal data for monetary consideration by a controller to a third party.

(b) "Sale," "sell," or "sold" does not include:

(i) a controller's disclosure of personal data to a processor who processes the personal data on behalf of the controller;

(ii) a controller's disclosure of personal data to an affiliate of the controller;

(iii) considering the context in which the consumer provided the personal data to the controller, a controller's disclosure of personal data to a third party if the purpose is consistent with a consumer's reasonable expectations;

(iv) the disclosure or transfer of personal data when a consumer directs a controller to:

(A) disclose the personal data; or

(B) interact with one or more third parties;

(v) a consumer's disclosure of personal data to a third party for the purpose of providing a product or service requested by the consumer or a parent or legal guardian of a

child;

(vi) the disclosure of information that the consumer:

(A) intentionally makes available to the general public via a channel of mass media; and

(B) does not restrict to a specific audience; or

(vii) a controller's transfer of personal data to a third party as an asset that is part of a proposed or actual merger, an acquisition, or a bankruptcy in which the third party assumes control of all or part of the controller's assets.

(32) (a) "Sensitive data" means:

(i) personal data that reveals:

(A) an individual's racial or ethnic origin;

(B) an individual's religious beliefs;

(C) an individual's sexual orientation;

(D) an individual's citizenship or immigration status; or

(E) information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional;

(ii) the processing of genetic personal data or biometric data, if the processing is for the purpose of identifying a specific individual; or

(iii) specific geolocation data.

(b) "Sensitive data" does not include personal data that reveals an individual's:

(i) racial or ethnic origin, if the personal data are processed by a video communication service; or

(ii) if the personal data are processed by a person licensed to provide health care under Title 26, Chapter 21, Health Care Facility Licensing and Inspection Act, or Title 58, Occupations and Professions, information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional.

(33) (a) "Specific geolocation data" means information derived from technology, including global position system level latitude and longitude coordinates, that directly identifies an individual's specific location, accurate within a radius of 1,750 feet or less

(b) "Specific geolocation data" does not include:

(i) the content of a communication; or

(ii) any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(34) (a) "Targeted advertising" means displaying an advertisement to a consumer where the advertisement is selected based on personal data obtained from the consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests.

(b) "Targeted advertising" does not include advertising:

(i) based on a consumer's activities within a controller's website or online application or any affiliated website or online application;

(ii) based on the context of a consumer's current search query or visit to a website or online application;

(iii) directed to a consumer in response to the consumer's request for information, product, a service, or feedback; or

(iv) processing personal data solely to measure or report advertising:

(A) performance;

(B) reach; or

(C) frequency.

(35) "Third party" means a person other than:

(a) the consumer, controller, or processor; or

(b) an affiliate or contractor of the controller or the processor.

(36) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(a) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from the information's disclosure or use; and

(b) is the subject of efforts that are reasonable under the circumstances to maintain the information's secrecy.

Section 3. Section **13-61-102** is enacted to read:

13-61-102. Applicability.

(1) This chapter applies to any controller or processor who:

(a) (i) conducts business in the state; or

(ii) produces a product or service that is targeted to consumers who are residents of the state;

(b) has annual revenue of $25,000,000 or more; and

(c) satisfies one or more of the following thresholds:

(i) during a calendar year, controls or processes personal data of 100,000 or more consumers; or

(ii) derives over 50% of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers.

(2) This chapter does not apply to:

(a) a governmental entity or a third party under contract with a governmental entity when the third party is acting on behalf of the governmental entity;

(b) a tribe;

(c) an institution of higher education;

(d) a nonprofit corporation;

(e) a covered entity;

(f) a business associate;

(g) information that meets the definition of:

(i) protected health information for purposes of the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. Sec. 1320d et seq., and related regulations;

(ii) patient identifying information for purposes of 42 C.F.R. Part 2;

(iii) identifiable private information for purposes of the Federal Policy for the Protection of Human Subjects, 45 C.F.R. Part 46;

(iv) identifiable private information or personal data collected as part of human subjects research pursuant to or under the same standards as:

(A) the good clinical practice guidelines issued by the International Council for

Harmonisation; or

(B) the Protection of Human Subjects under 21 C.F.R. Part 50 and Institutional Review Boards under 21 C.F.R. Part 56;

(v) personal data used or shared in research conducted in accordance with one or more of the requirements described in Subsection (2)(g)(iv);

(vi) information and documents created specifically for, and collected and maintained by, a committee listed in Section 26-1-7;

(vii) information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, 42 U.S.C. Sec. 11101 et seq., and related regulations;

(viii) patient safety work product for purposes of 42 C.F.R. Part 3; or

(ix) information that is:

(A) deidentified in accordance with the requirements for deidentification set forth in 45 C.F.R. Part 164; and

(B) derived from any of the health care-related information listed in this Subsection (2)(g);

(h) information originating from, and intermingled to be indistinguishable with, information under Subsection (2)(g) that is maintained by:

(i) a health care facility or health care provider; or

(ii) a program or a qualified service organization as defined in 42 C.F.R. Sec. 2.11;

(i) information used only for public health activities and purposes as described in 45 C.F.R. Sec. 164.512;

(j) (i) an activity by:

(A) a consumer reporting agency, as defined in 15 U.S.C. Sec. 1681a;

(B) a furnisher of information, as set forth in 15 U.S.C. Sec. 1681s-2, who provides information for use in a consumer report, as defined in 15 U.S.C. Sec. 1681a; or

(C) a user of a consumer report, as set forth in 15 U.S.C. Sec. 1681b;

(ii) subject to regulation under the federal Fair Credit Reporting Act, 15 U.S.C. Sec. 1681 et seq.; and

(iii) involving the collection, maintenance, disclosure, sale, communication, or use of

any personal data bearing on a consumer's:

(A) credit worthiness;

(B) credit standing;

(C) credit capacity;

(D) character;

(E) general reputation;

(F) personal characteristics; or

(G) mode of living;

(k) a financial institution or an affiliate of a financial institution governed by, or personal data collected, processed, sold, or disclosed in accordance with, Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. Sec. 6801 et seq., and related regulations;

(l) personal data collected, processed, sold, or disclosed in accordance with the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. Sec. 2721 et seq.;

(m) personal data regulated by the federal Family Education Rights and Privacy Act, 20 U.S.C. Sec. 1232g, and related regulations;

(n) personal data collected, processed, sold, or disclosed in accordance with the federal Farm Credit Act of 1971, 12 U.S.C. Sec. 2001 et seq.;

(o) data that are processed or maintained:

(i) in the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent the collection and use of the data are related to the individual's role;

(ii) as the emergency contact information of an individual described in Subsection (2)(o)(i) and used for emergency contact purposes; or

(iii) to administer benefits for another individual relating to an individual described in Subsection (2)(o)(i) and used for the purpose of administering the benefits;

(p) an individual's processing of personal data for purely personal or household purposes; or

(q) an air carrier.

