THOMSON REUTERS
PRACTICAL LAW™

Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA)

by Practical Law Data Privacy & Cybersecurity

Status: **Law Stated as of December 31, 2022** | Jurisdiction: **California**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/w-017-4166**
Request a free trial and demonstration at: **us.practicallaw.tr.com/practical-law**

A Practice Note discussing the California Consumer Privacy Act of 2018 (CCPA), as amended by the voter-approved California Privacy Rights Act of 2020 (CPRA). The Note explains the laws' consumer rights and protections, including personal information sale opt-out rights, corresponding business obligations, rulemaking requirements, and enforcement.

California often leads the US in codifying privacy protections. It became the first US state to enact a comprehensive consumer privacy law with the California Consumer Privacy Act of 2018 (CCPA) (Cal. Civ. Code §§ 1798.100 to 1798.199.95; Cal. Code Regs. tit. 11, §§ 7000 to 7102). California voters subsequently expanded the CCPA's protections by enacting the California Privacy Rights Act of 2020 (CPRA) through a ballot initiative. The CPRA will eventually replace the CCPA, with most of its provisions becoming effective on January 1, 2023. It also creates the first state agency focused exclusively on privacy, the California Privacy Protection Agency.

The CCPA and CPRA grant California residents new rights regarding their personal information and impose various data protection duties on certain entities conducting business in California. Businesses subject to the laws must also comply with additional regulations related to processing California residents' personal information that address, among other things:

- Updating or creating privacy notices.
- Consumer choice requirements for selling personal information.
- Restrictions on data monetization business models.
- Accommodating consumers' rights to access their personal information.
- Honoring the right to deletion.
- Producing requested data in portable format.

Given their expansiveness and broad reach, the CCPA and CPRA are likely to significantly impact entities both in California and around the world that collect and process California residents' personal information. Most of the CPRA's substantive CCPA amendments do not take effect until January 1, 2023, so businesses should continue to follow the CCPA and CCPA Regulations while they prepare for the CPRA's new requirements.

This Note discusses the CCPA and CPRA's core requirements, including:

- When it applies to a business (see Jurisdictional Scope and Key Definitions).
- Consumer rights (see Consumer Rights).
- Business obligations, including specific rules for selling personal information (see Business Obligations).
- Sharing personal information with service providers and third parties (see Service Providers and Third Parties).
- Rulemaking authority and process (see Rulemaking).
- Enforcement and penalties for violations (see Enforcement).

For more on how the CCPA and CPRA evolved, including legislative amendments and the ballot initiative process, see Box, History of the CCPA and CPRA. For more on the Agency's development of new and revised regulation for the CCPA and CPRA, see CPRA Regulation Tracker.

Businesses processing California residents' personal information still must pay careful attention to compliance with other applicable privacy laws, including, for example:

- Other California laws addressing marketing and advertising practices (see Practice Note, California Privacy and Data Security Law: Overview).

- Other US federal and state privacy and data security laws (see Practice Notes, US Privacy and Data Security Law: Overview and Cyber Incident and Data Breach Notification).

For additional CCPA and CPRA resources, include high-level comparisons between the CCPA, CPRA, and privacy laws from other jurisdictions, see California Privacy Toolkit (CCPA and CPRA).

Jurisdictional Scope and Key Definitions

Protected Individuals

The CCPA provides personal information rights and protections for consumers, defined as natural persons who are California residents according to the state regulations effective as of September 1, 2017 (Cal. Civ. Code § 1798.140(g)). Under those state regulations, California residents include individuals who are either:

- In California for other than a temporary or transitory purpose.
- Domiciled in California, but currently outside the state for a temporary or transitory purpose.

(Cal. Code Regs. tit. 18, § 17014.)

Defining consumers as any California resident leads to much broader coverage for the CCPA than the term "consumer" usually implies. In addition to customers of household goods and services, the CCPA's definition of consumers likely includes California-based:

- Employees.
- Contacts from business customers or vendors.

However, temporary exceptions relieve businesses from some CCPA requirements relating to certain employee and business-to-business (B2B) related personal information until January 1, 2023 (see Temporary Exemptions).

The CCPA's protections apply regardless of how the business identifies an individual consumer, including by any unique identifier, household, or device (Cal. Civ. Code § 1798.140(g), (x)).

CPRA Revisions: Protected Individuals

The CPRA does not change the CCPA's expansive consumer definition (Cal. Civ. Code § 1798.140(i) (effective January 1, 2023)).

Covered Businesses

The CCPA's obligations apply to a business, which it defines as a for-profit entity (including a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity) that:

- Collects a consumer's personal information (directly or on its behalf) and determines the purposes and means of processing (alone or jointly with others).
- Does business in California and meets one of the following thresholds:
  - annual gross revenue that exceeds $25 million (adjusted for inflation);
  - annually buys, receives, shares, or sells the personal information of more than 50,000 consumers, households, or devices for commercial purposes (alone or in combination); or
  - derives 50% or more of annual revenues from selling consumers' personal information.

(Cal. Civ. Code § 1798.140(c)(1).)

The CCPA's business definition also includes any entity that both:

- Controls or is controlled by a covered business, meaning:
  - ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a business;
  - control in any manner over the election of most of the directors or of individuals exercising similar functions; or
  - the power to exercise a controlling influence over the entity's management.
- Shares common branding with a covered business, such as a shared name, service mark, or trademark.

(Cal. Civ. Code § 1798.140(c)(2).)

Parts of the CCPA also apply specifically to:

- Service providers.
- Third parties.

(See Service Providers and Third Parties.)

The CCPA does not apply to non-profit or public entities. California regulates personal information disclosures by those entities in other laws, such as California Government Code Chapter 3.5, which governs the inspection of public records (Cal. Gov't Code §§ 6250 to 6276.48). However, any for-profit subsidiaries or commercial joint ventures of

non-profit organizations meeting the CCPA's jurisdictional thresholds may fall under its requirements.

The CCPA provides numerous exceptions to its application based on:

- Jurisdictional concerns, such as when:
  - every aspect of commercial conduct takes place wholly outside of California (see Commercial Conduct Wholly Outside of California).
  - completing a single, one-time transaction that does not retain collected personal information; or
  - another sector-specific privacy or data protection law covers the conduct (see Preemption).
- Common business operation needs, such as to allow the sale of personal information as part of a larger merger or acquisition transaction (see Mergers and Acquisitions Exception).
- Legal or conflicts of laws issues, such as to comply with other laws, defend legal claims, or cooperate with law enforcement.

(Cal. Civ. Code §§ 1798.100(e), 1798.145, and 1798.190.)

For more on these exceptions, see Coverage Exceptions and Extraterritorial Application and Personal Information Sales.

CPRA Revisions: Covered Businesses

The CPRA changes the covered business definition, including the jurisdictional thresholds. Once it takes effect:

- Entities will determine whether they meet the annual gross revenue threshold by looking to their total sales from the prior calendar year (January to December) (Cal. Civ. Code § 1798.140(d)(1)(A) (effective January 1, 2023)). This means an entity with less than $25 million in gross revenue (adjusted for inflation) for the entire 2023 calendar year would not meet the coverage threshold for all of 2024, even if its gross revenue in January 2024 alone exceeded that amount. In this example, the entity would not become a covered business under the CPRA until January 1, 2025. This gives growing businesses time to adjust to the new requirements and provides clarity on when the CPRA's requirements begin.
- The consumer-based threshold:
  - increases to 100,000 consumers or households, but no longer counts devices;
  - applies to buying, selling, or sharing personal information; and
  - no longer requires a commercial purpose.
  - (Cal. Civ. Code § 1798.140(d)(1)(B) (effective January 1, 2023).)
- Commonly branded and controlled entities that do not independently meet the CPRA's thresholds must actually share personal information with their CPRA-covered affiliates before the CPRA also applies to them (Cal. Civ. Code § 1798.140(d)(2) (effective January 1, 2023)).
- Joint ventures or partnerships composed of other covered businesses that each have at least a 40 percent interest in the entity are also covered businesses, and the joint venture or partnership cannot disclose personal information received from one business partner to the other business partner (Cal. Civ. Code § 1798.140(d)(3) (effective January 1, 2023)).
- Uncovered businesses that operate in California can voluntarily agree to the CPRA's jurisdiction by submitting a compliance agreement and certification to the California Privacy Protection Agency (Cal. Civ. Code § 1798.140(d)(4) (effective January 1, 2023)). Businesses that might want take advantage of this option could include service providers whose customers require CPRA compliance or third parties who must contractually agree to CPRA coverage in order to purchase personal information from a CPRA-covered business (Cal. Civ. Code § 1798.100(d)(2) (effective January 1, 2023).

(Cal. Civ. Code § 1798.140(d) (effective January 1, 2023).)

The CPRA also creates a new type of covered entity called contractors that must meet certain CPRA requirements, similar to service providers and certain third parties under the CCPA (Cal. Civ. Code § 1798.140(j) (effective January 1, 2023); see CPRA Revisions: Service Provider, Contractor, Third Party Definitions).

Personal Information

The CCPA defines personal information more broadly than California's other laws. It includes any information that either directly or indirectly:

- Identifies, relates to, or describes a particular consumer or household.
- Is reasonably capable of being associated with or could reasonably be linked to a particular consumer or household.

(Cal. Civ. Code § 1798.140(o)(1).)

The CCPA lists specific examples of potential personal information, such as internet protocol (IP) addresses, but

the statute also emphasizes that each data example must actually identify, relate, describe, or reasonably associate or link, directly or indirectly, to a particular individual or household before it qualifies as personal information.

The CCPA protects data even if it does not relate to a single individual because it covers households and devices and it protects information connected to any unique identifier instead of a person's name (Cal. Civ. Code § 1798.140(o)(1), (x)). The CCPA Regulations define a household as a person or group who all:

- Reside at the same address.
- Share a common device or the business's service.
- Use the same group account or unique identifier.

(Cal. Code Regs. tit. 11, § 7001(k).)

Personal information does not include:

- Information lawfully made available from government records (see Publicly Available Government Records).
- Deidentified or aggregate consumer information (see Deidentified or Aggregated Consumer Information).

(Cal. Civ. Code § 1798.140(o)(2), (3).)

CPRA Revisions: Personal Information

The CPRA does not change the CCPA's current personal information definition, but it does add a new category for sensitive personal information (Cal. Civ. Code § 1798.140(v)(1)(L), (ae) (effective January 1, 2023); see CPRA Revisions: New Sensitive Personal Information Category)). It also broadens the exclusion for publicly available information (Cal. Civ. Code § 1798.140(v)(2) (effective January 1, 2023); see CPRA Revisions: Publicly Available Information).

Personal Information Categories

The personal information definition provides a list of 11 personal information categories with examples, highlighting that the examples only qualify as personal information if the data meets the underlying criteria of directly or indirectly linking to a particular consumer or household. The 11 categories are:

- Identifiers, such as:
  - a real name;
  - an alias;
  - a postal address;
  - an email address;
  - a unique personal or online identifier;
  - an IP address;
  - an account name;
  - a Social Security number (SSN);
  - a driver's license or passport number; or
  - another form of persistent or probabilistic identifier that can identify a particular consumer, family, or device.
- Personal information categories described in the California Customer Records statute, which, in addition to the identifiers described above, also lists a person's:
  - signature;
  - state identification card number;
  - physical characteristics or description;
  - insurance policy number;
  - education;
  - employment or employment history;
  - bank account number, credit card number, debit card number, or any other financial information; or
  - medical information or health insurance information.

  (Cal. Civ. Code § 1798.80(e).)
- Characteristics of protected classifications under California or federal law, like race, national origin, religion, gender, or sexual orientation (see State Q&A, Anti-Discrimination Laws: California).
- Commercial information, including records of personal property and purchasing habits.
- Biometric information, including genetic, physiological, behavioral, and biological characteristics, or activity patterns from which organizations can extract a template or other identifier or identifying information, such as:
  - fingerprints, faceprints, and voiceprints;
  - iris or retina scans;
  - keystroke, gait, or other physical patterns; and
  - sleep, health, or exercise data.
- Internet or other similar network activity, including:
  - browsing history;
  - search history; or
  - information regarding a consumer's interaction with an internet website, application, or advertisement.

- Geolocation data.
- Audio, electric, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Non-publicly available educational information as defined under the Family Educational Rights and Privacy Act (FERPA) and related regulations (20 U.S.C. § 1232g; 34 C.F.R. §§ 99.1 to 99.67).
- Inferences drawn from other personal information to create consumer profiles reflecting:
  - preferences;
  - characteristics;
  - psychological trends;
  - predispositions;
  - behavior;
  - attitudes;
  - intelligence;
  - abilities; or
  - aptitudes.

(Cal. Civ. Code § 1798.140(o)(1)(A) to (K).)

The CCPA also clarifies that its provisions apply regardless of the data collection method used, including, for example, to personal information collected or generated:

- Electronically on a computer.
- Online over the internet.
- Using a pen and paper.
- Using an algorithm.

(Cal. Civ. Code § 1798.175.)

CPRA Revisions: New Sensitive Personal Information Category

The CPRA creates a twelfth category for sensitive personal information, defined as:

- Personal information that reveals a consumer's:
  - social security, driver's license, state identification card, or passport number;
  - 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;
  - precise geolocation;
  - racial or ethnic origin;
  - religious or philosophical beliefs;
  - union membership; or
  - genetic data.
- The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.
- The processing of biometric information for the purpose of uniquely identifying a consumer.
- Personal information collected and analyzed concerning a consumer's health, sex life, or sexual orientation.

(Cal. Civ. Code § 1798.140(v)(1)(L), (ae) (effective January 1, 2023).)

However, the CPRA section establishing a consumer's right to limit sensitive information use and disclosure qualifies this definition. It excludes personal information that would otherwise fall into the sensitive personal information category if the business collected or processed it **without** the purpose of inferring characteristics about a consumer. When sensitive personal information qualifies for this exception, the business may treat it as just personal information for all CPRA sections. (Cal. Civ. Code § 1798.121(d) (effective January 1, 2023).)

The CPRA expects the California Privacy Protection Agency to issue regulations that further clarify when sensitive personal information might qualify for this narrow exception (Cal. Civ. Code §§ 1798.121(d) and 1798.185(a)(19)(C)(iv) (effective January 1, 2023); see CPRA Regulation Tracker).

Distinguishing Between Sales and Business Purposes Disclosures

The CCPA The CCPA places different restrictions and notice obligations on personal information sales and disclosures for a business purpose. For example, the CCPA:

- Grants consumers the right to stop personal information sales, but not business-related disclosures to service providers (see Sale Opt-Out and Opt-In Rights and Service Provider Exception).
- Prohibits sales of personal information about consumers under age 16 without obtaining affirmative opt-in consent (see Sale Opt-Out and Opt-In Rights).
- Requires a business to make separate statements about personal information sales and business purpose disclosures in its privacy policy and individual right

to know responses (see Box, Privacy Policy Required Elements List and Individual Right to Know).

- Uses whether a business derives 50% or more of its annual revenues from selling consumers' personal information as one of its coverage thresholds (see Covered Businesses).

Meeting the CCPA's obligations therefore requires a business to understand when providing personal information to another entity results in a sale (see Personal Information Sales) or a disclosure for a business purpose (see Business Purposes and Service Providers and Third Parties).

CPRA Revisions: New Type of Personal Information Transfer

The CPRA adds sharing personal information for cross-context behavioral advertising as a third transfer type and universally expands its personal information sale requirements to also cover sharing personal information (Cal. Civ. Code §§ 1798.120 and 1798.140(ah) (effective January 1, 2023); see CPRA Revisions: Sharing Personal Information).

Personal Information Sales

The CCPA defines the sale of personal information broadly to include any communication or transfer of consumer's personal information by a CCPA-covered business to another business or third party for monetary or other valuable consideration. The statute specifically includes the phrase "other valuable consideration," which indicates that many different types of non-cash transactions may classify as sales if the business receives any type of benefit in return for providing access to the personal information. A sale may include non-cash benefits, such as:

- Mutual access to each business's marketing list.
- Access to information or insights about the consumers, like an influencer score.
- The ability to target advertising to specific consumers.

The term "sale" includes actions, such as:

- Renting.
- Releasing.
- Disclosing.
- Disseminating.
- Making available.
- Transferring.
- Otherwise communicating personal information, by any means, including:
  - orally;
  - in writing; or
  - electronically.

(Cal. Civ. Code § 1798.140(t)(1).)

A recent California AG enforcement action found that a business sells consumers' personal information when cookies on the business' website share it with a third party in exchange for in-kind benefits that leverage the shared information, such as to provide website use analytics or targeted adverting (see Legal Update, California AG Announces $1.2 Million Settlement with Sephora for CCPA Personal Information Sales Violations).

The CCPA's sale definition contains four important exceptions relating to:

- Service providers (see Service Provider Exception).
- Consumer requests (see Consumer-Directed Transfer Exception).
- Mergers and acquisitions (see Mergers and Acquisitions Exception).
- Honoring sale opt-out requests (see Honoring Opt-Out Requests Exception).

(Cal. Civ. Code § 1798.140(t)(2).)

Businesses may take advantage of these exceptions to classify a personal information transfer as a business purpose disclosure instead of a sale (see Distinguishing Between Sales and Business Purposes Disclosures).

CPRA Revisions: Sales Definition

The CPRA slightly changes the CCPA's sales definition to clarify that a sale only occurs when the recipient is a third party, which the CPRA now defines as any person who is not:

- 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.
- A service provider to the business.
- A contractor.

(Cal. Civ. Code § 1798.140(ad), (ai) (effective January 1, 2023).)

Service Provider Exception

The CCPA treats providing qualified service providers with personal information as a business purpose disclosure instead of a sale (Cal. Civ. Code § 1798.140(t)(2)(C), (v); Cal. Code Regs. tit. 11, § 7051). However, service providers must meet specific requirements and strictly limit how they use the shared personal information to qualify for the exception. For more on the CCPA's service provider requirements and obligations, see Service Providers and Third Parties.