(3) A controller is in compliance with any obligation to obtain parental consent under

this chapter if the controller complies with the verifiable parental consent mechanisms under the Children's Online Privacy Protection Act, 15 U.S.C. Sec. 6501 et seq., and the act's implementing regulations and exemptions.

(4) This chapter does not require a person to take any action in conflict with the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. Sec. 1320d et seq., or related regulations.

Section 4. Section **13-61-103** is enacted to read:

13-61-103. Preemption -- Reference to other laws.

(1) This chapter supersedes and preempts any ordinance, resolution, rule, or other regulation adopted by a local political subdivision regarding the processing of personal data by a controller or processor.

(2) Any reference to federal law in this chapter includes any rules or regulations promulgated under the federal law.

Section 5. Section **13-61-201** is enacted to read:

Part 2. Rights Relating to Personal Data

13-61-201. Consumer rights -- Access -- Deletion -- Portability -- Opt out of certain processing.

(1) A consumer has the right to:

(a) confirm whether a controller is processing the consumer's personal data; and

(b) access the consumer's personal data.

(2) A consumer has the right to delete the consumer's personal data that the consumer provided to the controller.

(3) A consumer has the right to obtain a copy of the consumer's personal data, that the consumer previously provided to the controller, in a format that:

(a) to the extent technically feasible, is portable;

(b) to the extent practicable, is readily usable; and

(c) allows the consumer to transmit the data to another controller without impediment, where the processing is carried out by automated means.

(4) A consumer has the right to opt out of the processing of the consumer's personal

data for purposes of:

(a) targeted advertising; or

(b) the sale of personal data.

(5) Nothing in this section requires a person to cause a breach of security system as defined in Section 13-44-102.

Section 6. Section **13-61-202** is enacted to read:

13-61-202. Exercising consumer rights.

(1) A consumer may exercise a right by submitting a request to a controller, by means prescribed by the controller, specifying the right the consumer intends to exercise.

(2) In the case of processing personal data concerning a known child, the parent or legal guardian of the known child shall exercise a right on the child's behalf.

(3) In the case of processing personal data concerning a consumer subject to guardianship, conservatorship, or other protective arrangement under Title 75, Chapter 5, Protection of Persons Under Disability and Their Property, the guardian or the conservator of the consumer shall exercise a right on the consumer's behalf.

Section 7. Section **13-61-203** is enacted to read:

13-61-203. Controller's response to requests.

(1) Subject to the other provisions of this chapter, a controller shall comply with a consumer's request under Section 13-61-202 to exercise a right.

(2) (a) Within 45 days after the day on which a controller receives a request to exercise a right, the controller shall:

(i) take action on the consumer's request; and

(ii) inform the consumer of any action taken on the consumer's request.

(b) The controller may extend once the initial 45-day period by an additional 45 days if reasonably necessary due to the complexity of the request or the volume of the requests received by the controller.

(c) If a controller extends the initial 45-day period, before the initial 45-day period expires, the controller shall:

(i) inform the consumer of the extension, including the length of the extension; and

(ii) provide the reasons the extension is reasonably necessary as described in Subsection (2)(b).

(d) The 45-day period does not apply if the controller reasonably suspects the consumer's request is fraudulent and the controller is not able to authenticate the request before the 45-day period expires.

(3) If, in accordance with this section, a controller chooses not to take action on a consumer's request, the controller shall within 45 days after the day on which the controller receives the request, inform the consumer of the reasons for not taking action.

(4) (a) A controller may not charge a fee for information in response to a request, unless the request is the consumer's second or subsequent request during the same 12-month period.

(b) (i) Notwithstanding Subsection (4)(a), a controller may charge a reasonable fee to cover the administrative costs of complying with a request or refuse to act on a request, if:

(A) the request is excessive, repetitive, technically infeasible, or manifestly unfounded;

(B) the controller reasonably believes the primary purpose in submitting the request was something other than exercising a right; or

(C) the request, individually or as part of an organized effort, harasses, disrupts, or imposes undue burden on the resources of the controller's business.

(ii) A controller that charges a fee or refuses to act in accordance with this Subsection (4)(b) bears the burden of demonstrating the request satisfied one or more of the criteria described in Subsection (4)(b)(i).

(5) If a controller is unable to authenticate a consumer request to exercise a right described in Section 13-61-201 using commercially reasonable efforts, the controller:

(a) is not required to comply with the request; and

(b) may request that the consumer provide additional information reasonably necessary to authenticate the request.

Section 8. Section **13-61-301** is enacted to read:

Part 3. Requirements for Controllers and Processors

13-61-301. Responsibility according to role.

(1) A processor shall:

(a) adhere to the controller's instructions; and

(b) taking into account the nature of the processing and information available to the processor, by appropriate technical and organizational measures, insofar as reasonably practicable, assist the controller in meeting the controller's obligations, including obligations related to the security of processing personal data and notification of a breach of security system described in Section 13-44-202.

(2) Before a processor performs processing on behalf of a controller, the processor and controller shall enter into a contract that:

(a) clearly sets forth instructions for processing personal data, the nature and purpose of the processing, the type of data subject to processing, the duration of the processing, and the parties' rights and obligations;

(b) requires the processor to ensure each person processing personal data is subject to a duty of confidentiality with respect to the personal data; and

(c) requires the processor to engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the same obligations as the processor with respect to the personal data.