CPRA Revisions: Service Provider Exception

The CPRA rewrote the sections dealing with service providers, sales, and third parties to streamline the language and clarify the exclusions. Under the CPRA:

- Sales only occur when the recipient is a third party, which is a defined term.
- By definition, a business's qualified service providers are not third parties.

(Cal. Civ. Code § 1798.140(ad), (ai)(2) (effective January 1, 2023).)

So while the CPRA removes CCPA's current service provider exclusion from the sales definition (Cal. Civ. Code §1798.140(t)(2)(C)), it retains the exception through a different statutory formulation (see CPRA Revisions: Sales Definition and CPRA Revisions: Service Provider, Contractor, Third Party Definitions).

Consumer-Directed Transfer Exception

Acting on a consumer's request to interact with or disclose their personal information to a third party does not constitute a sale under the CCPA if:

- The consumer intentionally requests the action in a deliberate interaction.
- The third party does not further sell the personal information unless the disclosure would be consistent with the CCPA.

Importantly, the CCPA specifically states that performing any of the following actions on a piece of content does not indicate a consumer's intent to interact with a third party:

- Hovering over.
- Muting.
- Pausing.
- Closing.

(Cal. Civ. Code § 1798.140(t)(2)(A).)

CPRA Revisions: Consumer-Directed Transfer Exception

The CPRA kept this exception but streamlined the language by making "intentionally interacts" a defined term and removing the redundant qualifier restricting further sales by the third-party recipient. Under the CPRA, a business does not sell personal information when a consumer uses or directs the business to intentionally:

- Disclose personal information.
- Interact with one or more third parties.

(Cal. Civ. Code § 1798.140(ad)(2)(A) (effective January 1, 2023).)

A consumer intentionally interacts with a person when they initiate a deliberate interaction, such as visiting the person's website or purchasing their goods or services. As with the CCPA, hovering over, muting, pausing, or closing a given piece of content does not indicate the consumer's intent to interact with a person. (Cal. Civ. Code § 1798.140(s) (effective January 1, 2023).)

Importantly, the person receiving a consumer's personal information under this exception "collects" it under the CPRA and should evaluate whether the CPRA's protections and restrictions apply to it directly (Cal. Civ. Code § 1798.140(d), (f) (effective January 1, 2023); see Covered Businesses).

Mergers and Acquisitions Exception

Personal information exchanges in mergers, acquisitions, bankruptcies, or other transactions in which a third party assumes control of the business (in whole or part) do not qualify as sales under the CCPA if:

- Any use or sharing of the information remains consistent with the CCPA's consumer disclosure provisions (see General Notice Rights and Individual Right to Know).
- The third party does not materially alter how it uses or shares the acquired personal information unless:
  - it provides prior notice to the consumer of the new or changed practice in a sufficiently prominent and robust manner to ensure that consumers can exercise their sale opt-out rights (see Sale Opt-Out and Opt-In Rights); and
  - the change does not violate the California Unfair and Deceptive Practices Act (Cal. Bus & Prof. Code §§ 17200 to 17210).

(Cal. Civ. Code § 1798.140(t)(2)(D).)

CPRA Revisions: Mergers and Acquisitions Exception

The CPRA retained this exception but conditioned its application on the continued use or sharing of the acquired information in compliance with the entire CPRA, not just the consumer disclosure and opt-out provisions (Cal. Civ. Code § 1798.140(ad)(2)(C) (effective January 1, 2023)).

Honoring Opt-Out Requests Exception

The disclosure of customer identifiers with third parties does not constitute a sale under the CCPA if the sole purpose of the disclosure is to inform others about consumer opt-out requests (Cal. Civ. Code § 1798.140(t)(2)(B)). This narrow exception is solely to help businesses honor the consumer's CCPA rights (see Sale Opt-Out and Opt-In Rights).

CPRA Revisions: Honoring Opt-Out Requests Exception

The CPRA kept this exception in place and expanded it to cover informing others about consumer requests to exercise the CPRA's new right to limit use of their sensitive personal information (Cal. Civ. Code § 1798.140(ad)(2)(B) (effective January 1, 2023)). For more on the CPRA's opt-out rights, see CPRA Revisions: Sharing Opt-Out and Opt-In Rights and CPRA Revisions: New Right to Restrict Sensitive Personal Information Processing.

CPRA Revisions: Sharing Personal Information

The CPRA introduces "sharing" as a separate, third type of personal information transfer, but with a definition that significantly differs from that term's common use. Under the CPRA, a business shares personal information when it is:

- Communicated to a third party.
- For cross-context behavioral advertising.

(Cal. Civ. Code § 1798.140(ah) (effective January 1, 2023).)

Sharing personal information for cross-context behavioral advertising:

- Does not require a particular communication method and includes:
  - renting;
  - releasing;
  - disclosing;
  - disseminating;
  - making available;
  - transferring; or
  - otherwise communicating orally, in writing, or by electronic or other means.
- Does not require any type of valuable consideration, monetary or otherwise.

(Cal. Civ. Code § 1798.140(ah) (effective January 1, 2023).)

Business Purposes

The CCPA provides different requirements when a business discloses personal information for a business purpose instead of a sale (see Distinguishing Between Sales and Business Purposes Disclosures). A business uses personal information for a business purpose if the use is both:

- For an operational purpose of the business or service provider, or anther notified purpose.
- Reasonably necessary for and proportionate to:
  - the operational purpose for which the personal information is first collected or processed; or
  - another contextually compatible operational purpose.

(Cal. Civ. Code § 1798.140(d).)

The CCPA identifies seven types of approved business purposes, which are:

- Auditing the interaction with the consumer and concurrent transactions, including counting ad impressions and verifying quality of ad impressions.
- Detecting or preventing security incidents or other illegal activity and prosecuting the responsible parties.
- Debugging.
- Short-term, transient use if the personal information is not:
  - disclosed to another third party; or
  - used to build a profile or otherwise alter an individual consumer's experience outside the current interaction.
- Performing services on behalf of the business or its service provider, such as customer service, order fulfillment, payment processing, financing and advertising, marketing, or analytic services.
- Undertaking internal research for technological development and demonstration.

- Verifying or maintaining quality or safety or improving or upgrading a service or device owned, manufactured, or controlled by or for the business.

(Cal. Civ. Code § 1798.140(d)(1) to (7).)

While those listed activities clearly qualify as business purposes under the statute, it is unclear whether the list merely provides examples of business purposes or restricts the term to just those activities. This ambiguity is one of many generated by the CCPA's hasty adoption and inconsistent phrasing (see Box, History of the CCPA and CPRA). The CCPA Regulations do not directly address this ambiguity.

CPRA Revisions: Business Purposes

The CPRA revised the CCPA's business purposes definition by clarifying the requirements, revising some of the listed business purposes, and adding a new business purpose focused on advertising.

Under the CPRA, the term "business purposes" means the use of personal information for:

- The business' operational purposes.
- The business' other notified purposes.
- The service provider's or contractor's operational purposes, as defined by regulations that the CPPA will adopt (Cal. Civ. Code § 1798.185(a)(11)).

(Cal. Civ. Code § 1798.140(e) (effective January 1, 2023).)

Any use of personal information for a business purpose must be reasonably necessary and proportionate:

- To achieve the purpose for which the personal information was collected or processed.
- For another purpose that is compatible with the context in which the personal information was collected.

(Cal. Civ. Code § 1798.140(e) (effective January 1, 2023).)

The eight business purposes specifically identified in the CPRA are:

- Auditing related to:
  - counting ad impressions to unique visitors;
  - verifying positioning and quality of ad impressions; and
  - compliance with the CPRA and other standards.
- Helping to ensure security and integrity.
- Debugging.
- Short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, if the consumer's personal information is not:
  - disclosed to another third party; or
  - used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.
- Performing services for 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 other similar services.
- Providing advertising and marketing services to the consumer (excluding cross-context behavioral advertising), if the service provider or contractor does not combine personal information from the business' opted-out consumers with personal information received from, or on behalf of, another person or persons or that it collected independently.
- Undertaking internal research for technological development and demonstration.
- Verifying or maintaining quality or safety or improving or upgrading a service or device owned, manufactured, or controlled by or for the business.

(Cal. Civ. Code § 1798.140(e)(1) to (8) (effective January 1, 2023).)

While it remains unclear whether this statutory list merely provides examples of business purposes or restricts the term to just those activities, the definition's reference to a business' "other notified purposes" indicates that the term should cover any purpose the business disclosed in its collection notices (see Notice at Collection). Future CPRA regulations may address this issue (see CPRA Regulation Tracker). However, the revised definition does clarify that service providers and contractors only use personal information for a business purpose when the use is for their operational purposes, which future CCPA regulations should define. The CPRA does not contain a definition for the term operational purposes.

Commercial Purposes

The CCPA also includes a related, but broader definition for the term commercial purposes. A business acts for a commercial purpose whenever it advances its 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.

- Directly or indirectly enabling or effecting a commercial transaction.

(Cal. Civ. Code § 1798.140(f).)

Engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism, is specifically excluded from the commercial purposes definition (Cal. Civ. Code § 1798.140(f)).

CPRA Revisions: Commercial Purposes

The CPRA keeps the commercial purposes definition intact, but it deletes the definition's carve out for non-commercial speech as redundant after the addition of a general exclusion stating that the CPRA's rights and obligations do not apply if they infringe on a person's or entity's free speech and press rights under California's Constitution (Cal. Civ. Code §§ 1798.140(g) and 1798.145(l) (effective January 1, 2023); Cal. Const. Art. I, §2(b); see CPRA Revisions: New Exclusions). As a result, the deletion does not substantively alter the commercial purposes definition.

Coverage Exceptions and Extraterritorial Application

The CCPA provides some limited exceptions to its jurisdictional scope and personal information definition, including:

- Temporary exceptions for certain employment and B2B related personal information (see Temporary Exemptions).
- Conduct occurring entirely outside of California (see Commercial Conduct Wholly Outside of California).
- Government records (see Publicly Available Government Records).
- Deidentified or aggregated data (see Deidentified or Aggregated Consumer Information).
- Preemption by other federal or state sector-specific privacy statutes (see Preemption).

The CCPA also does not restrict a business' ability to:

- Comply with other laws.
- Defend or exercise legal claims.
- Cooperate with law enforcement.
- Respond to subpoenas or regulator inquiries.

(Cal. Civ. Code § 1798.145(2) to (4).)

The CPRA expands the existing exclusions for law enforcement and government agency cooperation to include:

- Providing information to comply with a court order or subpoena.
- Retaining information for limited periods pursuant to an active law enforcement agency investigation, despite a consumer's deletion request.
- Cooperating with government agency emergency access requests if a natural person is a risk or danger of death or serious physical injury.

(Cal. Civ. Code § 1798.145(a)(1) to (5) (effective January 1, 2023).)

The CPRA also adds a number of new exclusions for unique situations (see CPRA Revisions: New Exclusions).

Temporary Exemptions

The 2019 CCPA Amendments and the CPRA included two temporary exceptions from certain CCPA requirements that expire on January 1, 2023:

- Workforce and employment related personal information (see Workforce Personal Information Exception).
- B2B communications (see B2B Communications Exception).

Workforce Personal Information Exception

The workforce personal information exception applies to personal information a business collects about natural persons acting as job applicants, employees, owners, directors, officers, medical staff members, or contractors for the business (workforce members), but only when collected and used either:

- Solely within the context of that individual's role.
- For that individual's emergency contact information.
- To administer that individual's benefits

(Cal. Civ. Code § 1798.145(h)(1).)

However, this temporary exception does not apply to the CCPA's:

- Collection notice requirement (Cal. Civ. Code § 1798.100(b); see Notice at Collection).
- Private right of action for data breaches (Cal. Civ. Code § 1798.150; see Private Right of Action for Data Breaches).

(Cal. Civ. Code § 1798.145(h)(3).)

The workforce exception contains specific definitions for the terms:

- Contractor, which requires a written contract.
- Director.
- Medical staff member.
- Officer.
- Owner.

(Cal. Civ. Code § 1798.145(h)(2)(A) to (E).)

For more on an employer's CCPA obligations, see Practice Note, California Privacy Laws (CCPA and CPRA): Impact on Employers. For more on an employer's CPRA obligations, see Practice Note, Administering California Employee Privacy Rights Under the CPRA.

B2B Communications Exception

The temporary B2B exception covers personal information:

- Reflecting a written or verbal communication or transaction between the business and a natural person acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency.
- The communication or transaction with the business of which occurs solely within the context of the business:
  - conducting due diligence; or
  - providing or receiving a product or service to or from that entity.

(Cal. Civ. Code § 1798.145(n)(1).)

The B2B exception only exempts business from complying with six specific CCPA sections addressing:

- General right to know, notice, and purpose limitation requirements (Cal. Civ. Code § 1798.100).
- Deletion rights (Cal. Civ. Code § 1798.105).
- Individual right to know requirements (Cal. Civ. Code §§ 1798.110 and 1798.115).
- Consumer right requests and privacy policy requirements (Cal. Civ. Code § 1798.130).
- Opt-out right notice requirements (Cal. Civ. Code § 1798.135).

Importantly, businesses must still comply with the CCPA's requirements on:

- Personal information sales opt-out and opt-in rights (Cal. Civ. Code § 1798.120) (see Sale Opt-Out and Opt-In Rights).
- Nondiscrimination obligations (Cal. Civ. Code § 1798.125) (see Freedom from Discrimination).
- Private right of action for data breaches (Cal. Civ. Code § 1798.150) (see Private Right of Action for Data Breaches).

The B2B exception also provides the same specific definitions for the terms contractor, director, officer, and owner as the employment exception (Cal. Civ. Code § 1798.145(n)(2)(A) to (D)).

For more on the B2B communications exception, see Practice Note, California Privacy Laws (CCPA and CPRA): Impact on Employers: B2B Communications Exception.

Commercial Conduct Wholly Outside of California

The CCPA does not prevent collections or sales of a California resident's personal information if every aspect of the commercial conduct takes place wholly outside California. To qualify for this exterritoriality exception, the business must:

- Collect the personal information while the consumer is outside of California.
- Ensure no part of the consumer's personal information sale occurs in California.
- Not sell personal information collected while the consumer was in California.

Importantly, the CCPA's extraterritoriality exception expressly prohibits a business from avoiding its intent by storing personal information about the consumer while present in California (including on a device) and then collecting that personal information when the consumer or stored personal information is later outside of California. (Cal. Civ. Code § 1798.145(a)(6).)

CPRA Revisions: Commercial Conduct Wholly Outside of California

The CPRA reverses the CCPA's circumscription prohibition and now expressly states that the section does not prohibit a business from storing personal information about the consumer while present in California (including on a device) and then collecting that personal information when the consumer or stored personal information is later outside of California (Cal. Civ. Code § 1798.145(a)(7) (effective January 1, 2023)).

However, selling personal information collected while the consumer was in California will still disqualify the business from claiming this exception applies. Commercial conduct

does not take place wholly outside of California when a business sells personal information collected while the consumer was in California (Cal. Civ. Code § 1798.145(a)(7) (effective January 1, 2023).

Publicly Available Government Records

Personal information does not include publicly available information. However, the CCPA's narrow definition of the term publicly available:

- Only includes information from federal, state, or local government records.
- Excludes biometric information collected without the consumer's knowledge

(Cal. Civ. Code § 1798.140(o)(2).)

CPRA Revisions: Publicly Available Information

The CPRA retains and significantly expands this exclusion. Under the CPRA, personal information does not include:

- Publicly available information, defined as information either:
  - lawfully made available from federal, state, or local government records;
  - 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
  - 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.
- Lawfully obtained, truthful information that is a matter of public concern.

(Cal. Civ. Code § 1798.140(v)(2) (effective January 1, 2023).)

Importantly, publicly available information still does not include biometric information collected without the consumer's knowledge, regardless of the source (Cal. Civ. Code § 1798.140(v)(2) (effective January 1, 2023)).

These revisions greatly expand the scope of publicly available information that will not receive the CPRA's personal information protections, such as publicly posted user profiles or social media posts.

Deidentified or Aggregated Consumer Information

The CCPA does not restrict businesses from collecting, using, retaining, selling, or disclosing data that meets the statutorily defined terms of deidentified or aggregate consumer information (Cal. Civ. Code §§ 1798.140(o)(3) and 1798.145(a)(5)). Data qualifies as:

- **Deidentified** when it cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, if the business using deidentified information:
  - implemented technical safeguards that prohibit reidentifying the consumer the information may pertain to;
  - implemented business processes that specifically prohibit reidentifying the information;
  - implemented business processes to prevent inadvertent release of deidentified information; and
  - makes no attempt to reidentify the information.

  (Cal. Civ. Code § 1798.140(h).)
- **Aggregate consumer information** when it relates to a group or category of consumers:
  - from which individual consumer identities were removed; and
  - that is not linked or reasonably linkable to any consumer or household, including via a device.

  (Cal. Civ. Code § 1798.140(a).)

The aggregate consumer information definition expressly excludes one or more individual consumer records that were deidentified (Cal. Civ. Code § 1798.140(a)).

CPRA Revisions: Deidentified or Aggregated Consumer Information

The CPRA retains the deidentified or aggregate consumer information exclusion but revises how it defines deidentified information (Cal. Civ. Code §§ 1798.140(b), (m), (v)(3) and 1798.145(a)(6) (effective January 1, 2023)).

Under the CPRA, information is deidentified when it cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer of the business possessing the deidentified information and the business:

- Takes reasonable measures to ensure that the information cannot be associated with a consumer or household.
- Publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information (except as needed to audit the deidentification process's compliance).

- Contractually obligates any deidentified information recipients to comply with all of the CPRA's deidentification provisions.

(Cal. Civ. Code §§ 1798.140(m) (effective January 1, 2023).)