(3) (a) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data are to be processed.

(b) A processor that adheres to a controller's instructions with respect to a specific processing of personal data remains a processor.

Section 9. Section **13-61-302** is enacted to read:

13-61-302. Responsibilities of controllers -- Transparency -- Purpose specification and data minimization -- Consent for secondary use -- Security -- Nondiscrimination -- Nonretaliation -- Nonwaiver of consumer rights.

(1) (a) A controller shall provide consumers with a reasonably accessible and clear privacy notice that includes:

(i) the categories of personal data processed by the controller;

(ii) the purposes for which the categories of personal data are processed;

(iii) how consumers may exercise a right;

(iv) the categories of personal data that the controller shares with third parties, if any; and

(v) the categories of third parties, if any, with whom the controller shares personal data.

(b) If a controller sells a consumer's personal data to one or more third parties or engages in targeted advertising, the controller shall clearly and conspicuously disclose to the consumer the manner in which the consumer may exercise the right to opt out of the:

(i) sale of the consumer's personal data; or

(ii) processing for targeted advertising.

(2) (a) A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices designed to:

(i) protect the confidentiality and integrity of personal data; and

(ii) reduce reasonably foreseeable risks of harm to consumers relating to the processing of personal data.

(b) Considering the controller's business size, scope, and type, a controller shall use data security practices that are appropriate for the volume and nature of the personal data at issue.

(3) Except as otherwise provided in this chapter, a controller may not process sensitive data collected from a consumer without:

(a) first presenting the consumer with clear notice and an opportunity to opt out of the processing; or

(b) in the case of the processing of personal data concerning a known child, processing the data in accordance with the federal Children's Online Privacy Protection Act, 15 U.S.C. Sec. 6501 et seq., and the act's implementing regulations and exemptions.

(4) (a) A controller may not discriminate against a consumer for exercising a right by:

(i) denying a good or service to the consumer;

(ii) charging the consumer a different price or rate for a good or service; or

(iii) providing the consumer a different level of quality of a good or service.

(b) This Subsection (4) does not prohibit a controller from offering a different price, rate, level, quality, or selection of a good or service to a consumer, including offering a good or service for no fee or at a discount, if:

(i) the consumer has opted out of targeted advertising; or

(ii) the offer is related to the consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(5) A controller is not required to provide a product, service, or functionality to a consumer if:

(a) the consumer's personal data are or the processing of the consumer's personal data is reasonably necessary for the controller to provide the consumer the product, service, or functionality; and

(b) the consumer does not:

(i) provide the consumer's personal data to the controller; or

(ii) allow the controller to process the consumer's personal data.

(6) Any provision of a contract that purports to waive or limit a consumer's right under this chapter is void.

Section 10. Section **13-61-303** is enacted to read:

13-61-303. Processing deidentified data or pseudonymous data.

(1) The provisions of this chapter do not require a controller or processor to:

(a) reidentify deidentified data or pseudonymous data;

(b) maintain data in identifiable form or obtain, retain, or access any data or technology for the purpose of allowing the controller or processor to associate a consumer request with personal data; or

(c) comply with an authenticated consumer request to exercise a right described in Subsections 13-61-202(1) through (3), if:

(i) (A) the controller is not reasonably capable of associating the request with the personal data; or

(B) it would be unreasonably burdensome for the controller to associate the request with the personal data;

(ii) the controller does not:

(A) use the personal data to recognize or respond to the consumer who is the subject of the personal data; or

(B) associate the personal data with other personal data about the consumer; and

(iii) the controller does not sell or otherwise disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

(2) The rights described in Subsections 13-61-201(1) through (3) do not apply to pseudonymous data if a controller demonstrates that any information necessary to identify a consumer is kept:

(a) separately; and

(b) subject to appropriate technical and organizational measures to ensure the personal data are not attributed to an identified individual or an identifiable individual.

(3) A controller who uses pseudonymous data or deidentified data shall take reasonable steps to ensure the controller:

(a) complies with any contractual obligations to which the pseudonymous data or deidentified data are subject; and

(b) promptly addresses any breach of a contractual obligation described in Subsection (3)(a).

Section 11. Section **13-61-304** is enacted to read:

13-61-304. Limitations.

(1) The requirements described in this chapter do not restrict a controller's or processor's ability to:

(a) comply with a federal, state, or local law, rule, or regulation;

(b) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, local, or other governmental entity;

(c) cooperate with a law enforcement agency concerning activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;

(d) investigate, establish, exercise, prepare for, or defend a legal claim;

(e) provide a product or service requested by a consumer or a parent or legal guardian of a child;

(f) perform a contract to which the consumer or the parent or legal guardian of a child is a party, including fulfilling the terms of a written warranty or taking steps at the request of the consumer or parent or legal guardian before entering into the contract with the consumer;

(g) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual;

(h) (i) detect, prevent, protect against, or respond to a security incident, identity theft, fraud, harassment, malicious or deceptive activity, or any illegal activity; or

(ii) investigate, report, or prosecute a person responsible for an action described inSubsection (1)(h)(i);

(i) (i) preserve the integrity or security of systems; or

(ii) investigate, report, or prosecute a person responsible for harming or threatening the integrity or security of systems, as applicable;

(j) if the controller discloses the processing in a notice described in Section 13-61-302, engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws;

(k) assist another person with an obligation described in this subsection;

(l) process personal data to:

(i) conduct internal analytics or other research to develop, improve, or repair a controller's or processor's product, service, or technology;

(ii) identify and repair technical errors that impair existing or intended functionality; or

(iii) effectuate a product recall;

(m) process personal data to perform an internal operation that is:

(i) reasonably aligned with the consumer's expectations based on the consumer's existing relationship with the controller; or

(ii) otherwise compatible with processing to aid the controller or processor in providing a product or service specifically requested by a consumer or a parent or legal guardian of a child or the performance of a contract to which the consumer or a parent or legal guardian of a child is a party; or

(n) retain a consumer's email address to comply with the consumer's request to exercise a right.

(2) This chapter does not apply if a controller's or processor's compliance with this chapter:

(a) violates an evidentiary privilege under Utah law;

(b) as part of a privileged communication, prevents a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Utah law; or

(c) adversely affects the privacy or other rights of any person.