Deidentified Patient Information

The 2020 CCPA Amendments added specific provisions addressing deidentified patient information that only permits exclusion if it is both:

- Derived from patient information originally collected, created, transmitted, or maintained by an entity regulated under either:
  - the California Confidentiality of Medical Information Act (CMIA) (Cal. Civ. Code §§ 56 to 56.37);
  - the Health Insurance Portability and Accountability Act of 1996 (HIPAA); or
  - the Federal Policy for the Protection of Human Subjects (Common Rule) (45 C.F.R. §§ 46.101 to 46.505).
- Deidentified using the HIPAA Privacy Rule's deidentification standards and approved methodologies (45 C.F.R. § 164.514).

(Cal. Civ. Code § 1798.146(a)(4)(A).)

The CCPA prohibits a business or other person from reidentifying or attempting to reidentify any deidentified patient information except for the following purposes:

- Treatment, payment, or health care operations conducted by CMIA providers of healthcare, HIPAA covered entities, or HIPAA business associates.
- Public health activities or purposes as described in the HIPAA Privacy Rule (45 C.F.R. § 164.512).
- Research, as defined by the HIPAA Privacy Rule (45 C.F.R. § 164.501), conducted in accordance with the Common Rule (45 C.F.R. §§ 46.101 to 46.505).
- By a person or entity the deidentified patient information's lawful holder expressly engages:
  - to conduct testing, analysis, or validation of the deidentification or related statistical techniques; and
  - under a contract that bans any other use or disclosure of the reidentified information and requires its return or destruction when the contract ends.
- Where otherwise required by law.

(Cal. Civ. Code § 1798.148(a).)

Reidentified patient information is not eligible for the CCPA exemption and remains subject to the applicable federal and state data privacy laws, such as the CMIA and HIPAA (Cal. Civ. Code §§ 1798.146(a)(4)(B) and 1798.148(b)).

The 2020 CCPA Amendments also added contract and privacy notice requirements for businesses that sell or license deidentified patient information (see Sales or Licenses of Deidentified Patient Information and Box, Privacy Policy Required Elements List).

CPRA Revisions: Deidentified Patient Information

The 2020 CCPA Amendments were enacted after the CPRA's text was submitted to the voters but before the election, so the CPRA does not directly amend or reenact these new CCPA sections on deidentified patient information requirements (Cal. Civ. Code §§ 1798.146 and 1798.148). While the CPRA's provisions prevail over any conflicting legislation enacted after January 1, 2020, legislation does not conflict if it is consistent with CPRA and furthers its purposes (Section 25(d), CA Prop. 24 (2020)).

Preemption

Businesses may be subject to both the CCPA and sector-specific privacy laws. In fact, the CCPA expressly states that it is meant to supplement, not replace, existing consumer protection laws, specifically identifying:

- Chapter 22 of Division 8 of the Business and Professions Code, also known as the California Online Privacy Protection Act (CalOPPA) (Cal. Bus & Prof. Code §§ 22575 to 22579).
- California Civil Code Title 1.81 on Customer Records, which includes California's Data Protection Act (CDPA), Shine the Light law, and data breach notification statute (Cal. Civ. Code §§ 1798.80 to 1798.84).

(Cal. Civ. Code § 1798.175; see Practice Note, California Privacy and Data Security Law: Overview.)

However, other CCPA exclusions do seek to avoid conflict with certain sector-specific privacy laws. For example, the CCPA specifically excludes from its scope:

- Medical information governed by the CMIA (see Practice Note, California Privacy and Data Security Law: Overview: Health Information Privacy).
- Protected Health Information (PHI) governed by the privacy, security, and breach notification rules established under HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH Act) (see Practice Notes, HIPAA Privacy Rule, HIPAA Security Rule, and HIPAA Breach Notification Rules).

- CMIA providers of healthcare, HIPAA covered entities, and HIPAA business associates that maintain, use, and disclose patient information in compliance with the CMIA, HIPAA, or HITECH Act.
- Information collected in a clinical trial or collected, used, or disclosed in research, as defined by the HIPAA Privacy Rule (45 C.F.R. § 164.501), conducted in accordance with:
  - the HIPAA Privacy Rule's applicable ethics, confidentiality, privacy, and security requirements (45 C.F.R. §§ 164.102 to 164.534);
  - the Common Rule (45 C.F.R. §§ 46.101 to 46.505; see Article, Key Changes to Human Study Subject Protections Pending Under the Common Rule);
  - the Food and Drug Administration's human subject protection requirements (21 C.F.R. §§ 50.1 to 50.56 and 56.101 to 56.124; see Legal Update, FDA Announces Guidance on Complying with Current FDA Human Subject Protection Regulations and the Revised Common Rule); or
  - the International Council for Harmonisation's E6 Good Clinical Practice (GCP) guidelines (see ICH: Efficacy Guidelines).
- Deidentified patient information (see Deidentified Patient Information). Reidentified patient information is not eligible for the exemption.

(Cal. Civ. Code §§ 1798.145(c), 1798.146, and 1798.148.)

The CCPA also excludes personal information governed by the following federal and state privacy statutes from every section **except** the CCPA's private right of action for certain data breaches:

- The federal Fair Credit Reporting Act (FCRA) (15 U.S.C. §§ 1681 to 1681x) (see Practice Note, FCRA Litigation: Key Issues and Considerations).
- The Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA) (see Practice Notes, GLBA: The Financial Privacy and Safeguards Rules and California Privacy and Data Security Law: Overview: Financial Privacy).
- The Driver's Privacy Protection Act of 1994 (18 U.S.C. §§ 2721 to 2725).

(Cal. Civ. Code § 1798.145(d) to (f).)

For more on the data breach private right of action that still applies to credit, financial, and driver's personal information, see Private Right of Action for Data Breaches.

CPRA Revisions: Preemption

The CPRA does not change the CCPA's general sections on conflicting provisions and preemption (Cal. Civ. Code §§ 1798.175 and 1798.180 (effective January 1, 2023)). However, it does alter the CCPA's specific exclusions that seek to avoid conflict with certain sector-specific privacy laws (Cal. Civ. Code § 1798.145 (effective January 1, 2023)). Revisions include:

- Altering the clinical trial exception to:
  - include biomedical research studies conducted under the same guidelines; and
  - qualify the exception on only selling or sharing the personal information in a manner consistent with the section unless participants are informed of the different use and provide consent.

  (Cal. Civ. Code § 1798.145(c)(1)(C) (effective January 1, 2023).)
- Excluding personal information governed by the Farm Credit Act of 1971 (12 U.S.C. §§ 2001 to 2279cc) from every CPRA section except the private right of action for certain data breaches (Cal. Civ. Code § 1798.145(e) (effective January 1, 2023)).

CPRA Revisions: New Exclusions

The CPRA also adds a number of new exclusions to protect certain special interests, such as for:

- Trade secrets (Cal. Civ. Code § 1798.100(f) (effective January 1, 2023)).
- Free speech and press rights for noncommerical activities protected by California's Constitution (Cal. Civ. Code § 1798.145(l) (effective January 1, 2023)).
- Certain commercial credit reporting agency actions from the CPRA's deletion and sale or sharing opt-out rights (Cal. Civ. Code § 1798.145(o) (effective January 1, 2023)).
- Household data from the CPRA's right to know, deletion, and correction business obligations (Cal. Civ. Code § 1798.145(p) (effective January 1, 2023)).
- Student grades, educational scores, or educational test results held for a local educational agency from the CPRA's deletion right and educational standardized assessments, including specific responses, from the right to know's disclosure requirements when disclosure could jeopardize its validity or reliability (Cal. Civ. Code § 1798.145(q) (effective January 1, 2023)).

- Physical items containing personal information, such as the consumer's photograph, if the consumer previously consented to their creation and other circumstances apply, from the CPRA's deletion and opt-out rights (Cal. Civ. Code § 1798.145(r) (effective January 1, 2023)).

Business that may qualify for one of these exclusions should carefully review the CPRA's specific requirements, definitions, restrictions, and caveats.

Conflict of Laws and Statutory Interpretation

The CCPA prescribes that in case of any conflicts with California laws, the law that affords the greatest privacy protections controls (Cal. Civ. Code § 1798.175). The CCPA also instructs courts that the new law "shall be liberally construed to carry out its purposes" (Cal. Civ. Code § 1798.194).

The CCPA's broad definitions and statutory requirement to liberally construe its text to protect personal information create the potential for expansive application and enforcement.

Both sections remain unchanged by the CPRA.

Consumer Rights

The CCPA grants consumers several rights, including:

- Notice and information rights (see General Notice Rights, Individual Right to Know, and Data Portability).
- Deletion rights (see Deletion Rights).
- Personal information sale prevention rights (see Sale Opt-Out and Opt-In Rights).
- Freedom from discrimination (see Freedom from Discrimination).

The California AG refers to the CCPA's bundle of information rights as the "right to know."

The CCPA also protects consumers against purported waivers of these rights (see Prohibition on Waiver of Applicability).

CPRA Revisions: New Consumer Rights

The CPRA creates new consumer rights to:

- Correct inaccurate personal information (see CPRA Revision: New Correction Rights).
- Opt-out of sharing personal information for cross-context behavioral advertising purposes (see CPRA Revisions: Sharing Opt-Out and Opt-In Rights).
- Restrict sensitive personal information processing (see CPRA Revisions: New Right to Restrict Sensitive Personal Information Processing).

General Notice Rights

The CCPA grants consumers the right to know a wide range of information about a business's personal information practices, including what personal information a business collects, sells, or discloses, the categories of third parties purchasing or receiving their data and how to exercise their CCPA rights. It spreads these obligations and rights out over several different sections (see Box, CCPA Provision and Regulation Index).

To help businesses understand their general notice obligations, the CCPA Regulations organize them into four distinct notice types:

- **Collection notices.** A business must provide this notice whenever it collects personal information (see Notice at Collection).
- **Privacy policy.** Every business must provide this notice (see Privacy Policy).
- **Opt-out right notices.** A business that sells personal information must provide this notice (see Opt-Out Right Notice).
- **Financial incentive notices.** A businesses must provide this notice whenever it offers a financial incentive, price difference, or service difference related to the collection, retention, or sale of personal information (see Notice of Financial Incentives).

(Cal. Code Regs. tit. 11, § 7010.)

For more on preparing each of these notices, see Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies.

CPRA Revisions: General Notice Rights

The CPRA reorganizes and expands these public notice requirements but does not change the four primary types of required notices outlined in the current CCPA Regulations. However, businesses should expect the California Privacy Protection Agency to update or issue new regulations regarding these required notices (see CPRA Regulation Tracker).

Shared Notice Presentation Requirements

The CCPA Regulations set out general presentation requirements that apply to all four public CCPA notices (see General Notice Rights). They require the business to design and present the notice information in a way that is easy to read and understandable to consumers, including:

- Using plain, straightforward language and avoiding technical or legal jargon.
- Making the policy readable by using the best format for the display, including on smaller screens, if applicable.
- Translating the policy, if applicable, so it appears in the language the business ordinarily uses to provide sales announcements, contracts, disclaimers, or other information to consumers in California.
- Ensuring consumers with disabilities can reasonably access the policy by, for example:
  - following generally recognized industry standards, such as the Web Content Accessibility Guidelines published by the World Wide Web Consortium for online notices (see W3C: Web Content Accessibility Guidelines (WCAG) Overview); and
  - for other contexts, describing how a consumer with a disability may access the policy in an alternative format.

(Cal. Code Regs. tit. 11, §§ 7012(a)(2)(A) to (D), 7013(a)(2)(A) to (D), 7016(a)(2)(A) to (D), and 7011(a)(2)(A) to (D).)

Notice at Collection

The CCPA's first notice obligation requires a business to disclose, before or at the point of collection, both:

- What personal information categories a business collects.
- Its intended use purposes.

(Cal. Civ. Code § 1798.100(b).)

The CCPA Regulations operationalize this provision by requiring a business to make a specific notice at collection readily available to consumers at or before the collection point (Cal. Code Regs. tit. 11, § 7001(l), 7010(b), and 7012; California AG Final Statement of Reasons for CCPA Regulations (CCPA FSOR) at 6 to 12 and California AG Initial Statement of Reasons for CCPA Regulations (CCPA ISOR) at 8 to 10).

The notice at collection must provide:

- A list of the personal information categories collected, presented in a way that provides consumers with a meaningful understanding of what the business collects.
- The business or commercial purpose for using the personal information categories.
- A link to or online location for the business's "Do Not Sell My Personal Information" notice (opt-out right notice), if applicable (see Opt-Out Right Notice).
- A link to or online location for the business's privacy policy (see Privacy Policy).

(Cal. Code Regs. tit. 11, § 7012(b).)

While the temporary exemption for employment-related personal information remains in effect, an employer's collection notice does not need to include links to an opt-out right notice or privacy policy (Cal. Code Regs. tit. 11, § 7012(f), (g); see Temporary Exemptions).

A business cannot:

- Collect any personal information if it does not provide the notice.
- Collect personal information categories not disclosed in the notice.
- Use collected personal information for unrelated purposes without providing the required notice.

(Cal. Civ. Code § 1798.100(b); Cal. Code. Regs tit. 11, § 7012(a)(5) to (6).)

The business must provide this notice at collection whenever and wherever it collects personal information, even in offline situations, such as when observing a consumer's physical behavior to create a profile. The CCPA Regulations clearly prohibit the surreptitious collection of personal information. (Cal. Code Regs. tit. 11, § 7012(a)(3), (6); CCPA ISOR at 9 and CCPA FSOR at 8 to 10.)

Businesses that collect personal information from indirect sources instead of directly from the consumer may find complying with the collection notice requirements difficult. The CCPA also requires third parties to give consumers explicit notice and an opportunity to opt out before re-selling personal information acquired from another business (Cal. Civ. Code § 1798.115(d); see Service Providers and Third Parties).

To help those businesses, the CCPA Regulations provide narrow exceptions to the notice at collection requirement if they either:

- Do not sell the consumers' personal information.
- Are a data broker that:
  - registered with the California AG (see Practice Note, California Privacy and Data Security Law: Overview: Data Broker Registration); and
  - provided a personal information sales opt-out instruction link with their registration submission (see OAG: Data Broker Registry and OAG: Data Broker Registration).

(Cal. Code. Regs tit. 11, § 7012(d) to (e).)

For more on preparing and presenting notices at collection, including specific requirements for offline, mobile, or online data collections, see Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies: Collection Notice. For model notices, see Standard Documents:

- Notice at Collection (CCPA and CPRA).
- CCPA Notice at Collection for California Employees and Applicants.
- CCPA Notice at Collection for California Independent Contractors.

CPRA Revisions: Notice at Collection

The CPRA rewrites and expands the CCPA's pre-collection disclosure obligations to include:

- The personal information categories the business will collect, including any sensitive personal information categories, along with:
  - the purposes for which it collects the personal information and sensitive personal information categories; and
  - whether that information is sold or shared.
- The retention period for each category of personal information or sensitive personal information, or the criteria used to determine the relevant retention period.

(Cal. Civ. Code § 1798.100(a) (effective January 1, 2023).)

As with the CCPA, the business cannot:

- Collect personal information or sensitive personal information categories not disclosed in a notice.
- Use the personal information or sensitive personal information it collects for additional purposes that are incompatible with use purposes disclosed in the collection notice.

(Cal. Civ. Code § 1798.100(a)(1), (2) (effective January 1, 2023).)

The CPRA also prohibits retaining personal information or sensitive personal information for time periods longer than reasonably necessary for each disclosed collection purpose (Cal. Civ. Code § 1798.100(a)(3) (effective January 1, 2023)).

The CPRA keeps the CCPA's requirement that third parties must give consumers explicit notice and an opportunity to opt-out before re-selling personal information acquired from another business and expands it to include re-sharing information shared by another business for cross-context behavioral advertising purposes (Cal. Civ. Code § 1798.115(d) (effective January 1, 2023)). However, the CPRA now explicitly allows a business that controls the collection of personal information about a consumer, but acts as a third party, to meet its collection notice obligation by prominently and conspicuously providing the required information on its internet website homepage (Cal. Civ. Code § 1798.100(b) (effective January 1, 2023)). This new provision should make it easier for businesses that acquire or indirectly collect personal information from sources other than the actual consumer to provide the required collection notices.

Privacy Policy

Several different CCPA sections require businesses to make affirmative disclosures to consumers using public notices (see Box, CCPA Provision and Regulation Index). The CCPA Regulations pull these disparate requirements together and define them as the business's "privacy policy" to distinguish them from the CCPA's other notice requirements (Cal. Code Regs. tit. 11, § 7001(p)).

The privacy policy provides consumers with detailed information about the business's personal information practices, including how it collects, uses, discloses, and sells personal information. It also explains the consumer's CCPA rights and tells the consumer how to exercise them. (Cal. Code Regs. tit. 11, § 7011.) The CCPA and CCPA Regulations list specific elements that a privacy policy must contain. For the complete list, see Box, Privacy Policy Required Elements List.

All businesses subject to the CCPA must make their privacy policy available to consumers:

- Online using a conspicuous link using the word "privacy" on the business's website homepage, if it operates one.
- In another manner conspicuously available to consumers, if it does not operate a website.
- On a mobile application's download or landing page and optionally in the app's settings menu.
- As part of any California-specific description of consumers' privacy rights, if provided.

(Cal. Civ. Code § 1798.130(a)(5); Cal. Code Regs. tit. 11, § 7011(b).)

The business must also ensure consumers can print the privacy policy out as a single document (Cal. Code Regs. tit. 11, § 7011(a)(2)(E)).

Businesses must review and update their privacy notice's content at least every 12 months (Cal. Civ. Code § 1798.130(a)(5)).

For more on preparing and presenting privacy policies, including providing meaningful disclosures, see Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies. For a model CCPA privacy policy, see Standard Document, CCPA Privacy Policy for California Residents.