(3) A controller or processor is not in violation of this chapter if:

(a) the controller or processor discloses personal data to a third party controller or processor in compliance with this chapter;

(b) the third party processes the personal data in violation of this chapter; and

(c) the disclosing controller or processor did not have actual knowledge of the third party's intent to commit a violation of this chapter.

(4) If a controller processes personal data under an exemption described in Subsection (1), the controller bears the burden of demonstrating that the processing qualifies for the exemption.

(5) Nothing in this chapter requires a controller, processor, third party, or consumer to disclose a trade secret.

Section 12. Section **13-61-305** is enacted to read:

13-61-305. No private cause of action.

A violation of this chapter does not provide a basis for, nor is a violation of this chapter subject to, a private right of action under this chapter or any other law.

Section 13. Section **13-61-401** is enacted to read:

Part 4. Enforcement

13-61-401. Investigative powers of division.

(1) The division shall establish and administer a system to receive consumer complaints regarding a controller's or processor's alleged violation of this chapter.

(2) (a) The division may investigate a consumer complaint to determine whether the controller or processor violated or is violating this chapter.

(b) If the director has reasonable cause to believe that substantial evidence exists that a person identified in a consumer complaint is in violation of this chapter, the director shall refer the matter to the attorney general.

(c) Upon request, the division shall provide consultation and assistance to the attorney general in enforcing this chapter.

Section 14. Section **13-61-402** is enacted to read:

13-61-402. Enforcement powers of the attorney general.

(1) The attorney general has the exclusive authority to enforce this chapter.

(2) Upon referral from the division, the attorney general may initiate an enforcement action against a controller or processor for a violation of this chapter.

(3) (a) At least 30 days before the day on which the attorney general initiates an enforcement action against a controller or processor, the attorney general shall provide the controller or processor:

(i) written notice identifying each provision of this chapter the attorney general alleges the controller or processor has violated or is violating; and

(ii) an explanation of the basis for each allegation.

(b) The attorney general may not initiate an action if the controller or processor:

(i) cures the noticed violation within 30 days after the day on which the controller or processor receives the written notice described in Subsection (3)(a); and

(ii) provides the attorney general an express written statement that:

(A) the violation has been cured; and

(B) no further violation of the cured violation will occur.

(c) The attorney general may initiate an action against a controller or processor who:

(i) fails to cure a violation after receiving the notice described in Subsection (3)(a); or

(ii) after curing a noticed violation and providing a written statement in accordance with Subsection (3)(b), continues to violate this chapter.

(d) In an action described in Subsection (3)(c), the attorney general may recover:

(i) actual damages to the consumer; and

(ii) for each violation described in Subsection (3)(c), an amount not to exceed $7,500.

(4) All money received from an action under this chapter shall be deposited into the Consumer Privacy Account established in Section 13-61-403.

(5) If more than one controller or processor are involved in the same processing in violation of this chapter, the liability for the violation shall be allocated among the controllers or processors according to the principles of comparative fault.

Section 15. Section **13-61-403** is enacted to read:

13-61-403. Consumer Privacy Restricted Account.

(1) There is created a restricted account known as the "Consumer Privacy Account."

(2) The account shall be funded by money received through civil enforcement actions under this chapter.

(3) Upon appropriation, the division or the attorney general may use money deposited into the account for:

(a) investigation and administrative costs incurred by the division in investigating consumer complaints alleging violations of this chapter;

(b) recovery of costs and attorney fees accrued by the attorney general in enforcing this chapter; and

(c) providing consumer and business education regarding:

(i) consumer rights under this chapter; and

(ii) compliance with the provisions of this chapter for controllers and processors.

(4) If the balance in the account exceeds $4,000,000 at the close of any fiscal year, the Division of Finance shall transfer the amount that exceeds $4,000,000 into the General Fund.

Section 16. Section **13-61-404** is enacted to read:

13-61-404. Attorney general report.

(1) The attorney general and the division shall compile a report:

(a) evaluating the liability and enforcement provisions of this chapter, including the effectiveness of the attorney general's and the division's efforts to enforce this chapter; and

(b) summarizing the data protected and not protected by this chapter including, with reasonable detail, a list of the types of information that are publicly available from local, state,

and federal government sources.

(2) The attorney general and the division may update the report as new information becomes available.

(3) The attorney general and the division shall submit the report to the Business and Labor Interim Committee before July 1, 2025.

Section 17. **Effective date.**
This bill takes effect on December 31, 2023.

.

Vermont Consumer Data Protection Act

Vermont requires “data brokers” to register with the Vermont Secretary of State and meet certain data security standards. A company acts as a “data broker” if the company collects and sells the information of Vermont consumers with whom the company does not have a direct relationship. Examples of direct relationships (i.e., relationships that do not trigger the law’s applicability) include past or present customers, clients, subscribers, users, registered users, employees, contractors, agents, investors, and donors.

The law also provides substantive exceptions, such as for:

1. developing or maintaining third-party e-commerce or application platforms;

2. providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier;

3. providing publicly available information related to a consumer’s business or profession; or

4. providing publicly available information via real-time or near real-time alert services for health or safety purposes.

The full text of Vermont’s data broker law is accessible at https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+CHAP0035.

KILPATRICK TOWNSEND

Virginia Consumer Data Protection Act

Virginia became the second U.S. state to have a comprehensive, general consumer privacy law when the Consumer Data Protection Act ("CDPA") was signed into law on March 2, 2021.

The CDPA takes effect on January 1, 2023, matching the effective date of the California Privacy Rights Act ("CPRA"). The full text of the CDPA is provided below.

Please see the Comprehensive Data Privacy Law Quick Reference Guide for a high-level comparison of the requirements of the CDPA compared to other comprehensive data privacy laws.

CDPA Official Text:

CHAPTER 35

An Act to amend the Code of Virginia by adding in Title 59.1 a chapter numbered 52, consisting of sections numbered 59.1-571 through 59.1-581, relating to Consumer Data Protection Act.

[H 2307]

Approved March 2, 2021

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding in Title 59.1 a chapter numbered 52, consisting of sections numbered 59.1-571 through 59.1-581, as follows:

CHAPTER 52.

CONSUMER DATA PROTECTION ACT.

§ 59.1-571. Definitions.

As used in this chapter, unless the context requires a different meaning:

"Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. For the purposes of this definition, "control" or "controlled" means (i) ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company; (ii) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or (iii) the power to exercise controlling influence over the management of a company.

"Authenticate" means verifying through reasonable means that the consumer, entitled to exercise his consumer rights in § 59.1-573, is the same consumer exercising such consumer rights with respect to the personal data at issue.

"Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. "Biometric data" does not include a physical or

digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

"Business associate" means the same meaning as the term established by HIPAA.

"Child" means any natural person younger than 13 years of age.

"Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

"Consumer" means a natural person who is a resident of the Commonwealth acting only in an individual or household context. It does not include a natural person acting in a commercial or employment context.

"Controller" means the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data.

"Covered entity" means the same as the term is established by HIPAA.

"Decisions that produce legal or similarly significant effects concerning a consumer" means a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water.

"De-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person. A controller that possesses "de-identified data" shall comply with the requirements of subsection A of § 59.1-577.

"Fund" means the Consumer Privacy Fund established pursuant to § 59.1-581.

"Health record" means the same as that term is defined in § 32.1-127.1:03.

"Health care provider" means the same as that term is defined in § 32.1-276.3.

"HIPAA" means the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d et seq.).

"Identified or identifiable natural person" means a person who can be readily identified, directly or indirectly.

"Institution of higher education" means a public institution and private institution of higher education, as those terms are defined in § 23.1-100.

"Nonprofit organization" means any corporation organized under the Virginia Nonstock Corporation Act (§ 13.1-801 et seq.) or any organization exempt from taxation under § 501(c)(3), 501(c)(6), or 501 (c)(12) of the Internal Revenue Code, and any subsidiaries and affiliates of entities organized pursuant to Chapter 9.1 (§ 56-231.15 et seq.) of Title 56.

"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include de-identified data or publicly available information.

"Precise geolocation data" means information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a natural person with precision and accuracy within a radius of 1,750 feet. "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

"Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

"Processor" means a natural or legal entity that processes personal data on behalf of a controller.

"Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

"Protected health information" means the same as the term is established by HIPAA.

"Pseudonymous data" means personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

"Publicly available information" means information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

"Sale of personal data" means the exchange of personal data for monetary consideration by the controller to a third party. "Sale of personal data" does not include:

1. The disclosure of personal data to a processor that processes the personal data on behalf of the controller;

2. The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;

3. The disclosure or transfer of personal data to an affiliate of the controller;

4. The disclosure of information that the consumer (i) intentionally made available to the general public via a channel of mass media and (ii) did not restrict to a specific audience; or

5. The disclosure or transfer of personal data to a third party 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 controller's assets.

"Sensitive data" means a category of personal data that includes:

1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;

2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;

3. The personal data collected from a known child; or

4. Precise geolocation data.

"State agency" means the same as that term is defined in § 2.2-307.

"Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. "Targeted advertising" does not include:

1. Advertisements based on activities within a controller's own websites or online applications;

2. Advertisements based on the context of a consumer's current search query, visit to a website, or online application;

3. Advertisements directed to a consumer in response to the consumer's request for information or feedback; or

4. Processing personal data processed solely for measuring or reporting advertising performance, reach, or frequency.

"Third party" means a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller.

§ 59.1-572. Scope; exemptions.

A. This chapter applies to persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that (i) during a calendar year, control or process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data.

B. This chapter shall not apply to any (i) body, authority, board, bureau, commission, district, or agency of the Commonwealth or of any political subdivision of the Commonwealth; (ii) financial institution or data subject to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.); (iii) covered entity or business associate governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and the Health Information Technology for Economic and Clinical Health Act (P.L. 111-5); (iv) nonprofit organization; or (v) institution of higher education.

C. The following information and data is exempt from this chapter:

1. Protected health information under HIPAA;

2. Health records for purposes of Title 32.1;

3. Patient identifying information for purposes of 42 U.S.C. § 290dd-2;

4. Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. Part 46; identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use; the protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, or personal data used or shared in research conducted in accordance with the requirements set forth in this chapter, or other research conducted in accordance with applicable law;

5. Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986 (42 U.S.C. § 11101 et seq.);

6. Patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act (42 U.S.C. § 299b-21 et seq.);

7. Information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;

8. Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as information exempt under this subsection that is maintained by a covered entity or business associate as defined by HIPAA or a program or a qualified service organization as defined by 42 U.S.C. § 290dd-2;

9. Information used only for public health activities and purposes as authorized by HIPAA;

10. The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);

11. Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721 et seq.);

12. Personal data regulated by the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g et seq.);

13. Personal data collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act (12 U.S.C. § 2001 et seq.); and

14. Data processed or maintained (i) in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected

and used within the context of that role; (ii) as the emergency contact information of an individual under this chapter used for emergency contact purposes; or (iii) that is necessary to retain to administer benefits for another individual relating to the individual under clause (i) and used for the purposes of administering those benefits.

D. Controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) shall be deemed compliant with any obligation to obtain parental consent under this chapter.

§ 59.1-573. Personal data rights; consumers.

A. A consumer may invoke the consumer rights authorized pursuant to this subsection at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke such consumer rights on behalf of the child regarding processing personal data belonging to the known child. A controller shall comply with an authenticated consumer request to exercise the right:

1. To confirm whether or not a controller is processing the consumer's personal data and to access such personal data;

2. To correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

3. To delete personal data provided by or obtained about the consumer;

4. To obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means; and

5. To opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

B. Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to subsection A as follows:

1. A controller shall respond to the consumer without undue delay, but in all cases within 45 days of receipt of the request submitted pursuant to the methods described in § 59.1-573 A. The response period may be extended once by 45 additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of any such extension within the initial 45-day response period, together with the reason for the extension.

2. If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but in all cases and at the latest within 45 days of receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision pursuant to subsection C.

3. Information provided in response to a consumer request shall be provided by a controller free of charge, up to twice annually per consumer. If requests from a consumer are manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.