CPRA Revisions: Privacy Notice

A business must still publicly post a privacy policy on its internet website that receives updates at least once every 12 months under the CPRA (Cal. Civ. Code § 1798.130(a)(5) (effective January 1, 2023)). California Privacy Protection Agency regulations should eventually provide more detailed guidance about the privacy policy's expected content and requirements (see CPRA Regulation Tracker). For a complete list of privacy policy elements directly added by CPRA, see Box, CPRA Revisions: Privacy Policy Required Elements List.

Opt-Out Right Notice

Businesses that sell personal information must provide consumers with a specific notice about their rights to opt-out of those sales (Cal. Civ. Code §§ 1798.120(b) and 1798.135; Cal. Code Regs. tit. 11, § 7013). The opt-out right notice must contain:

- A description of the consumer's right to opt-out of personal information sales (see Sale Opt-Out and Opt-In Rights).
- The interactive form that enables a consumer to submit an opt-out request online, if the business operates a website. Otherwise, a description of the offline submission method.
- Instructions for any other opt-out submission methods the consumer may use.

(Cal. Civ. Code § 1798.135; Cal. Code Regs. tit. 11, § 7013(c).)

A business that shares personal information with service providers should also include a statement disclosing that practice to qualify for the CCPA's personal information sales service provider exception (Cal. Civ. Code § 1798.140(t)(2)(C)(i); see Service Provider Exception and Qualifying for the Service Provider Sales Exception).

The opt-out right notice's presentation and location depends on the business's operation methods. The vast majority of business are likely to place the notice on the internet page where it sends consumers clicking on a "Do Not Sell My Personal Information" link (Cal. Civ. Code § 1798.135; Cal. Code Regs. tit. 11, § 7013(b)). Businesses selling personal information collected through offline methods must provide consumers with opt-out notices using offline methods (Cal. Code Regs. tit. 11, § 7013(b)(3)). For more on placement in unique situations, such as when a business does not operate a website at all or operates a separate, California-only website homepage, see Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies: Opt-Out Right Notice.

Importantly, a business can **avoid** posting the opt-out notice and opt-out links if it:

- Does not sell any personal information collected when the notice is absent.
- Affirmatively states in its privacy policy that it does not sell personal information.

(Cal Code Regs tit. 11, § 7013(d).)

A business cannot sell personal information collected when it did not post an opt-out notice unless it obtains that consumer's affirmative authorization (Cal Code Regs tit. 11, § 7013(e)).

To supplement the opt-out notice, businesses may use this uniform opt-out icon:

(Cal. Code Regs. tit. 11, § 7013(f); Cal. Civ. Code § 1798.185(a)(4)(C).)

The icon cannot replace any requirement to post the opt-out notice or the "Do Not Sell My Personal Information" text link. When used, the icon must appear in approximately the same size the webpage's other icons. (Cal. Code Regs. tit. 11, § 7013(f).)

To download the icon from the California AG's website, see OAG: CCPA Opt-Out Icon.

For more on responding to opt-out requests, including the submission form requirements, see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests.

CPRA Revisions: Opt-Out Right Notice

The CPRA expands the opt-out right notice to cover the consumer's new rights to opt out of sharing personal information for cross-context behavioral advertising and to restrict sensitive personal information use (Cal. Civ. Code § 1798.135(a) (effective January 1, 2023)). The California Privacy Protection Agency will likely issue new

or revised regulations on the notice's exact requirements, but the CPRA's changes include:

- Using the title "Do Not Sell or Share My Personal Information" for the links to the internet page that processes a consumer's request to opt out of personal information sales and sharing.
- Using the title "Limit the Use of My Sensitive Personal Information" for links to the internet page that processes a consumer's request to limit the use or disclosure of their personal information.
- Alternatively, allowing a business to:
  - use a single, clearly labeled link instead of separate opt-out links if the page easily allows a consumer to exercise both rights; or
  - not provide the links at all if it enables consumers to exercise their opt-out rights through browser- or platform-based preference signals, like Do Not Track (DNT), as established by future regulations.
- Giving the consumer a financial incentives notice whenever any opt-out request response informs the consumer of a charge to use any product or service.

(Cal. Civ. Code § 1798.135(a), (b) (effective January 1, 2023); see CPRA Regulation Tracker.) The CPRA also simplifies the CCPA's complicated sales definition exception for service providers, which required the business' opt-out notice to disclose that it shared personal information with service providers to perform necessary business purposes (Cal. Civ. Code § 1798.140(t)(2)(C)(i); Cal. Civ. Code § 1798.140(ad) (effective January 1, 2023); see CPRA Revisions: Service Provider Exception).

Notice of Financial Incentives

The CCPA and CCPA Regulations place a fourth notice obligation on businesses that provide financial incentives related to the collection, retention, or sale of personal information, which may result in price, quality, or service differences. This requirement was established, in part, to address the tension between the CCPA's prohibition on discriminating against consumers exercising their CCPA rights, such as opting out of personal information sales, and its specific provisions allowing certain financial incentives (see Freedom from Discrimination and Lawful Financial Incentive Offers).

One key aspect to lawfully providing financial incentives is explaining the offer's material terms in way that enables consumers to make informed decisions about opting-in to the program (Cal. Civ. Code § 1798.125(b)(2), (3)). A notice of financial incentive must provide:

- A succinct summary of the financial incentive offered.
- The financial incentive's material terms, including the categories of personal information that the offer may impact and the value of the consumer's data to the business.
- Instructions for opting-in to the financial incentive, notice about the consumer's right to withdraw from program at any time, and instructions on how to exercise that right.
- An explanation of how the financial incentive reasonably relates to the value of the consumer's data to the business, including:
  - a good-faith estimate of the value of the consumer's data that forms the basis for the incentive; and
  - a description of the method used to calculate that value (see Calculating Consumer Data Value).

(Cal. Code Regs. tit. 11, § 7016(b).)

Businesses offering financial incentives must make the notice readily available where consumers will encounter it before opting into the program (Cal. Code Regs. tit. 11, § 7016(a)(2)(E)). However, if a separate privacy policy section contains all of the required financial incentive notice information, an online business can provide the notice by linking directly to that section (Cal. Code Regs. tit. 11, § 7016(a)(3)).

For more on financial incentive notice presentation and delivery requirements, see Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies: Financial Incentive Notice.

CPRA Revisions: Notice of Financial Incentives

The CPRA retains the financial incentives notice requirement and expands it to cover payments to consumers for retaining personal information or sharing it for cross-context behavioral advertising purposes (Cal. Civ. Code § 1798.125(b) (effective January 1, 2023)). The California Privacy Protection Agency will likely issue new or revised regulations on the notice's exact requirements (see CPRA Regulation Tracker).

Individual Right to Know

The CCPA grants consumers an individualized right to know what personal information a business collected, sold, or disclosed about them, including the categories of third parties purchasing or receiving their data and the specific pieces of personal information held (Cal. Civ. Code §§ 1798.100, 1798.110, 1798.115, and 1798.130;

(Cal. Code Regs. tit. 11, §§ 7024 and 7031). The CCPA Regulations refer to this specific information right as a "request to know," where verified consumers can ask the business to send them:

- The specific pieces of personal information collected about the consumer (see Data Portability).
- The personal information categories collected about the consumer.
- The source categories from which the business collected the personal information.
- The personal information categories sold, if any, and the categories of third parties purchasing that personal information.
- The personal information categories disclosed for a business purpose, if any, and the categories of third parties receiving that personal information.
- The business or commercial purpose for collecting or selling personal information.

(Cal. Code Regs. tit. 11, § 7001(r).)

However, the CCPA tempers these rights by:

- Requiring the consumer to reasonably verify their identity in light of the nature of the personal information requested.
- Limiting the request response scope to only personal information collected, sold, or disclosed in the past 12 months.
- Only permitting a maximum of two requests in a 12-month period.

(Cal. Civ. Code §§ 1798.100(c), (d), 1798.130(a)(2), and 1798.140(y).)

For more on responding to consumer right to know requests, see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests.

CPRA Revisions: Right to Know

The CPRA retains a consumer's individualized right to know, but revises it by:

- Expanding the right to include the same information about any personal information shared for cross-context behavioral advertising.
- Allowing a business to meet this obligation by directing consumers to its corresponding privacy policy disclosures, **if** those disclosures exactly match what the business would provide the consumer in an individualized disclosure. This does not apply to a consumer's request for the specific pieces of personal information collected about them.
- Allowing the California Privacy Protection Agency to adopt regulations that increase or remove the response's current 12-month look-back period, unless providing information for the longer time period proves impossible or would involve a disproportionate effort. The expanded disclosure timeframe would only apply to personal information collected on or after January 1, 2022.

(Cal. Civ. Code §§ 1798.110(a), (b), 1798.115(a), (b), and 1798.130(a)(2) to (4) (effective January 1, 2023); see CPRA Regulation Tracker.)

The CPRA added a general, broader exclusion stating that compliance with the statute does not require a business, service provider, or contractor to:

- Reidentify or otherwise link information to maintain it as personal information, if it would not normally do so.
- Retain personal information that it would not normally retain.
- Maintain information in identifiable, linkable, or associable form, or collect, obtain, retain, or access any data or technology so that it can link or associate a verifiable consumer request with personal information.

(Cal. Civ. Code § 1798.145(j) (effective January 1, 2023).)

As a result, the CPRA deleted similar language contained in the CCPA's right know section as redundant (Cal. Civ. Code § 1798.110(d); Cal. Civ. Code § 1798.110 (effective January 1, 2023)).

Data Portability

The requirement to provide the "specific pieces of personal information" the business has collected about that consumer creates what many refer to as a data portability right (Cal. Civ. Code §§ 1798.100(a), 1798.110(a)(5), (b), (c)(5) and 1798.130(a)(2)). The CCPA defines the term "collected" quite broadly. It includes:

- Buying.
- Renting.
- Gathering.
- Obtaining.
- Receiving.
- Accessing.

It also includes any means used to obtain the data, including:

- Actively from the consumer.
- Passively from the consumer.
- By observing the consumer's behavior.

Businesses must also provide derived personal information like inferences generated about a consumer unless a clear exception applies. Recent guidance from the California AG confirms that internal profile inferences generated by analyzing personal information and external profile inferences obtained from third parties, like a person's "influencer" score, meet the CCPA's collected personal information definition and businesses should disclose them when responding to a consumer's request to know (see California AG Opinion 20-303 (March 10, 2022) and Legal Update, California AG Issues Opinion on Data Inferences and CCPA Consumer Rights). Given the CCPA's liberal construction direction, a business should consider including all the personal information it holds about the consumer when responding to requests unless the CCPA Regulations or a clear CCPA exception support withholding it (see Conflict of Laws and Statutory Interpretation).

For more on responding to consumer data portability requests, see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests.

CPRA Revisions: Data Portability

The CPRA retains both the CCPA's data portability right and its expansive definition for the term collected (Cal. Civ. Code §§ 1798.110(a)(5) and 1798.140(f) (effective January 1, 2023)). However, it clarifies that the term "specific pieces of information" does not include data generated to help ensure security and integrity, which it defines as the ability of:

- Networks or information systems to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.
- Businesses to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions and to help prosecute those responsible for those actions.
- Businesses to ensure the physical safety of natural persons.

(Cal. Civ. Code §§ 1798.130(a)(3)(B)(iii) and 1798.140(ac).)

It also specifically allows the California Privacy Protection Agency to draft regulations excluding other data, such as system log information, from the consumer's data portability right (Cal. Civ. Code § 1798.185(a)(14); see CPRA Regulation Tracker).

The CPRA's amendments do not change the California AG's analysis on when to include internal or external inferences in a consumer's right to know response (see California AG Opinion 20-303 (March 10, 2022) and Legal Update, California AG Issues Opinion on Data Inferences and CCPA Consumer Rights).

Deletion Rights

The CCPA grants consumers the right to request that a business and its service providers delete their personal information (Cal. Civ. Code § 1798.105(a)). However, this is not an absolute right and a business may deny deletion requests when it needs to retain personal information for certain statutory business reasons (Cal. Civ. Code § 1798.105(d)).

For more on responding to consumer deletion requests, see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests.

CPRA Revisions: Deletion Rights

The CPRA retained the consumer's right to delete, but it revised the circumstances under which a business may deny the deletion requests (Cal. Civ. Code § 1798.105(d) (effective January 1, 2023)). The CPRA also requires:

- A business to notify:
  - all third parties to whom it has sold or shared the consumer's personal information to delete that information unless this proves impossible or involves disproportionate effort; and
  - its service providers or contractors to delete the consumer's personal information from their records.
- A service provider or contractor to:
  - cooperate with the business in responding to a verifiable consumer request;
  - delete or enable the business to delete the consumer's personal information at the business's direction;
  - notify its own service providers or contractors to delete the consumer's personal information that they collect, use, process, or retain.
  - notify any service providers, contractors, or third parties who may have accessed the consumer's personal information from or through it rather than the original business, to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.

(Cal. Civ. Code § 1798.105(c) (effective January 1, 2023).)

CPRA Revision: New Correction Rights

The CPRA grants consumers a new right to request that a business correct any inaccuracies in the personal information it holds about them, taking into account the nature of the personal information and the personal information's processing purposes (Cal. Civ. Code § 1798.106 (effective January 1, 2023)). As with the consumer's deletion right, the correction right is not absolute. A business must use commercially reasonable efforts to correct inaccurate personal information once it receives the consumer's request (Cal. Civ. Code § 1798.106(c) (effective January 1, 2023)).

The California Privacy Protection Agency should establish regulations governing how businesses respond to verified consumer correction requests, including resolving disagreements about the information's accuracy and the possibility of appending a written addendum to a consumer's record when the request involves the consumer's health (Cal. Civ. Code § 1798.185(a)(8); CPRA Regulation Tracker).

For more on responding to consumer correction requests, see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests: CPRA Revisions: Correction Request Substantive Response.

Sale Opt-Out and Opt-In Rights

Consumers at least 16 years old can prevent sales of their personal information at any time by directing a business to stop (Cal. Civ. Code § 1798.120(a)). This is known as the CCPA's right to opt-out.

For consumers under age 16, the CCPA provides a right to opt-in by prohibiting a business from selling any of their personal information unless it first:

- Obtains affirmative, opt-in consent from a consumer between ages 13 and 15.
- A parent or legal guardian affirmatively authorizes the sale for any consumer under age 13.

(Cal. Civ. Code § 1798.120(c) to (d).)

The business must have actual knowledge of the minor's age for the sale prohibition to apply. However, the CCPA treats a business's willful disregard of the consumer's age as actual knowledge (Cal. Civ. Code § 1798.120(c)).

Once a consumer opts-out or refuses to opt-in, the business must honor the request unless that consumer provides express authorization to resume personal information sales (Cal. Civ. Code §§ 1798.120(d) and 1798.135(a)(4)). Business must also wait at least 12 months before asking the consumer to reauthorize future personal information sales (Cal. Civ. Code § 1798.135(a)(5)).

For more on whether a disclosure is a sale under the CCPA, see Distinguishing Between Sales and Business Purposes Disclosures. For more on responding to opt-out right requests and obtaining opt-in consent, see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests.

Vehicle and Vessel Information Exception

The CCPA provides a narrow exception to this personal information sales restriction right solely to enable warranty or recall related repairs, for motor vehicle information, vessel information, or ownership information retained or shared between motor vehicle or vessel dealers and manufacturers. The dealer or manufacturer cannot sell, share, or use the exempt information for any other purpose. The exception contains specific definitions for the terms motor vehicle, vehicle information, vessel information, ownership information, and vessel dealer that a business should review before determining whether the exception applies. (Cal Civ. Code § 1798.145(g).)

CPRA Revisions: Sharing Opt-Out and Opt-In Rights

The CPRA expands the CCPA's personal information sales opt-out and opt-in rights to include sharing personal information with a third party for cross-context behavioral advertising purposes (Cal. Civ. Code §§ 1798.120 and 1798.140(ah) (effective January 1, 2023)).

However, other CPRA revisions may end up narrowing the practical impact of this right's expansion, including that, by definition:

- Service providers and contractors are not third parties (Cal. Civ. Code § 1798.140(ai) (effective January 1, 2023)). This means that an opt-out request does not prevent a business from sharing a consumer's personal information with those entities to conduct cross-context behavioral advertising. Similarly, the business would not need to obtain opt-in consent before sharing a minor's personal information with its service providers or contractors.
- Consumer requests to intentionally interact with a third party, perhaps by actively clicking on a third party's "like" button, do not result in sharing or selling information to a third party, even if the business received monetary consideration for the consumer's action (Cal. Civ. Code § 1798.140(ad)(2)(A), (ah)(2)(A) (effective January 1, 2023)). This may broaden the

conduct businesses can engage in after receiving an opt-out request or without obtaining opt-in consent. Passive interactions, including hovering over, muting, pausing, or closing a given piece of content do not indicate a consumer's intent to interact with the third party (Cal. Civ. Code § 1798.140(s) (effective January 1, 2023)).

- Sharing is limited to communications by the business to a third party for cross-context behavioral advertising (Cal. Civ. Code § 1798.140(ah) (effective January 1, 2023)). This suggests the consumer's opt-out or opt-in rights do not apply when the business shares (but does not sell) personal information with third parties for other purposes. The sales definition does not contain a similar purpose restriction (Cal. Civ. Code § 1798.140(ad) (effective January 1, 2023)).

Businesses should expect the California Privacy Protection Agency to provide regulations on the scope and operation of the consumer's opt-out and opt-in rights (see CPRA Regulation Tracker).

For more on how the CPRA changes the CCPA's sales and third party definitions, see CPRA Revisions: Sales Definition and CPRA Revisions: Service Provider, Contractor, Third Party Definitions.

CPRA Revisions: New Right to Restrict Sensitive Personal Information Processing

The CPRA grants a consumer the right to restrict how a business uses and discloses their sensitive personal information (Cal. Civ. Code § 1798.121 (effective January 1, 2023)). This restriction right does not apply to sensitive personal information that the business collected or processed without the purpose of inferring characteristics about a consumer (Cal. Civ. Code § 1798.121(d) (effective January 1, 2023)). Regulations developed by the California Privacy Protection Agency should further define when a business collects or processes information without such as purpose (Cal. Civ. Code § 1798.185(a)(19)(C); Cal. Civ. Code § 1798.121(d) (effective January 1, 2023); see CPRA Regulation Tracker).

At any time, the consumer can restrict the business's use and disclosure of such information to just:

- Actions necessary for the performance of services or provision of goods, that an average consumer requesting those goods or services would reasonably expect.
- Use that helps to ensure security and integrity, but only to the extent that the use is reasonably necessary and proportionate.
- Short-term, transient use, including but not limited to non-personalized advertising shown as part of a consumer's current interaction with the business, if the business **does not**:
  - disclose the sensitive personal information to another third party; or
  - use it to build a profile about the consumer or otherwise alter the consumer's experience outside their current interaction with the business.
- Perform services for 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 for the business.
- Activities required:
  - 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.
- As otherwise authorized by regulations the California Privacy Protection Agency may adopt.

(Cal. Civ. Code §§ 1798.121(a) and 1798.140(e)(2), (4), (5), (8) (effective January 1, 2023); Cal. Civ. Code § 1798.185(a)(19)(C); see CPRA Regulation Tracker.)

For more on what personal information is considered sensitive, see CPRA Revisions: New Sensitive Personal Information Category.

Freedom from Discrimination

The CCPA explicitly protects consumers exercising their rights under the CCPA from discrimination (Cal. Civ. Code § 1798.125(a)(1)). It generally prohibits businesses from:

- Denying goods or services to those consumers.
- Charging them different prices or rates, including by using discounts or other benefits.
- Providing them with a different level or quality of service.
- Suggesting that they may receive a different level or quality of service.

(Cal. Civ. Code § 1798.125(a)(1)(A) to (D).)

A practice is discriminatory (and therefore prohibited) if it treats a consumer differently because the person exercised its CCPA-related rights (Cal. Code Regs. tit. 11, § 7080(a); CCPA FSOR at 50 to 52, CCPA ISOR at 36 to 37).

A practice is not discriminatory if it:

- Validly denies a consumer rights request for a reason the CCPA or CCPA Regulations permit.
- Charges a reasonable fee for manifestly unfounded or excessive consumer rights requests, as the CCPA permits.
- Directly results from a price or service difference enacted to comply with state or federal law.

(Cal. Code Regs. tit. 11, § 7080 (c), (f) to (g).)

For more on identifying discriminatory practices, see Distinguishing Between Discriminatory Practices and Financial Incentive Offers.

CPRA Revisions: Freedom from Discrimination

The CPRA expands this right to prohibit retaliating against an employee, applicant for employment, or independent contractor for exercising their CPRA rights (Cal. Civ. Code § 1798.125(a)(1)(E) (effective January 1, 2023)).

Lawful Financial Incentive Offers

Although businesses cannot discriminate, the CCPA does permit a business to:

- Impose price, quality, or service difference reasonably related to the business value of the consumer's data.
- Make financial incentive offers (including payments).

(Cal. Civ. Code § 1798.125(b)(1).)

When implementing price differential or financial incentive programs, a business must:

- Ensure that the program reasonably reflects the value a consumer's data provides to the business (see Calculating Consumer Data Value).
- Notify consumers about the program's material terms, including that the consumer may revoke consent at any time (see Notice of Financial Incentives).
- Not engage in discriminatory, unjust, unreasonable, coercive, or usurious financial incentive practices.
- Obtain the consumer's prior opt-in consent.

(Cal. Civ. Code § 1798.125(a)(2), (b)(1), (4); Cal. Code Regs. tit. 11, § 7080(b).)

A business cannot offer a financial incentive or difference in price or service if it cannot calculate a consumer data value estimate in good faith or cannot show that a financial incentive or difference in price or service reasonably relates to that estimate (Cal. Code Regs. tit. 11, § 7080(b); see Calculating Consumer Data Value).

For more on developing financial incentive offers, see Establish Financial Incentive and Anti-Discrimination Programs.

CPRA Revisions: Lawful Financial Incentive Offers

The CPRA add a statement specifically declaring that the anti-discrimination clause does not prevent a business from offering loyalty, rewards, premium features, discounts, or club card programs consistent with the CPRA's requirements (Cal. Civ. Code § 1798.125(a)(3) (effective January 1, 2023)).

Prohibition on Waiver of Applicability

The CCPA explicitly prohibits any agreement or contract provision that seeks to waive or limit a consumer's rights under the CCPA. This includes waiving any right to a remedy or specific means of enforcement. A consumer can still opt not to request information from a business or decline to take other actions under the CCPA (Cal Civ. Code § 1798.192).

CPRA Revisions: Prohibition on Waiver of Applicability

The CPRA expands the CCPA's non-waiver section to specifically identify representative action waivers as void and unenforceable actions deemed contrary to public policy and make other minor changes to incorporate the CPRA's new rights (Cal Civ. Code § 1798.192 (effective January 1, 2023)). For more on the enforceability of a class action waiver, see Practice Note, Class Arbitration Waivers in the US: Case Tracker and Standard Document, Mutual Agreement to Arbitrate Employment-Related Disputes (CA), and Standard Clause, Mandatory Arbitration of Employment-Related Claims (CA).

Business Obligations

The numerous consumer rights granted by the CCPA obligate businesses to take several measures to comply with its requirements. Businesses should review their data inventory, collection, and sharing practices to determine which sections of the CCPA apply to their businesses, particularly if they sell consumer personal information

(see Distinguishing Between Sales and Business Purposes Disclosures).

Even for businesses that do not sell personal information, the CCPA's use restrictions and consumer disclosures may require implementation of clear internal processes for responding to consumer requests.

To meet its CCPA obligations, a covered business should:

- Protect personal information (see Implement Reasonable Security Practices and Procedures).
- Make all required notice disclosures (see Publish and Maintain Required Notices).
- Review all price, service, or quality differences relating to personal information relating to the collection, retention, or sale of personal information (see Establish Financial Incentive and Anti-Discrimination Programs).
- Establish internal procedures to receive, verify, process, and respond to consumer rights requests (see Establish Consumer Rights Response Program).
- Comply with employee training and recordkeeping requirements (see Training and Recordkeeping Obligations).
- Review service provider and third-party personal information data sharing contracts for alignment with the CCPA's requirements (see Service Providers and Third Parties).

For a checklist on meeting the CCPA's different obligations, see Implementing the California Consumer Privacy Act (CCPA) Checklist.

CPRA Revisions: Business Obligations

The CPRA rewrites the CCPA's opening section to specifically focus on the general duties of a business that collects or uses personal information (Cal. Civ. Code § 1798.100 (effective January 1, 2023)). It expands a business's obligations regarding personal information in several ways, including:

- Imposing clear data minimization and purpose limitation requirements (see CPRA Revisions: Data Minimization and Purpose Limitation).
- Deleting personal information after its retention is no longer reasonably necessary for its disclosed collection purpose (see CPRA Revisions: Retention Restrictions).
- Establishing audit requirements for high-risk processing activities (see CPRA Revisions: High Risk Audit Requirements).
- Requiring written contracts containing specific provisions whenever it shares or sells personal information to a third party or discloses it to a service provider or contractor for a business purpose (see CPRA Revisions: Required Contract Provisions).

CPRA Revisions: Data Minimization and Purpose Limitation

The CPRA directs the business to:

- Limit its collection, use, retention, and sharing of a consumer's personal information to actions reasonably necessary and proportionate to achieve:
  - the purposes for which the personal information was collected or processed; or
  - another disclosed purpose that is compatible with the context of the personal information collection.
- Not further process the information in a manner incompatible with those purposes.

Cal. Civ. Code § 1798.100(c) (effective January 1, 2023)

This new obligation may require businesses to take a hard look at their current data use practices and make significant changes, including to practices commonly found in the US, such as perpetual personal information retention or extended secondary data uses. Implementing strong data governance and review programs may also help the business ensure that its current and proposed personal information collection, use, retention, and sharing meet the CPRA's new reasonably necessary and proportional tests.

CPRA Revisions: Retention Restrictions

A new CPRA privacy policy content requirement to disclose personal information retention periods also creates a corresponding business obligation to delete that information once the retention period expires. Under the CPRA, a business that controls the collection of personal information must tell consumers:

- The length of time it intends to retain each category of personal information collected, including sensitive personal information.
- Alternatively, if providing an exact timeframe is not possible, the criteria used to determine the expected retention period.

(Cal. Civ. Code §§ 1798.100(a)(3) (effective January 1, 2023).)

Importantly, the business cannot set a longer retention period than what is reasonably necessary for the disclosed purpose (Cal. Civ. Code §§ 1798.100(a)(3) (effective January 1, 2023)).

Businesses should establish policies and procedures that both:

- Determine the appropriate retention time period or criteria for each personal information category collected based on the disclosed use purposes.
- Ensure the business actually deletes personal information once the publicly disclosed retention period expires.

CPRA Revisions: High Risk Audit Requirements

When a business's personal information processing activities present a significant risk to consumers' privacy or security, regulations eventually promulgated under the CPRA will require it to:

- Conduct annual cybersecurity audits.
- Regularly submit risk assessments regarding their personal information process activities to the California Privacy Protection Agency.

(Cal. Civ. Code § 1798.185(a)(15).)

Implement Reasonable Security Practices and Procedures

The CCPA does not directly impose data security requirements. However, it does establish a private right of action for certain data breaches that result from violations of a business's duty to implement and maintain reasonable security practices and procedures appropriate to the risk (Cal. Civ. Code § 1798.150(a)(1); see Private Right of Action for Data Breaches).

To help minimize the risk of a consumer action, businesses must implement and maintain reasonable security practices and procedures that are appropriate to the nature of the protected personal information.

The CCPA does not define reasonable security and it is not codified elsewhere in California law. However, other California statutes similarly require businesses that own, license, or maintain personal information about California residents to provide reasonable security for that information (Cal. Civ. Code § 1798.81.5(a); Practice Note, California Privacy and Data Security Law: Overview: Data Security Safeguards).

The California AG's 2016 California Data Breach Report also contains recommendations that may equate to reasonable security, including adopting the the Center for Internet Security's Critical Security Controls as a minimum base-level in developing a comprehensive information security program (see OAG: California Data Breach Report (February 2016)).

For more on reasonable data security practices generally, see Information Security Toolkit and Cybersecurity Tech Basics Toolkit.

For more on California's data breach laws, see Practice Note, California Privacy and Data Security Law: Overview: Breach Notification and State Q&A, Data Breach Notification Laws: California.

CPRA Revisions: Implement Reasonable Security Practices and Procedures

The CPRA makes the CCPA's implied data security requirements explicit. Under the CPRA, a covered business must implement reasonable security procedures and practices appropriate to the nature of the personal information to protect it from unauthorized or illegal access, destruction, use, modification, or disclosure (Cal. Civ. Code § 1798.100(e) (effective January 1, 2023)). The section incorporates the requirements of California's existing data security safeguards law (Cal. Civ. Code § 1798.81.5(a); Practice Note, California Privacy and Data Security Law: Overview: Data Security Safeguards).

It also defines the term security and integrity to mean the ability of:

- Networks or information systems to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.
- Businesses to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions and to help prosecute those responsible for those actions.
- Businesses to ensure the physical safety of natural persons.

(Cal. Civ. Code § 1798.140(ac) (effective January 1, 2023).)

Publish and Maintain Required Notices

All covered businesses must publish several disclosures regarding their personal information practices and the consumer's rights under the CCPA (see General Notice Rights). Those public disclosures include:

- Notices at collection (see Notice at Collection).
- A privacy policy (see Privacy Policy).

- A notice of the right to opt-out, for businesses that sell personal data (see Opt-Out Right Notice).
- A notice of financial incentives, if applicable (see Notice of Financial Incentives and Lawful Financial Incentive Offers).

Businesses should regularly review their CCPA notices to ensure the information provided remains accurate and up to date. They should also audit all consumer request submission methods, opt-out tools, and other similar contact or request operations to ensure they work as descripted. At minimum, the business must review its privacy policy once every 12 months (Cal. Civ. Code § 1798.130(a)(5)).

For more on preparing these disclosures, see Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies. For more on general considerations when drafting privacy notices, see Practice Note, Drafting Privacy Notices.

CPRA Revisions: Publish and Maintain Required Notices

The CPRA reorganized, consolidated, and expanded a business's public notice requirements, but it did not change the four core notice types (Cal. Civ. Code §§ 1798.100(a), (b), 1798.125(b), 1798.130(a)(5), and 1798.135(a) (effective January 1, 2023); see CPRA Revisions: General Notice Rights).

One important notice change that also creates a new business obligation is the requirement to tell consumers:

- The length of time it intends to retain each category of personal information, including sensitive personal information.
- Alternatively, if providing an exact timeframe is not possible, the criteria used to determine the expected retention period.

(Cal. Civ. Code §§ 1798.100(a)(3) (effective January 1, 2023).)

Importantly, the business cannot set a longer retention period than what is reasonably necessary for the disclosed purpose (Cal. Civ. Code §§ 1798.100(a)(3) (effective January 1, 2023)).

Businesses should establish policies and procedures that both establish the relevant retention time periods or criteria and ensure the business actually deletes personal information once the publicly stated retention period expires (see CPRA Revisions: Retention Restrictions).

For more on the CPRA's consumer notice revisions, see Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies.

Establish Financial Incentive and Anti-Discrimination Programs

Many businesses offer loyalty programs, premium services, and other similar programs that use and sometimes share personal information collected from their customers. If not properly reviewed and formatted, these programs may run afoul of the CCPA's anti-discrimination requirements (see Freedom from Discrimination).

Businesses must carefully review these programs to see if they can take advantage of the CCPA's financial incentive exceptions and ensure:

- The program structure does not discriminate against a consumer exercising their CCPA-related rights (see Distinguishing Between Discriminatory Practices and Financial Incentive Offers).
- The financial incentives reasonably relate to the value it receives from consumer's personal information (see Calculating Consumer Data Value).
- Consumers receive accurate and complete financial incentive notices before opting into the program (see Notice of Financial Incentives).

CPRA Revisions: Customer Loyalty Programs

The CPRA resolves one area of ambiguity by explicitly permitting loyalty, rewards, premium features, discounts, or club card programs consistent with the CPRA's requirements. Those programs, however, must still provide the required financial incentive notice, obtain the consumer's consent, and cannot discriminate against consumers who exercise their CPRA rights. (Cal. Civ. Code § 1798.125(a)(3), (b) (effective January 1, 2023).)

Distinguishing Between Discriminatory Practices and Financial Incentive Offers

The CCPA's somewhat contradictory statutory language creates clear tension between the prohibition on discrimination and permitted pricing differentials. It remains uncertain how these permitted pricing differentials may work in practice.

To help businesses better understand these requirements, the CCPA Regulations provide different examples of permissible and impermissible conduct. One example compares a music streaming business with a free service and a premium service costing $5 per month. When the business only allows premium subscribers to opt-out of personal information sales, the practice is:

- **Not discriminatory**, if the $5 per month payment reasonably relates to the value that those blocked personal information sales provide the business.
- **Discriminatory**, if the value the business receives from selling that personal information does not reasonably relate to the $5 monthly charge.

(Cal. Code Regs. tit. 11, § 7080(d)(1); CCPA FSOR at 51, CCPA ISOR at 37.)

A similar example involves a grocery store's loyalty program that gives participants coupons and special discounts when they provide their phone numbers. Removing consumers from that loyalty program after they opt out of personal information sales violates the CCPA's non-discrimination requirement unless the grocery store can demonstrate that the value of the program's coupons and special discounts reasonably relates to the business value of the consumer's data. (Cal. Code Regs. tit. 11, § 7080(d)(3).)

The CCPA Regulations also provide two other examples that explore both discriminatory practices and the proper handling of deletion request by analyzing:

- A clothing store's loyalty program that emails participants a $5 coupon each time they spend $100 at the store.
- An online bookseller that collects consumer information, including email addresses, browsing activity, and purchase history, but periodically provides discount offers from browser pop-up windows as the consumer visits the website.

When a consumer submits a request to delete all personal information to each business, but wants to continue participation in loyalty program or receiving discounts:

- The clothing store **can** deny the deletion request for the consumer's email address and spending history, because managing the program's benefits requires both data elements.
- The online bookseller **cannot** deny the deletion request for the consumer's email address and spending history, because it does not need those data elements to keep providing the consumer with periodic browser-based online discount offers.
- Preventing the consumer from receiving discount offers after the deletion request is discriminatory unless the store can demonstrate that the discount offers' value reasonably relates to the business value of the consumer's deleted data.

(Cal. Code Regs. tit. 11, § 7080(d)(2), (4).)

The continued ambiguity around permitted and prohibited discriminatory practices places covered businesses in a difficult position. However, as enforcement responsibility for this section rests solely with the California AG and also requires both a written violation notice and a 30-day cure period, businesses operating in good faith to balance the CCPA's non-discrimination and price difference sections should have time to adjust their practices as needed (see Enforcement).

On January 28, 2022, the California AG announced that it sent a series of 30-day cure notices to major corporations in the retail, home improvement, travel, and food service industries alleging that their customer loyalty programs did not comply with the CCPA's financial incentive requirements. The California AG noted:

- Offline data collections, such as when a customer enters their telephone number at a grocery store to receive a discount or a brick-and-mortar store tracks customer purchases to grant loyalty rewards like redeemable points or free gifts, are financial incentives.
- Loyalty programs that collect personal information must provide a financial incentive notice that clearly describes its material terms and obtain the consumers prior opt-in consent.
- California businesses that operate loyalty programs should review them for CCPA compliance and be transparent about how they use their customer's data.