4. If a controller is unable to authenticate the request using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action under subsection A and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request.

C. A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision pursuant to subdivision B 2. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to subsection A. Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

§ 59.1-574. Data controller responsibilities; transparency.

A. A controller shall:

1. Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer;

2. Except as otherwise provided in this chapter, not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;

3. Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. Such data security practices shall be appropriate to the volume and nature of the personal data at issue;

4. Not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer. However, nothing in this subdivision shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised his right to opt out pursuant to § 59.1-573 or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program; and

5. Not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.).

B. Any provision of a contract or agreement of any kind that purports to waive or limit in any way consumer rights pursuant to § 59.1-573 shall be deemed contrary to public policy and shall be void and unenforceable.

C. Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

1. The categories of personal data processed by the controller;

2. The purpose for processing personal data;

3. How consumers may exercise their consumer rights pursuant § 59.1-573, including how a consumer may appeal a controller's decision with regard to the consumer's request;

4. The categories of personal data that the controller shares with third parties, if any; and

5. The categories of third parties, if any, with whom the controller shares personal data.

D. If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing.

E. A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights under this chapter. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the identity of the consumer making the request. Controllers shall not require a consumer to create a new account in order to exercise consumer rights pursuant to § 59.1-573 but may require a consumer to use an existing account.

§ 59.1-575. Responsibility according to role; controller and processor.

A. A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under this chapter. Such assistance shall include:

1. Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as this is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests pursuant to § 59.1-573.

2. Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of the system of the processor pursuant to § 18.2-186.6 in order to meet the controller's obligations.

3. Providing necessary information to enable the controller to conduct and document data protection assessments pursuant to § 59.1-576.

B. A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The contract shall also include requirements that the processor shall:

1. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

2. At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

3. Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter;

4. Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request; and

5. Engage any subcontractor pursuant to a written contract in accordance with subsection C that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

C. Nothing in this section shall be construed to relieve a controller or a processor from the liabilities imposed on it by virtue of its role in the processing relationship as defined by this chapter.

D. Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

§ 59.1-576. Data protection assessments.

A. A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

1. The processing of personal data for purposes of targeted advertising;

2. The sale of personal data;

3. The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers;

4. The processing of sensitive data; and

5. Any processing activities involving personal data that present a heightened risk of harm to consumers.

B. Data protection assessments conducted pursuant to subsection A shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller.

C. The Attorney General may request, pursuant to a civil investigative demand, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in § 59.1-574. Data protection assessments shall be confidential and exempt from public inspection and copying under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.). The disclosure of a data protection assessment pursuant to a request from the Attorney General shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

D. A single data protection assessment may address a comparable set of processing operations that include similar activities.

E. Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may comply under this section if the assessments have a reasonably comparable scope and effect.

F. Data protection assessment requirements shall apply to processing activities created or generated after January 1, 2023, and are not retroactive.

§ 59.1-577. Processing de-identified data; exemptions.

A. The controller in possession of de-identified data shall:

1. Take reasonable measures to ensure that the data cannot be associated with a natural person;

2. Publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and

3. Contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter.

B. Nothing in this chapter shall be construed to (i) require a controller or processor to re-identify de-identified data or pseudonymous data or (ii) maintain data in identifiable form, or collect, obtain, retain, or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

C. Nothing in this chapter shall be construed to require a controller or processor to comply with an authenticated consumer rights request, pursuant to § 59.1-573, if all of the following are true:

1. The controller is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;

2. The controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and

3. The controller does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.

D. The consumer rights contained in subdivisions A 1 through 4 of § 59.1-573 and § 59.1-574 shall not apply to pseudonymous data in cases where the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.

E. A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

§ 59.1-578. Limitations.

A. Nothing in this chapter shall be construed to restrict a controller's or processor's ability to:

1. Comply with federal, state, or local laws, rules, or regulations;

2. Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

3. Cooperate with law-enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;

4. Investigate, establish, exercise, prepare for, or defend legal claims;

5. Provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer prior to entering into a contract;

6. Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

7. Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action;

8. Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, or similar independent oversight entities that determine: (i) if the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller; (ii) the expected benefits of the

research outweigh the privacy risks; and (iii) if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or

9. Assist another controller, processor, or third party with any of the obligations under this subsection.

B. The obligations imposed on controllers or processors under this chapter shall not restrict a controller's or processor's ability to collect, use, or retain data to:

1. Conduct internal research to develop, improve, or repair products, services, or technology;

2. Effectuate a product recall;

3. Identify and repair technical errors that impair existing or intended functionality; or

4. Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

C. The obligations imposed on controllers or processors under this chapter shall not apply where compliance by the controller or processor with this chapter would violate an evidentiary privilege under the laws of the Commonwealth. Nothing in this chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the Commonwealth as part of a privileged communication.

D. A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirements of this chapter, is not in violation of this chapter if the third-party controller or processor that receives and processes such personal data is in violation of this chapter, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this chapter is likewise not in violation of this chapter for the transgressions of the controller or processor from which it receives such personal data.

E. Nothing in this chapter shall be construed as an obligation imposed on controllers and processors that adversely affects the rights or freedoms of any persons, such as exercising the right of free speech pursuant to the First Amendment to the United States Constitution, or applies to the processing of personal data by a person in the course of a purely personal or household activity.

F. Personal data processed by a controller pursuant to this section shall not be processed for any purpose other than those expressly listed in this section unless otherwise allowed by this chapter. Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is:

1. Reasonably necessary and proportionate to the purposes listed in this section; and

2. Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used, or retained pursuant to subsection B shall, where applicable, take into account the nature and purpose or purposes of such collection, use, or retention. Such data shall be subject to

reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use, or retention of personal data.

G. If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsection F.

H. Processing personal data for the purposes expressly identified in subdivisions A 1 through 9 shall not solely make an entity a controller with respect to such processing.

§ 59.1-579. Investigative authority.

Whenever the Attorney General has reasonable cause to believe that any person has engaged in, is engaging in, or is about to engage in any violation of this chapter, the Attorney General is empowered to issue a civil investigative demand. The provisions of § 59.1-9.10 shall apply mutatis mutandis to civil investigative demands issued under this section.