(See OAG: On Data Privacy Day, Attorney General Bonta Puts Businesses Operating Loyalty Programs on Notice for Violations of California Consumer Privacy Act.)

When reviewing a price or service difference, a business should consider the following factors:

- Ensuring transparent and clear written disclosures around the incentive (see Notice of Financial Incentives).
- Analyzing and documenting the value that the consumer's personal information provides to the business, in good faith (see Calculating Consumer Data Value).

Calculating Consumer Data Value

Establishing a valid financial incentive program requires the business to calculate the value of the consumer's data using reasonable and good faith methods (Cal. Civ. Code § 1798.125(a)(2), (b); Cal. Code Regs. tit. 11, §§ 7080(b) and 7081).

The CCPA Regulations provide several calculation options for business to consider using one of the following methods:

- Marginal value to the business of the sale, collection, or deletion of a consumer's data.
- Average value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data.
- Revenue generated by the business from the sale, collection, or retention of consumers' personal information.
- Expenses related to the sale, collection, or retention of consumer's personal information.
- Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference.
- Profit generated by the business from the sale, collection, or retention of consumers' personal information.
- Any other practical and reliable good-faith method of calculation.

(Cal. Code Regs. tit. 11, § 7081(a).)

Businesses may also consider the value of the data from all natural persons in the US to the business and not just consumers (California residents) when calculating value (Cal. Code Regs. tit. 11, § 7081(b); CCPA FSOR at 53).

The California AG discussed the difficulties with calculating value and acknowledged the current absence of generally accepted methodologies when developing the CCPA Regulations (CCPA FSOR at 52 and 53, CCPA ISOR at 37 to 39). As a result, the CCPA Regulations promote several different methods, with a requirement that the business pick one in good faith and document the method used (Cal. Code Regs. tit. 11, § 7081(a)). The California AG's comments also highlight the importance of clearly and transparently documenting the calculation process to help the office understand and investigate discrimination claims and improve accountability (CCPA ISOR at 37 to 39).

Establish Consumer Rights Response Program

Consumers may exercise their CCPA personal information rights by submitting to a business:

- Requests to know (see Individual Right to Know).
- Requests to delete (see Deletion Rights).
- Personal information sales opt-out or opt-in requests (see Sale Opt-Out and Opt-In Rights).

The CCPA and CCPA Regulations provide detailed requirements for enabling these rights and responding to consumer rights requests, including submission methods, verification requirements, locating responsive information, acting on the request, and responding to consumers.

Businesses should establish and document clear procedures for honoring these consumer rights within the required timeframes. They must also train their employees on directing consumers to submit rights requests and providing appropriate responses (Cal. Civ. Code §§ 1798.130(a)(6) and 1798.135(a)(3); Cal. Code Regs. tit. 11, § 7100(a).)

For a detailed discussion on receiving and responding to consumer rights requests, see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests.

CPRA Revisions: Establish Consumer Rights Response Program

The CPRA adds to consumer rights request list:

- Requests to correct (see CPRA Revision: New Correction Rights).
- Requests to restrict sensitive personal information use and disclosure (see CPRA Revisions: New Right to Restrict Sensitive Personal Information Processing).
- Personal information sharing opt-out or opt-in requests (see CPRA Revisions: Sharing Opt-Out and Opt-In Rights).

For a detailed discussion on the CPRA's changes to receiving and responding to consumer rights requests, see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests.

Training and Recordkeeping Obligations

The CCPA Regulations include a separate section on general training and recordkeeping obligations for all business that:

- Require all individuals responsible for handing consumer inquiries about the business's privacy practices or CCPA compliance to receive training on the CCPA's requirements and how to direct consumers to exercise their CCPA rights.
- Require maintenance of records documenting how the business responded to consumer rights requests for at least 24 months (CRR Records).
- Permit keeping the CRR Records in a ticket or log format.

(Cal. Code Regs. tit. 11, §§ 7100(a) and 7101(a), (b).)

When maintaining CRR Records, the business must:

- Implement and maintain reasonable security procedures and practices for protecting them.
- Not use information retained for CRR Records purposes for any other purpose, except as reasonably necessary to review and modify its processes for CCPA compliance.
- Not share information maintained for CRR Records purposes with any third party, except as necessary to comply with a legal obligation (see Definitions for Third Party, Restricted Third Party, and Service Provider).

(Cal. Code Regs. tit. 11, § 7101(a), (d).)

A business is also not required to retain personal information just to fulfill a CCPA consumer request, unless it must retain that information to meet its CRR Records obligation (Cal. Code Regs. tit. 11, § 7101(e)).

For a list compiling the general recordkeeping or documentation obligations found in other CCPA Regulation sections, see Box, CCPA Regulations Required Documentation List.

Metrics for Large Businesses

The CCPA Regulations establish new recordkeeping requirements for large businesses to track and publish specific metrics around consumer rights requests (CRR Metrics). This metrics rule applies to a business that knows or should know that it, alone or in combination, buys, sells, or for commercial purposes, receives or shares the personal information of more than 10 million consumers in a calendar year, which represents approximately 25% of California's current population. (Cal. Code Regs. tit. 11, § 7102; CCPA FSOR at 41 and 42.)

Those large businesses must compile, and publish in their privacy policies by July 1 of each calendar year, the following CRR Metrics for the prior calendar year:

- For each request type (requests to know, requests to delete, and requests to opt-out), the number:
  - received;
  - complied with in whole or in part; and
  - denied.
- The median or mean number of days the business took to substantively respond to each request type.

(Cal. Code Regs. tit. 11, § 7102(a).)

Optionally, the large businesses may:

- Break the CRR Metrics on denials down into requests denied in whole or part because they:
  - were not verifiable;
  - were not made by a consumer;
  - called for information exempt from disclosure; or
  - were denied on other grounds.
- Compile and disclose the CRR Metrics on requests received from all individuals instead of just consumers (California residents), provided its disclosure identifies how the metrics were calculated and, if requested, the business can provide consumer-only CRR Metrics to the California AG.

(Cal. Code Regs. tit. 11, § 7102(a)(2)(A), (b).)

Large businesses must also document their employee training policy for handling CCPA consumer request to ensure compliance (Cal. Code Regs. tit. 11, § 7100(b)).

Service Providers and Third Parties

The CCPA establishes additional obligations when working with service providers and third parties. Qualifying as a service provider rather than a third party also provides businesses and their service providers with certain advantages (see Advantages to Service Provider and Restricted Third Party Arrangements).

Definitions for Third Party, Restricted Third Party, and Service Provider

The CCPA identifies three distinct entity types that a covered business may disclose personal information to:

- Third parties.
- Restricted third parties.
- Service providers.

The CCPA defines a third party as any person or entity that is not the covered business. For example, a third party might be a customer, an affiliate, a non-profit organization, or a government organization. The definition of a third party then provides a narrow exclusion for a restricted third party, which is an entity that receives personal information:

- Directly from the covered business.
- For a business purpose (see Business Purposes).
- Under a written contract that contains specific clauses (see Required Contract Provisions).

(Cal. Civ. Code § 1798.140(w).)

Importantly, the definitions for a third party and a restricted third party do not reference or include the term

service provider. Instead, using language similar to the definition for a restricted third party, the CCPA defines a service provider as a for-profit entity (including a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity) that both:

- Processes personal information on behalf of a covered business.
- Receives that information from a covered business:
  - for a business purpose only (see Business Purposes); and
  - under a written contract that contains similar, but different clauses than contracts with restricted third party (see Required Contract Provisions).

(Cal. Civ. Code § 1798.140(v).)

To close some gaps in the CCPA's service provider definitions, the CCPA Regulations clarify that for-profit entities that otherwise qualify as service providers do not lose that designation if they:

- Provide services to non-profits, government entities, or other businesses falling outside of the CCPA's scope.
- Collect or obtain personal information for the covered business from a consumer or other third party instead of directly from the covered business itself.

(Cal. Code Regs. tit. 11, § 7051(a), (b); see also, CCPA FSOR at 30 to 32 and CCPA ISOR at 21.)

CPRA Revisions: Service Provider, Contractor, Third Party Definitions

The CPRA retains these three distinct entity types, but it provides much needed clarifications by deleting the complicated exception that created the restricted third parties and establishing a new entity type – contractors (Cal. Civ. Code § 1798.140(j), (ai) (effective January 1, 2023)).

Under the CPRA, a third party is now any person who is not:

- The business that collects personal information from an intentional interaction with the consumer as part of their current business interaction under the CPRA.
- A service provider to the business, defined as a person that processes a consumer's personal information for a covered business (obtained from the business or on its behalf), for a business purpose under a written contract with specific terms.
- A contractor, defined as a person to whom the business makes available a consumer's personal information for a business purpose under a written contract with specific terms.

(Cal. Civ. Code § 1798.140(j), (ai), (ag) (effective January 1, 2023).)

Service providers no longer have to be for-profit entities or obtain the personal information directly from the business (Cal. Civ. Code § 1798.140(ag) (effective January 1, 2023)).

While the new definitions make it easier to categorize a business's different relationships, some open questions remain, such as:

- How to properly classify a business's parent company, subsidiaries, or other affiliates.
- What the third party definition means for CPRA-covered businesses that passively collect personal information from consumers through unintentional consumer interactions, such as observations.
- What actions might fall inside or outside of the CPRA's business purposes definition and how those business purposes might differ between contractors and service providers.

Future California Privacy Protection Agency regulations may address these issues (Cal. Civ. Code § 1798.185(a)(10) to (12); see CPRA Regulation Tracker).

Service Provider and Restricted Third Party Differences

The primary differences between the CCPA's service provider and the restricted third party definitions are that:

- The restricted third party's contract clause requirements are more detailed (see Required Contract Provisions).
- The service provider must only process the personal information on the business's behalf, while the restricted third party can process the personal information for any purpose that the business notified the consumer about at the time of collection.
- The restricted third party must receive the personal information directly from the covered business.

A single entity can operate as a CCPA service provider in some contexts, but as a CCPA covered business or third party in others. Those entities must fully comply with the CCPA's business obligations when acting in a business capacity. (Cal. Code Regs. tit. 11, § 7051(f); see also, CCPA ISOR at 23.)

CPRA Revisions: Service Provider and Contractor Differences

The CPRA's service provider and contractor definitions are extremely similar. What ultimately distinguishes the two entity types is why the person receives the personal information, namely:

- Service providers process the personal information for another CPRA-covered business.
- Contractors access the personal information for their own business purposes.

(Cal. Civ. Code § 1798.140(j)(1), (ag)(1) (effective January 1, 2023).

The CPRA provides service providers and contractors with essentially the same benefits and obligations, however contractor agreements must contain certain additional provisions (see CPRA Revisions: Required Contract Provisions).

Required Contract Provisions

To qualify as a **service provider** under the CCPA, the business's written contract with the entity must prohibit it from retaining, using, or disclosing the personal information for:

- Any purpose except performing the services specified in the contract or that the CCPA otherwise permits a service provider to take.
- A commercial purpose other than providing the services specified in the contract.

(Cal. Civ. Code § 1798.140(v).)

For more on service provider use restrictions, see Service Provider Use Restrictions. For model contract clauses, see Standard Clause, CCPA Contract Clauses for Service Providers.

Written contacts with **restricted third parties** must:

- Prohibit retaining, using, or disclosing the personal information for any purpose except performing the services specified in the contract, including prohibiting use for a different commercial purpose (similar to service providers).
- Prohibit the recipient from:
  - selling the personal information; and
  - retaining, using, or disclosing the information outside of the direct business relationship between the recipient and the business.
- Include a certification that the recipient understands the restrictions and intends to comply with them.

(Cal. Civ. Code § 1798.140(w).)

Entities receiving personal information without using a compliant contract cannot qualify as either service providers or restricted third parties. Those transfers likely constitute a third-party sale under the CCPA, which subjects the business and third party to additional obligations (see Distinguishing Between Sales and Business Purposes Disclosures). For example, non-restricted third parties must give consumers explicit notice and an opportunity to opt out before re-selling personal information that it acquired from another business (Cal Civ. Code § 1798.115(d); see Sale Opt-Out and Opt-In Rights and Notice at Collection). However, entities that qualify as service providers or restricted third parties under the CCPA receive specific benefits from those designations (see Advantages to Service Provider and Restricted Third Party Arrangements).

Although not explicitly required by the CCPA for service provider contracts, businesses should also consider including contractual provisions that:

- Comply with the contract requirements for a restricted third party, such as representing that the service provider is aware of and intends to abide by the CCPA's terms and any related regulations.
- Require the service provider to help the business meet its own CCPA obligations, including:
  - fulfilling any valid deletion requests; and
  - assisting with valid consumer rights requests, including providing a copy of the personal information it retains in a portable and readily usable format on request (see Practice Note, Responding to CCPA Consumer Rights Requests).

Sales or Licenses of Deidentified Patient Information

Any contract for the sale or license of deidentified patient information where one of the parties resides or does business in California must include the following provisions:

- A statement that the deidentified information sold or licensed includes deidentified patient information.
- A statement the CCPA prohibits purchasers or licensees of deidentified patient information from reidentifying or attempting to reidentify it.

- A requirement prohibiting the purchaser or licensee from further disclosing the deidentified patient information to any third party not contractually bound by the same or stricter restrictions and conditions, unless otherwise required by law.

(Cal. Civ. Code § 1798.148(b).)

For more on deidentified patient information, see Deidentified Patient Information.

CPRA Revisions: Required Contract Provisions

The CPRA creates a new obligation requiring a business that collects a consumer's personal information to execute written contracts containing specific provisions whenever it:

- Discloses that personal information to a service provider or contractor for a business purpose.
- Sells or shares that personal information with a third party.

(Cal. Civ. Code § 1798.100(d) (effective January 1, 2023).)

Those contracts must:

- Specify that the business sells or discloses the personal information only for limited and specified purposes.
- Obligate the third party, service provider, or contractor:
  - to comply with applicable CPRA obligations; and
  - provide the same level of privacy protection as the CPRA requires.
- Require the third party, service provider, or contractor to notify the business if it determines that it can no longer meet its obligations under the CPRA.
- Grant the business the rights:
  - to take reasonable and appropriate steps to help insure that the third party, service provider, or contractor uses the transferred personal information in a manner consistent with the business's CPRA obligations; and
  - upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

(Cal. Civ. Code § 1798.100(d)(1) to (5) (effective January 1, 2023).)

Service providers and contractor agreements must also prohibit the person from:

- Selling or sharing the personal information.
- Retaining, using, or disclosing the personal information for any purpose other than what the contract specifies as the business purposes, including for a commercial or business purpose not specified in the contract, or as the CPRA otherwise permits.
- Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.
- Unless used for a business purpose that does not involve cross-context behavioral advertising and is permitted under eventual CPRA regulations, combining the personal information the person receives from, or on behalf of, the business with personal information that:
  - it receives from, or on behalf of, another person or persons; or
  - it collects from its own consumer interaction.

(Cal. Civ. Code § 1798.140(j)(1)(A), (ag)(1)(A) to (D) (effective January 1, 2023).)

Contractor agreements must and service provider agreements may permit the business to monitor the person's contract compliance through administrative measures (subject to person's agreement), including but not limited to, ongoing manual reviews, automated scans, and regular assessments, audits, or other technical and operational testing at least once every 12 months (Cal. Civ. Code § 1798.140(j)(2), (ag)(1)(D) (effective January 1, 2023)).

Finally, contractor agreements must contain a certification that the contractor understands the CPRA's contractually required restrictions and will comply with them (Cal. Civ. Code § 1798.140(j)(1)(B) (effective January 1, 2023)).

Advantages to Service Provider and Restricted Third Party Arrangements

Instead of directly imposing data protection requirements on third parties receiving personal information from a business, the CCPA incentivizes the business to voluntarily enter into contracts that restrict personal information use by providing liability and sales definition exclusions.

When the entity receiving personal information from the business qualifies as a:

- **Service provider**:
  - the parties can treat shared personal information as a business purpose disclosure instead of a sale (see Distinguishing Between Sales and Business Purposes Disclosures and Service Provider Exception);
  - the service provider is not liable for the business's CCPA obligations; and

  - the business is not liable for the service provider's personal information use that violates the CCPA if, at the time of disclosure, it did not have actual knowledge or reason to believe that the service provider intended to violate the CCPA.
  - (Cal. Civ. Code § 1798.145(j).)
- **Restricted third party**:
  - the restricted third party is liable for its own CCPA violations; and
  - the business is not liable for the restricted third party's personal information use that violates the CCPA if, at the time of disclosure, it did not have actual knowledge or reason to believe that the restricted third party intended to violate the CCPA.
  - (Cal. Civ. Code § 1798.140(w)(2)(B)).

Despite the CCPA's more favorable treatment of service providers, both third parties and service providers must also adhere to the CCPA's general requirements. For example, a business must direct service providers to delete a consumer's personal information after receiving and verifying a consumer's request (Cal Civ. Code § 1798.105(c); see Deletion Rights). The CCPA also establishes direct liability for restricted third parties that violate the CCPA's restrictions (Cal. Civ. Code § 1798.140(w)(2)(B)).

CPRA Revisions: Advantages to Service Provider and Contractor Arrangements

The CPRA shifts to imposing direct obligations on businesses that disclose personal information to a service provider or contractor. Businesses can only disclose that information under a written contract that obligates the recipient to provide the same level of privacy protection as the CPRA and comply with any applicable CPRA obligations (Cal. Civ. Code § 1798.100(d) (effective January 1, 2023)). It also imposes direct obligations on the service provider or contractor receiving the personal information, such as to:

- Notify the business of any sub-processor or sub-contractor arrangements and require the sub-processor or sub-contractor to execute a written contract containing the same terms the CPRA requires of service providers or contractors (Cal. Civ. Code § 1798.140(j)(2), (ag)(2) (effective January 1, 2023)).
- Cooperate with the business in responding to verifiable consumer requests by, for example:
  - providing responsive personal information in its possession obtained during the relationship to the business;
  - deleting or allowing the business to delete the personal information and notifying downstream entities about the deletion request; and
  - correcting or enabling the business to correct inaccurate information.