§ 59.1-580. Enforcement; civil penalty; expenses.

A. The Attorney General shall have exclusive authority to enforce the provisions of this chapter.

B. Prior to initiating any action under this chapter, the Attorney General shall provide a controller or processor 30 days' written notice identifying the specific provisions of this chapter the Attorney General alleges have been or are being violated. If within the 30-day period, the controller or processor cures the noticed violation and provides the Attorney General an express written statement that the alleged violations have been cured and that no further violations shall occur, no action shall be initiated against the controller or processor.

C. If a controller or processor continues to violate this chapter following the cure period in subsection B or breaches an express written statement provided to the Attorney General under that subsection, the Attorney General may initiate an action in the name of the Commonwealth and may seek an injunction to restrain any violations of this chapter and civil penalties of up to $7,500 for each violation under this chapter.

D. The Attorney General may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees, in any action initiated under this chapter.

E. Nothing in this chapter shall be construed as providing the basis for, or be subject to, a private right of action for violations of this chapter or under any other law.

§ 59.1-581. Consumer Privacy Fund.

There is hereby created in the state treasury a special nonreverting fund to be known as the Consumer Privacy Fund. The Fund shall be established on the books of the Comptroller. All civil penalties, expenses, and attorney fees collected pursuant to this chapter shall be paid into the state treasury and credited to the Fund. Interest earned on moneys in the Fund shall remain in the Fund and be credited to it. Any moneys remaining in the Fund, including interest thereon, at the end of each fiscal year shall not revert to the general fund but shall

remain in the Fund. Moneys in the Fund shall be used to support the work of the Office of the Attorney General to enforce the provisions of this chapter, subject to appropriation.

2. The Chairman of the Joint Commission on Technology and Science shall create a work group composed of the Secretary of Commerce and Trade, the Secretary of Administration, the Attorney General, the Chairman of the Senate Committee on Transportation, representatives of businesses who control or process personal data of at least 100,000 persons, and consumer rights advocates. The work group shall review the provisions of this act and issues related to its implementation. The Chairman of the Joint Commission on Technology and Science shall submit the work group's findings, best practices, and recommendations regarding the implementation of this act to the Chairmen of the Senate Committee on General Laws and Technology and the House Committee on Communications, Technology and Innovation no later than November 1, 2021.

3. That any reference to federal law or statute in this act shall be deemed to include any accompanying rules or regulations or exemptions thereto. Further, this enactment is declaratory of existing law.

4. That the provisions of the first and third enactments of this act shall become effective on January 1, 2023.

KILPATRICK TOWNSEND

Washington House Bill 1493 on Biometric Identifiers

Although Washington has not yet passed a comprehensive data privacy law, Washington was the second state to comprehensively regulate biometrics.

Washington's biometrics law has been in effect since 2017. The full text of Washington's biometrics law is accessible at https://app.leg.wa.gov/RCW/default.aspx?cite=19.375&full=true#19.375.020.

Please see the Biometrics Law Quick Reference Guide for a high-level comparison of the requirements of Washington's biometrics law compared to other comprehensive biometrics laws.

KILPATRICK TOWNSEND

Comprehensive Data Privacy Law Quick Reference Guide

	California (CCPA, as amended by the CPRA)	Virginia (CDPA)	Colorado (CPA)	Connecticut ("CTDPA")	Utah ("UCPA")
Effective Date	January 1, 2023	January 1, 2023	July 1, 2023	July 1, 2023	December 31, 2023
Applicability threshold	Generally, the CPRA applies to businesses that do business in the State of California, and satisfy one or more of the following thresholds: 1) as of January 1 of the calendar year, had annual gross revenues in excess of $25,000,000 in the preceding calendar year, as adjusted pursuant to the CPRA, 2) alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more California residents or households, and 3) derives 50% or more of its annual revenues from selling or sharing California resident's personal information.	Generally, the CDPA applies to persons that conduct business in the Commonwealth of Virginia or produce products or services that are targeted to residents of the Commonwealth and that: 1) during a calendar year, control or process personal data of at least 100,000 Virginia residents; or 2) control or process the personal data of at least 25,000 Virginia residents and derive over 50% of gross revenue from the sale of personal data.	Generally, the CPA applies to controllers that conduct business in Colorado or produce or deliver commercial products or services that are intentionally targeted to Colorado residents and satisfy one or both of the following thresholds: 1) control or process personal data of 100,000 Colorado residents or more per calendar year; or 2) derive revenue or receive a discount on the price of goods or services from the sale of personal data and control or process the personal data of at least 25,000 Colorado residents.	Generally, the CTDPA applies to persons that conduct business in Connecticut or persons that produce products or services that are targeted to Connecticut residents and that during the preceding calendar year controlled or processed the personal data of: (1) not less than 100,000 Connecticut residents, excluding personal data controlled or processed for the purpose of completing a payment transaction; or (2) not less than 25,000 Connecticut residents and derived more than 25% of their gross annual revenue from the sale of personal data.	Generally, the UCPA applies to any controller or processor who: (a) (i) conducts business in Utah; or (ii) produces a product or service that is targeted to consumers who are residents of Utah; (b) has annual revenue of $25,000,000 or more; and (c) satisfies one or more of the following thresholds: (i) during a calendar year, controls or processes personal data of 100,000 or more Utah residents; or (2) derives over 50% of the entity's gross revenue from the sale of personal data and controls or processors data of 25,000 or more Utah residents.
Privacy notice requirement	✓	✓	✓	✓	✓