  (Cal. Civ. Code §§ 1798.105(c)(3) and 1798.130(a)(3)(A) (effective January 1, 2023)).
- Limit sensitive personal information use upon the business's instruction (Cal. Civ. Code § 1798.121 (a), (c) (effective January 1, 2023)).

Importantly, consumers cannot require service providers and contractors to directly respond to a verifiable request to exercise their CPRA rights (Cal. Civ. Code §§ 1798.105(c)(3) and 1798.130(a)(3)(A) (effective January 1, 2023)). Such requests must go to the responsible business. For more on service provider or contractor obligations when consumers exercise their personal data rights, see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests: CPRA Revisions: Service Provider and Contractor Responsibility for Consumer Requests.

Like the CCPA, the CPRA also provides liability limitation protections for businesses, service providers, and contractors. A business is not liable for a service provider's or contractor's CPRA violations if:

- The personal information disclosure complied with all CPRA requirements.
- The business did not have actual knowledge or reason to believe that the service provider or contractor intended to violate the CPRA when it disclosed the personal information.

(Cal. Civ. Code § 1798.145(i)(1) (effective January 1, 2023).)

Similarly, a service provider or contractor is not liable for the business's CPRA obligations. It is only liable for its own CPRA violations. (Cal. Civ. Code § 1798.145(i)(1) (effective January 1, 2023).)

Qualifying for the Service Provider Sales Exception

To qualify for the CCPA's personal information sales service provider exception, a business must meet all of the following conditions:

- Sharing or using the personal information with the service provider is necessary to perform a business purpose, as defined by the CCPA (see Business Purposes).
- The business disclosed that it uses or shares personal information with a service provider in required CCPA

notices (see Service Provider Exception and Opt-Out Right Notice).

- The service provider does not further collect, sell, or use the consumers' personal information, except as necessary to perform the business purpose (see Service Provider Use Restrictions).
- The parties executed a written contract containing the required clauses (see Required Contract Provisions).

(Cal. Civ. Code § 1798.140(t)(2)(C); see Personal Information Sales and Definitions for Third Party, Restricted Third Party, and Service Provider).

However, giving service providers access to personal information does qualify as a disclosure for a business purpose (see Business Purposes). The business should include these service provider disclosures when making required public or individual notices (see Box, Privacy Policy Required Elements List and Individual Right to Know).

CPRA Revisions: Qualifying for the Service Provider Sales Exception

The CPRA changes and streamlines the service provider framework. Sales only occur when the recipient is a third party, which by definition directly excludes service providers (Cal. Civ. Code § 1798.140(ad), (ai)(2) (effective January 1, 2023); see CPRA Revisions: Service Provider Exception and CPRA Revisions: Service Provider, Contractor, Third Party Definitions).

Service Provider Use Restrictions

The CCPA Regulations prohibit service providers from retaining, using, or disclosing personal information it obtains from a covered business customer except:

- To process or maintain personal information for the business that either provided it or directed its collection, in compliance with the written services contract required by the CCPA.
- To retain and employ subcontractors also meeting the CCPA's service provider requirements.
- For internal use to build or improve the quality of its services, but only if the use:
  - does not include building or modifying household or consumer profiles used to provide services to another business; or
  - correcting or augmenting data from another source.
- To detect data security incidents or protect against fraudulent or illegal activity.
- For the purposes permitted in the CCPA's legal claims preemption section, which includes:
  - compliance with federal, state, or local laws;
  - compliance with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities;
  - cooperation 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; or
  - the exercise or defend legal claims (Cal. Civ. Code § 1798.145(a)(1) to (4)).

(Cal. Code Regs. tit. 11, § 7051(c); CCPA FSOR at 32 to 35.)

The CCPA Regulations also prohibit a service provider from selling a consumer's personal information after that individual opts out of its customer's personal information sales (Cal. Code Regs. tit. 11, § 7051(d); CCPA FSOR at 35).

CPRA Revisions: Service Provider Use Restrictions

CPRA-compliant contracts must restrict the service provider's use of any personal information it obtains to the contractually specified business purposes. It must also restrict combining personal information obtained through the contract with personal information obtained elsewhere to specific business purposes that future regulations will define. (Cal. Civ. Code § 1798.100(d) (effective January 1, 2023).)

The CPRA directs the California Privacy Protection Agency to develop regulations that further define when and how a service provider or contractor may use or combine personal information (Cal. Civ. Code § 1798.185(10), (11); see CPRA Revisions: Business Purposes and CPRA Regulation Tracker).

Rulemaking

The CCPA directly authorizes (and in some cases, directs) the California AG to adopt implementing regulations to further its purposes as needed. It instructs the California AG to solicit broad input and issue regulations that, for example:

- Clarify the exact information businesses must include in their notices to consumers.
- Define what is a "California-specific description of consumers' privacy rights."
- Prescribe a standardized "Do Not Sell My Personal Information" logo or button.

- Set out other processes regarding how businesses must respond to consumer deletion, access, and opt-out requests.
- Add categories of personal information and unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns.
- Establish rules and procedures on how to process and comply with verifiable consumer requests for specific pieces of personal information.

(Cal. Civ. Code § 1798.185.)

The CCPA also currently allows businesses to seek the California AG's opinion or advice on any statutory compliance questions (Cal. Civ. Code § 1798.155(a)).

Because the statute applies broadly across industries, it is important for businesses across industries to participate in the rulemaking process. To keep up to date on the California AG's rulemaking process, see OAG: Subscribe to the California Consumer Privacy Act (CCPA) Mailing List.

CPRA Revisions: Rulemaking and the California Privacy Protection Agency

The new California Privacy Protection Agency is charged with implementing and enforcing the CPRA (Cal. Civ. Code § 1798.199.10(a)). The Agency's responsibilities include to:

- Protect the fundamental privacy rights of natural persons with respect to the use of their personal information through implementation of the CPRA.
- Enforce and implement the CPRA through bringing administrative actions and conducting business audits (see CPRA Revisions: Enforcement).
- Develop and maintain CCPA and CPRA regulations, taking over this responsibility from the California AG.
- Monitor relevant developments relating to personal information protection, information and communication technology advances, and commercial practices.
- Provide guidance to consumers and businesses regarding their CPRA rights and obligations and promote public awareness and understanding of personal information processing risks, rules, responsibilities, safeguards, and rights.
- Advise the California Legislature, upon request, on privacy-related legislation.
- Cooperate with privacy or data protection agencies in other jurisdictions to ensure consistent application of privacy protections.

(Cal. Civ. Code § 1798.199.40.)

Like the CCPA, the CPRA contains a long list of topics for which the Agency should develop regulations. New regulation topic areas include:

- Harmonizing the CPRA's requirements on consumer notices, opt-out mechanisms, and other operational requirement to promote clarity.
- How businesses must respond to the CPRA's new consumer rights around correction, sharing personal information, and sensitive personal information limitations.
- Standards for if and when a business can limit request to know responses to just the past 12 months.
- Opt-out preference signals.
- How to best implement the consumer's data portability right to maximize the consumer's access while minimizing the delivery of information that may not be useful, such as log or technical data, and protecting the most sensitive personal information.
- Further defining what constitutes a business purpose, including when service providers and contractors:
  - may combine personal information obtained from different sources; or
  - use personal information received from a business under contract for their own purposes.
- Precise geolocation use.
- High-risk processing that may require cybersecurity audits, and regular risk assessment reporting.
- Automated decision-making technology, including profiling, and requiring access requests to include meaningful information about the logic involved in those processes and the likely outcome of the processes for the consumer.
- The Agency's audit authority and processes.

(Cal. Civ. Code § 1798.185(a)(1) to (22).)

The CPRA directs the Agency to adopt final CPRA regulations by July 1, 2022 (Cal. Civ. Code § 1798.185(d)). To learn more about the Agency's rulemaking process, including its progress on proposing and finalizing CPRA regulations, see CPRA Regulation Tracker.

Enforcement

California Attorney General Enforcement Actions

The CCPA grants regulatory and enforcement authority to the California AG. Before initiating an action for a CCPA violation, the California AG must give the offending business, service provider, or other person notice of the alleged violation and at least 30 days to cure it. If the business does not (or cannot) cure the violations, the California AG may seek civil penalties up to either:

- $2,500 per violation.
- $7,500 per intentional violation.

(Cal. Civ. Code § 1798.155(b).)

While unclear, these civil penalties likely extend to each affected individual and may result in large aggregate fines. The California AG must deposit all civil fine proceeds in a new Consumer Privacy Fund to offset the state courts' and California AG's enforcement costs (Cal. Civ. Code §§ 1798.155(c) and 1798.160).

The California AG provides consumers with an interactive tool to use when they encounter potential CCPA violations (see OAG: Consumer Privacy Interactive Tool). The interactive tool guides consumers through a series of questions designed to help them evaluate and understand the potential CCPA violation and returns a draft notice of noncompliance based on the responses that the consumer can send to businesses and the California AG's office.

In its first formal enforcement action, the California AG announced that Sephora USA, Inc. paid a $1.2 million fine and agreed to several practice changes to settle allegations that the company violated the CCPA by failing to disclose that it sold consumers' personal information and failing to process consumers' personal information sales opt-out requests made through user-enabled global privacy control (GPC) signals (see OAG: Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act). For more on the specific case allegations and settlement terms, see Legal Update, California AG Announces $1.2 Million Settlement with Sephora for CCPA Personal Information Sales Violations.

Enforcement Case Examples and Investigation Sweeps

The California AG has resolved many of its CCPA violation investigations informally during the law's 30-day notice and cure period. The California AG does not typically release information to the public about pending or concluded investigations that do not result in formal charges. To help businesses better understand the California AG office's enforcement priorities, the types of violations encountered, and the types of changes that businesses made to resolve the allegations, the California AG has periodically released summaries of the resolved enforcement actions that do not disclose the parties involved.

Priorities highlighted by the first set of enforcement case examples include violations relating to:

- Incomplete, inadequate, or missing privacy notices, sale disclosures, or financial incentive notices.
- Failure to provide a separate notice at collection.
- Failure to provide a "Do Not Sell My Personal Information" website link or to provide clear, effective, or operational opt-out submission methods.
- Failure to obtain opt-in consent before selling the personal information of minors under 16 years old.
- Service provider contracts that did not include the CCPA's required contract terms, such as prohibiting personal information use, retention, or disclosure for any purpose other than performing the specified services.
- Untimely responses to consumer requests.

(See OAG: Press Release: First Year CCPA Enforcement Update and OAG: CCPA Enforcement Case Examples Updated 07/19/2021).

Priorities highlighted by the second set of enforcement case examples include violations relating to:

- Failing to honor user-enabled GPC signals to opt a consumer out of personal information sales.
- Insufficient financial incentive notices and consumer consent processes for customer loyalty program participation.
- Improperly placing conditions on a consumer's exercise of their CCPA right or requiring additional steps to opt-out of personal information sales, for example, by directing consumers to a third-party trade association's tool designed to manage online advertising.
- Providing confusing or incomplete information at the business's "Do Not Sell My Personal Information" webpage.

(See OAG: CCPA Enforcement Case Examples Updated 08/24/2022).

The California AG announced a 2022 investigation sweep focused on customer loyalty program compliance. It warned major corporations in the retail, home improvement, travel, and food service industries that their customer loyalty programs did not comply with the CCPA's financial incentive requirements and gave them 30-days to bring those practices into compliance (see OAG: On Data Privacy Day, Attorney General Bonta Puts Businesses Operating Loyalty Programs on Notice for Violations of California Consumer Privacy Act). For more on offering financial incentives, see Establish Financial Incentive and Anti-Discrimination Programs.

The California AG also announced a similar investigation sweep focused on the failure to process consumer opt-out requests made via user-enabled GPC signals (see OAG: Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act).

CPRA Revisions: Enforcement

The California AG remains empowered to investigate CPRA violations and seek the same civil penalties and injunctions (Cal. Civ. Code § 1798.199.90(a)). However, the CPRA also empowers the newly created California Privacy Protection Agency to enforce the statute and any enacted regulations through administrative proceedings that may result in a cease and desist order along with the same potential administrative fines (Cal. Civ. Code §§ 1798.155(a), 1798.199.45, and 1798.199.55).

To mitigate potential jurisdictional conflicts, the CPRA prevents a business from paying both an administrative fine and a civil penalty for the same violation. The California AG cannot bring a civil action against the same business for the same violation after the Agency has issued:

- A decision with respect to a complaint or administrative fine; or
- An order based on a CPRA violation.

(Cal. Civ. Code § 1798.199.90(d).)

However, the California AG may instruct the Agency to stay an administrative action or investigation while its own investigation remains active, and the Agency cannot limit the California AG's enforcement authority (Cal. Civ. Code § 1798.199.90(c)).

The CPRA also:

- Removes the 30-day cure period from the Attorney General's enforcement process but imposes a 30-day cure period for Agency probable cause findings.
- Broadens the circumstances in which the highest fine of $7,500 per violation applies. For example, violations involving minors under 16 years of age now trigger the higher $7,500 per violation penalty.

((Cal. Civ. Code §§ 1798.155(a), 1798.199.50, and 1798.199.55(a)(2).)

Private Right of Action for Data Breaches

The CCPA extends the current landscape for data breach liability under California law. It permits a private right of action for unauthorized access, theft, or disclosure of nonencrypted and nonredacted personal information (as defined within that section) due to the business failing to implement reasonable security practices and procedures appropriate for the particular type of personal information ((Cal. Civ. Code § 1798.150(a)(1)); see Implement Reasonable Security Practices and Procedures).

Importantly, the data breach liability section defines personal information much more narrowly than the general CCPA definition. The section adopts the personal information definition found in just the first part of the California Data Protection Act (CDPA), citing to California Civil Code Section 1798.81.5(d)(1)(A).

Specifically, it limits personal information to an individual's first name (or first initial) and last name in combination with one of the following:

- SSN or other tax identification number.
- Driver's license number, California ID number, passport number, or military identification number.
- Any other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
- Account number, credit or debit card number, in combination with the security code, password, or other information required to access the account.
- Medical information.
- Health insurance information.
- Unique biometric data generated from measurements or technical analysis of human body characteristics used to authenticate a specific individual, such as:
  - a fingerprint;
  - a retina or iris image; and
  - a physical or digital photograph, but only when used or stored for facial recognition purposes.
- Genetic data.

(Cal. Civ. Code § 1798.81.5(d)(1)(A).)

Interestingly, the section does not include the second part of the CDPA's personal information definition, which covers a username or email address in combination with a password or security question and answer that permits access to an online account (Cal. Civ. Code § 1798.81.5(d)(1)(B)).

The narrow subset of personal information covered in the private right of action may lead to situations where an entity must provide notice of a data breach, but does not face a private right of action, or vice versa.

The potential damages a consumer may seek in a CCPA private action include:

- Either statutory damages between $100 to $750 per California resident and per incident, or actual damages, whichever is greater.
- Injunctive or declaratory relief.
- Any other relief a court deems proper.

(Cal. Civ. Code § 1798.150(a)(A) to (C).)

However, statutory damages are only available if, before filing a data breach lawsuit:

- The consumer provides the business with a written notice identifying the specific CCPA violations and a 30-day period to cure those violations, if possible.
- The business does not (or cannot) cure the alleged violation and does not provide the consumer with an express written statement within the 30-day period that:
  - it has cured the violation; and
  - no further violations will occur.

If the business continues with its alleged violations, the consumer can file a lawsuit requesting statutory damages for the original violation, and any new CCPA violation occurring after the notice, including breaching the written statement. (Cal. Civ. Code § 1798.150(b).)

The CCPA also explicitly prohibits any agreement or contract provision that seeks to waive or limit a consumer's rights under the CCPA (see Prohibition on Waiver of Applicability) (Cal Civ. Code § 1798.192).

CPRA Revisions: Private Right of Action for Data Breaches

The CPRA makes two substantive changes to this section. It:

- Expands the personal information definition to include an email address in combination with a password or security question and answer that permits access to an online account.
- Clarifies that implementing and maintaining reasonable security procedures and practices after a breach does not constitute a cure for that breach.

(Cal. Civ. Code § 1798.150(a)(1), (b) (effective January 1, 2023).)

The CPRA's revised personal information definition still leaves a major gap because, unlike the CDPA, it does not cover the loss of a consumer's username plus password or other online account access information, whenever the username is not the consumer's email address.

The CPRA also expanded the non-waiver section to specifically state that representative action waivers are also invalid (Cal Civ. Code § 1798.192 (effective January 1, 2023)).

History of the CCPA and CPRA

The CCPA began as a controversial privacy ballot initiative designed to significantly expand Californian's consumer privacy rights through a state constitutional amendment (see OAG: The Consumer Right to Privacy Act of 2018). To avoid that ballot initiative and the requirement to make any future amendments or changes through another ballot initiative, the California legislature negotiated with the initiative's sponsor, Alastair Mactaggart, to enact a compromise bill providing new consumer privacy protections instead. The resulting compromise bill specifically conditioned the CCPA's operative effect on the 2018 ballot initiative's withdrawal (Cal. Civ. Code § 1798.198(b)).

Under a hard deadline to enact the bill in time to withdraw the initiative from the November 2018 ballot, the legislature quickly revised a previously dead California Assembly Bill dealing with data privacy and drafted the compromise statute (AB 375 (2017-2018)). The CCPA's resulting statutory text is a combination of the initial ballot initiative and the original AB 375 bill's text. It often reads more like a ballot initiative than a statute, with descriptive text and general ideals at the outset, and more specific provisions enacting those general ideals occurring later. The quick action also led to sometimes contradictory and confusing terms.

Despite its drawbacks, the legislature unanimously passed the CCPA on June 28, 2018 (the deadline for withdrawing California ballot initiatives) and Governor Brown signed the bill that same day.