	California (CCPA, as amended by the CPRA)	Virginia (CDPA)	Colorado (CPA)	Connecticut ("CTDPA")	Utah ("UCPA")
Data subject rights	Right to access Right to delete Right to correct inaccurate personal information Right to know what information is sold or shared Right to opt-out of sale or sharing Right to limit use and disclosure of sensitive personal information	Right to access Right to correct Right to delete Right to data portability Right to opt-out of: 1) targeted advertising, 2) sale, and 3) profiling in advancing decisions that produce legal or similarly significant affects concerning the consumer	Right to access Right to correct Right to delete Right to data portability Right to opt-out of: 1) targeted advertising, 2) sale, and 3) profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer	Right to access Right to correct Right to delete Right to data portability Right to opt-out of: 1) targeted advertising, 2) sale, and 3) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer	Right to access Right to delete Right to data portability Right to opt-out of: 1) targeted advertising, and 2) sale.
Timeline to respond to data subject requests	Confirm receipt within 10 days of a request to know or delete. Within 45 calendar days of receiving a verifiable consumer request to access, delete, or correct, with a 45 calendar day extension period, but only 15 business days to opt-out of sale.	Within 45 days of the receipt of the request with a 45 day extension option, which is not exercisable if the controller declines to take action.	Within 45 days of the receipt of the request with a 45 day extension option, which is not exercisable if the controller declines to take action.	Within 45 days of the receipt of the request with a 45 day extension option, which is not exercisable if the controller declines to take action.	Within 45 days of the receipt of the request with a 45 day extension option, which is not exercisable if the controller declines to take action.
Right to appeal denials of data subject requests	✗	✓	✓	✓	✗
Sale	Monetary or other valuable consideration	Monetary consideration	Monetary or other valuable consideration	Monetary or other valuable consideration	Monetary consideration
Right to opt-out of sale	✓	✓	✓	✓	✓
Opt-in or opt-out for processing of sensitive information	Opt-out	Opt-in	Opt-in	Opt-in	Opt-out

Back to Table of Contents

	California (CCPA, as amended by the CPRA)	Virginia (CDPA)	Colorado (CPA)	Connecticut ("CTDPA")	Utah ("UCPA")
Contract requirements for service providers or processors	✓	✓	✓	✓	✓
Express obligations regarding de-identified data	×	✓	✓	✓	✓
Requirement to perform data protection impact assessments	✓	✓	✓	✓	×
Right of private action	✓ (for security breaches)	×	×	×	×
Governmental enforcement entities	California Privacy Protection Agency, Attorney General	Attorney General	Attorney General, District Attorneys	Attorney General	Attorney General
Cure period for violations	30 day cure period (CPRA – no automatic cure period – left to the regulator's discretion)	30 day cure period	60 day cure period "if a cure is deemed possible"; expires January 1, 2025	60 day cure period ending on December 31, 2024; left to the Attorney General's discretion thereafter	30 day cure period
Penalties	Up to $2,500 per violation and up to $7,500 per intentional violation or violation involving minors.	Up to $7,500 per violation.	Fines governed by Colorado Consumer Protection Act. Up to $20,000 per violation.	Fines governed by Connecticut Unfair Trade Practices Act. Up to $5,000 per willful violation.	Actual damages and up to $7,500 per violation.

KILPATRICK TOWNSEND

Biometrics Law Quick Reference Guide

	Illinois (BIPA)	Texas (CUBI)	Washington
Scope of information	"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared based on an individual's biometric identifier used to identify an individual. "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.	"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.	"Biometric identifier" means data generated by automatic measurements of an individual's biological characteristics, such as fingerprint, voiceprint, eye retinas, or other unique biological patterns or characteristics that is used to identify a specific individual.
Consent for collecting biometrics	✓	✓	✓
Exception for "security purpose"	×	×	✓
Notable exclusions	1) financial institutions or affiliates covered by the Gramm-Leach-Bliley Act 2) contractors, subcontractors, or agents of state agencies or local government	Voiceprint data retained by financial institutions or affiliates covered by the Gramm-Leach-Bliley Act	1) financial institutions or affiliates covered by the Gramm-Leach-Bliley Act 2) activities subject to Title V of HIPAA 3) law enforcement
Private right of action	✓	×	×
Governmental enforcement entities	×	Attorney General	Attorney General
Penalties	Negligent violations = greater of $1,000 or actual damages Intentional or reckless violations = greater of $5,000 or actual damages	Up to $25,000 per violation	Up to $7,500 per violation

Back to Table of Contents

KILPATRICK TOWNSEND

Acronym Quick Reference Guide

BIPA: The Illinois Biometric Information Privacy Act

CCPA: California Consumer Privacy Act

CDPA: Virginia's Consumer Data Protection Act

CPA: Colorado Privacy Act

CPRA: California Privacy Rights Act

CTDPA: Connecticut's An Act Concerning Personal Data Privacy and Online Monitoring

CUBI: Texas's Capture or Use of Biometric Identifier Act

GDPR: General Data Protection Regulation

UCPA: Utah Consumer Privacy Act

VCDPA: Virginia Consumer Data Protection Act

KILPATRICK TOWNSEND

Contacts

Amanda M. Witt
Partner
404.815.6008
awitt@kilpatricktownsend.com

Meghan K. Farmer
Partner
404.541.6816
mfarmer@kilpatricktownsend.com

Jon Neiditz
Partner
404.815.6004
jneiditz@kilpatricktownsend.com

John M. Brigagliano
Senior Associate
404.815.6135
jbrigagliano@kilpatricktownsend.com

Alexander J. Borovsky
Associate
404.815.6065
aborovsky@kilpatricktownsend.com

Jennie L. Cunningham
Associate
202.508.5869
jcunningham@kilpatricktownsend.com

Zain Haq
Associate
404.815.6046
zhaq@kilpatricktownsend.com

Click here to follow our blog.

KILPATRICK TOWNSEND

ANCHORAGE
ATLANTA
AUGUSTA
BEIJING
CHARLOTTE
CHICAGO
DALLAS
DENVER
HOUSTON
LOS ANGELES
NEW YORK
PHOENIX
RALEIGH
SAN DIEGO
SAN FRANCISCO
SEATTLE
SHANGHAI
SILICON VALLEY
STOCKHOLM
TOKYO
WALNUT CREEK
WASHINGTON D.C.
WINSTON-SALEM

Counsel to Innovative Businesses and Brands Around the World

We help leaders create, expand, and protect the value of their businesses and most prized assets. Our attorneys bring a balance of business savvy, technical skills, and creative thinking to the opportunities and issues our clients face daily. From the most complex challenges to the routine, we work together to make businesses better protected, smarter, and more competitive.

www.kilpatricktownsend.com