CCPA Amendments and Regulations

2018 to 2020 Amendments

The legislature revisited the CCPA just two months later to address drafting errors and make minor amendments and clarifications with Senate Bill 1121 (2017-2018) (2018 CCPA Amendments), which Governor Brown signed into law on September 23, 2018. For more on the 2018 CCPA Amendments, see Legal Update, California Amends the Consumer Privacy Act of 2018.

Debate about the CCPA's scope and requirements continued in the 2019 legislative session. By the session's end in October 2019, Governor Newsom signed six bills into law that amended or altered the CCPA's scope (2019 CCPA Amendments), including temporary one-year exemptions from most CCPA provisions for workforce-related personal information and personal information reflected in certain business-to-business (B2B) communications (see Practice Note, CCPA Proposed Amendments and Other California Privacy-Related Legislation Tracker: Enacted CCPA Amendments). For more on the 2019 CCPA Amendments, see Legal Update, California Governor Signs CCPA and Data Breach Law Amendments.

Of the many different CCPA-related amendments under consideration in the 2020 legislative session, only three bills were signed into law in late September 2020: AB 713, AB 1281, and SB 1371 (2019-2020)) (2020 CCPA Amendments) (see Legal Updates, California Governor Signs CCPA Amendments on Information Use for Research and Public Health Purposes and California Extends Temporary Workforce and Business-to-Business CCPA Exemptions).

2020 CCPA Regulations

After a lengthy development process, CCPA Regulations promulgated by the California Attorney General's office (California AG) became effective on August 14, 2020 (Cal. Code Regs. tit. 11, §§ 7000 to 7081). The Office of Administrative Law approved amendments to the CCPA Regulations on March 15, 2021 (see Legal Update, California OAL Approves Additional CCPA Regulations). For more on the development process see Box, CCPA Regulations Development Timeline.

2020 CPRA Ballot Initiative

In response to legislative efforts to dilute the CCPA, Alastair Mactaggart and his Californians for Consumer Privacy advocacy group filed a November 2020 ballot initiative for a voter-enacted statute to amend and expand the CCPA, the California Privacy Rights Act of 2020 (CPRA).

California voters approved the CPRA on November 3, 2020. Most of the CPRA's substantive CCPA amendments do not take effect until January 1, 2023, so businesses should continue to follow the CCPA and CCPA Regulations while they prepare for the CPRA's new requirements. However, except for access requests, the CPRA's new obligations will apply to any personal information the business collects on or after January 1, 2022.

Among other changes, the CPRA expands the CCPA's personal information protection rights and business obligations, particularly around sensitive information like precise geolocation data, provides transparency around automated decision making, and creates a dedicated state agency to protection consumer privacy called the California Privacy Protection Agency. It also contains a one-way rachet amendment process that allows legislature-initiated amendments that improve consumer privacy but requires a new ballot initiative to reduce privacy protections.

The CPRA also extends the CCPA's partial exemptions relating to workforce and employment-related personal information and business-to-business communications through January 1, 2023 (see Temporary Exemptions).

For an overview of the CPRA and its new requirements, see Article, Expert Q&A: The California Privacy Rights Act of 2020 (CPRA).

Amendments Enacted After CPRA Passage

In October 2021, Governor Gavin Newsom signed three more bills that directly or indirectly amended the CCPA and CPRA: (AB 335, AB 694, and AB 825 (2021-2022) (2021 CCPA Amendments). For more on these amendments, which go into effect on January 1, 2021, see Legal Update, California Enacts Genetic Information Privacy Law, CPRA and CMIA Amendments, and Other Privacy-Related Bills.

Privacy Policy Required Elements List

The business's CCPA privacy policy must include the following information:

- Right to know disclosures, including:
  - an explanation of the consumer's right to request that a business disclose what personal information it collects, uses, discloses, and sells about that consumer (see Individual Right to Know);
  - instructions for submitting a verifiable consumer request to know and links to any online request form or portal provided to make those requests (see Practice Note, Responding to CCPA Consumer Rights Requests: Verifying Consumer Identities);
  - a general description of the business's process for verifying consumer requests, including any information the consumer must provide (see Practice Note, Responding to CCPA Consumer Rights Requests: Verifying Consumer Identities);
  - the personal information categories collected about consumers in the preceding 12 months (see Personal Information Categories);
  - the categories of sources from which the business collected personal information; and
  - the business or commercial purpose for collecting or selling personal information (see Business Purposes and Commercial Purposes).
- A statement on personal information disclosures for a business purpose that either:
  - lists the personal information categories disclosed for a business purpose in the preceding 12 months and the categories of third parties receiving that information; or
  - states that no personal information disclosures occurred.

  (See Business Purposes.)
- A statement on personal information sales that either:
  - lists the personal information categories sold by business in the preceding 12 months and the categories of third parties purchasing that information; or
  - states that no personal information sales occurred.

  (See Personal Information Sales.)
- A statement disclosing whether the business has actual knowledge that it sells personal information about consumers under age 16 and if it does, a description of the process for:
  - opting into personal information sales; and
  - submitting verified consumer requests to know and delete for minors.

(See Practice Note, Responding to CCPA Consumer Rights Requests: Responding to Sales Opt-Out and Opt-In Requests.)

- Right to deletion disclosures, including:
  - an explanation of the consumer's right to request deletion of their personal information collected by the business (See Deletion Rights);
  - instructions for submitting a verifiable consumer request to delete and links to any online request form or portal provided to make those requests (see Practice Note, Responding to CCPA Consumer Rights Requests: Verifying Consumer Identities); and
  - a general description of the business's process for verifying consumer requests, including any information the consumer must provide (see Practice Note, Responding to CCPA Consumer Rights Requests: Verifying Consumer Identities).
- Right to opt-out disclosures, including:
  - an explanation of the consumer's right to opt-out from the business's sale of their personal information (see Sale Opt-Out and Opt-In Rights);
  - a statement disclosing whether the business sells personal information; and
  - if the business sells personal information, the contents of or a link to its opt-out right notice (see Opt-Out Right Notice).
- Right to non-discrimination disclosure, that explains the consumer's right not to receive discriminatory treatment by the business for exercising their CCPA consumer rights (see Freedom from Discrimination).
- Authorized agent disclosure, describing how agents can make CCPA-related requests on the consumer's behalf (see Practice Note, Responding to CCPA Consumer Rights Requests: Verifying Requests from Authorized Agents).
- Contact information consumers can use to submit questions or concerns about the business's privacy practices, using a method that reflects how the business primarily interacts with consumers.
- For large businesses meeting the disclosure thresholds, statistical metrics on the business's response to consumer rights requests (see Metrics for Large Businesses).
- For businesses that sell or disclose deidentified patient information exempt from the CCPA (see Preemption and Deidentified Patient Information), a statement disclosing whether:
  - it sells or discloses deidentified patient information; and
  - if it used one or more of HIPAA's deidentification methodologies, specifically the HIPAA expert determination method (45 C.F.R. § 164.514(b)(1)) or the HIPAA safe harbor method (45 C.F.R. § 164.514(b)(2)).
- Date it was last updated or reviewed.

(Cal. Civ. Code §§ 1798.105, 1798.115, 1798.120, and 1798.130; Cal. Code Regs. tit. 11, § 7011(c).)

The business must use personal information categories, source categories, third party categories and purpose descriptions that provide consumers a with meaningful understanding those items (Cal. Code Regs. tit. 11, §§ 7001(d), (e) and 7011(c)(1)(D), (F)). The CCPA further requires that personal information category disclosures follow the personal information's definition category that most closely describe the personal information collected (Cal. Civ. Code § 1798.130(a)(5), (c); see Personal Information Categories).

For more on preparing and presenting privacy policies, including providing meaningful category and purpose descriptions, see Practice Note, Drafting CCPA Notices and Privacy Policies.

CPRA Revisions: Privacy Policy Required Elements List

Businesses will not know the exact privacy policy content and format expectations until the California Privacy Protection Agency issues new or updated regulations (see CPRA Regulation Tracker). However, the CPRA's changes to the current privacy policy and collection notice content requirements include:

- Expanding personal information disclosure requirements to include similar disclosures on sensitive personal information.
- Describing the new consumer right to correction and how to make a correction request.
- Expanding sales disclosure requirements to include similar disclosures on sharing personal information for cross-context behavioral advertising purposes.
- Confirming the requirement to provide two or more designated methods for submitting consumer rights requests, except for businesses operating exclusively online with direct consumer relationships that only need to provide an email address.
- The intended retention period for each personal information and sensitive personal information category. If providing a specific time period is not, the criteria used to determine the retention period.

(Cal. Civ. Code §§ 1798.100(a) and 1798.130(a)(5) (effective January 1, 2023).)

The CPRA potentially overwrites the deidentified patient information disclosure requirement that AB 713 (2019-2020) added to the CCPA on September 25, 2020 because the corresponding CPRA section approved by the voters did not contain that new language (Cal. Civ. Code § 1798.130(a)(5)(D); Cal. Civ. Code § 1798.130(a)(5) (effective January 1, 2023)). Although the CPRA's provisions prevail over any conflicting legislation enacted after January 1, 2020, legislation does not conflict if it is consistent with CPRA and furthers its purposes (Section 25(d), CA Prop. 24 (2020)).

CCPA Regulations Required Documentation List

A business must keep records documenting how it responded to consumer rights requests for at least 24 months (CRR Records) (Cal. Code Regs. tit. 11, § 7101(a)). It may keep CRR Records in a ticket or log format that tracks the:

- Request date.
- Nature of the request.
- How the consumer made the request.
- When the business responded.
- How the business responded.
- The basis for any denials in whole or in part, if applicable.

(Cal. Code Regs. tit. 11, § 7101(b).)

General recordkeeping or documentation obligations for all businesses found in other CCPA Regulation sections include:

- Documenting the business's method for verifying a consumer's identity or its justification for not having a reasonable verification method (Cal. Code Regs. tit. 11, §§ 7060(a) and 7062(g)).

- For businesses that required a signed declaration under penalty of perjury from the requestor as part of their verification process, retaining the signed declaration as part of the CRR Record (Cal. Code Regs. tit. 11, § 7062(c)).
- Documenting the business's method for verifying that a person submitting a consumer rights request for a child under age 13 is that child's parent or guardian (Cal. Code Regs. tit. 11, §§ 7070(c)).
- For businesses with actual knowledge it sells personal information from children under age 13, documenting the method used to confirm the person authorizing personal information sales is actually the child's legal parent or guardian (Cal. Code Regs. tit. 11, § 7070(a)(1); see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests: Obtaining Opt-In Consent for Minors).
- For businesses with actual knowledge it sells personal information from children at least 13 but under 16 years of age, documenting the reasonable process used to allow those minors to opt-in to personal information sales (Cal. Code Regs. tit. 11, § 7071(a); see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests: Obtaining Opt-In Consent for Minors).
- Documenting the business's reasonable and good faith method for calculating the value of the consumer's data (Cal. Code Regs. tit. 11, § 7081(a); see Calculating Consumer Data Value).
- For businesses that do not operate a website or that collect personal information through offline methods, documenting the method by which it informs consumers of their right to direct a business that sells their personal information to stop these sales (Cal. Code Regs. tit. 11, § 7013(b)(2), (3); see Opt-Out Right Notice).
- Large businesses must track specific CRR Metrics and must document their employee training policy for handling CCPA consumer requests (Cal. Code Regs. tit. 11, § 7100(b) and 7102; see Metrics for Large Businesses).

CCPA Provision and Regulation Index

Topic to Section

Topic	Sections
Authorized Agents	Cal. Civ. Code § 1798.185(a)(7); Cal. Code Regs. tit. 11, § 7063
Calculating the Value of Consumer Data	Cal. Code Regs. tit. 11, § 7081
Civil Penalties	Cal. Civ. Code § 1798.155(a)
Consumer Privacy Fund	Cal. Civ. Code §§ 1798.155(c) and 1798.160
Data Portability	Cal. Civ. Code § 1798.100(d)
Definitions	Cal. Civ. Code § 1798.140
Disclosure of Deletion Rights	Cal. Civ. Code § 1798.105(b)
Exceptions to Deletion Requirement	Cal. Civ. Code § 1798.105(d)
Exclusions and Exceptions to CCPA Compliance	Cal. Civ. Code §§ 1798.145, 1798.146

Topic	Sections
Financial Incentives for Consumers	Cal. Civ. Code § 1798.125(b)
Household Information Requests to Know or Delete	Cal. Code Regs. tit. 11, § 7031
Methods for Submitting Requests to Know and Delete	Cal. Civ. Code § 1798.130(a)(1); Cal. Code Regs. tit. 11, § 7020
Non-Discrimination	Cal. Civ. Code § 1798.125(a); Cal. Code Regs. tit. 11, § 7080
Notice of Right to Opt-Out	Cal. Civ. Code § 1798.135(a)(1), (2); Cal. Code Regs. tit. 11, § 7013
Notice of Financial Incentive	Civ. Code § 1798.125(b)(2), (3); Cal. Code Regs. tit. 11, § 7016
Public Notice Requirements	Cal. Civ. Code §§ 1798.100(b), 1798.105(b), 1798.110(c), 1798.115(c), 1798.120(b), 1798.130(a)(5), and 1798.135(a)(1), (2); Cal. Code Regs. tit. 11, §§ 7010 to 7011
Overview of Required Notices	Cal. Code Regs. tit. 11, § 7010
One-Time Transaction Exception	Cal. Civ. Code § 1798.100(3)
Operative Date	Cal. Civ. Code § 1798.198
Opt-In Rights and the Sale of Minor's Personal Information	Cal. Civ. Code § 1798.120(c), (d); Cal. Code Regs. tit. 11, §§ 7070 to 7072
Opt-Out Rights for the Sale of Personal Information	Cal. Civ. Code §§ 1798.120(a) and 1798.135(a)(4) to (6); Cal. Code Regs. tit. 11, §§ 7026 and 7028
Preemption of Local Law	Cal. Civ. Code § 1798.180
Privacy Policy	Cal. Civ. Code § 1798.130(a)(5); Cal. Code Regs. tit. 11, § 7011
Private Right of Action for Data Breaches	Cal. Civ. Code § 1798.150(a), (b)
Prohibition on Contractual Limitation on CCPA Rights	Cal. Civ. Code § 1798.192
Purpose Limitation	Cal. Civ. Code § 1798.100(b)
Reasonable Security Procedures	Cal. Civ. Code § 1798.150(a)(1)
Regulatory Action	Cal. Civ. Code § 1798.180
Reidentification of Deidentified Patient Information	Cal. Civ. Code § 1798.148
Right to Cure Violations	Cal. Civ. Code §§ 1798.150(b)(1) and 1798.155(a)
Right to Delete	Cal. Civ. Code § 1798.105(a); Cal. Code Regs. tit. 11, §§ 7020, 7021(a), (b), 7022, and 7031

Topic	Sections
Right to Know (Access)	Cal. Civ. Code § 1798.110(a) and 1798.130(a)(2), (6), (7); Cal. Code Regs. tit. 11, §§ 7020, 7021(a), (b), 7024, and 7031
Right to Information Disclosure and Notice	Cal. Civ. Code §§ 1798.100(a), (b) and 1798.115(a)
Sale or Disclosure for Business Purposes Requirements	Cal. Civ. Code §§ 1798.115(a) to (c), 1798.120, and 1798.135(a)
Service Providers	Cal. Civ. Code §§ 1798.140(v), (w) and 1798.145(j); Cal. Code Regs. tit. 11, § 7051
Statutory Damages	Cal. Civ. Code § 1798.150(b)
Supplementation of Existing Law	Cal. Civ. Code §§ 1798.175 and 1798.196
Third Party: Personal Information Sales Restriction	Cal. Civ. Code § 1798.115(d) and 1798.140(w)
Training and Recordkeeping Requirements	Cal. Civ. Code §§ 1798.130(a)(6) and 1798.135(a)(3); Cal. Code Regs. tit. 11, §§ 7100 to 7102
Verifiable Consumer Requests	Cal. Civ. Code §§ 1798.100(a), (c), (d), 1798.105(c), 1798.110(b) and 1798.115(b)
Verification: General Rules	Cal. Code Regs. tit. 11, § 7060
Verification: Password-Protected Accounts	Cal. Code Regs. tit. 11, § 7061
Verification: Non-Account Holders	Cal. Code Regs. tit. 11, § 7062

Section to Topic

Section	Topic
Cal. Civ. Code § 1798.100	Right to Information Disclosure and Notice
	Purpose Limitation
	Verifiable Consumer Requests
	Data Portability
	One-Time Transaction Exception
Cal. Civ. Code § 1798.105	Right to Deletion
	Disclosure of Deletion Rights
	Verifiable Consumer Requests
	Exceptions to Deletion Requirement

Section	Topic
Cal. Civ. Code § 1798.110	Right to Access Affirmative Disclosure Requirements Verifiable Consumer Requests
Cal. Civ. Code § 1798.115	Disclosure of Sale or Disclosure for Business Purposes Verifiable Consumer Requests Third-Party Restriction on Sale of Personal Information
Cal. Civ. Code § 1798.120	Notice of Opt-Out Rights for the Sale of Personal Information Opt-In Requirement for Sale of Minor Consumer's Personal Information
Cal. Civ. Code § 1798.125	Restriction on Discrimination Financial Incentives for Consumers
Cal. Civ. Code § 1798.130	Required Methods for Consumer Access Requests Response to Consumer Access Requests Required Disclosures Content of Privacy Notices
Cal. Civ. Code § 1798.135	Home Page Disclosure Requirements for Sale of Personal Information Compliance with Opt-Out Rights Opt-Out Rights for the Sale of Personal Information
Cal. Civ. Code § 1798.140	Definitions
Cal. Civ. Code § 1798.145	Exclusions and Exceptions to CCPA Compliance
Cal. Civ. Code § 1798.146	Additional Exclusions to CCPA Compliance for Medical and Health Information, CMIA Healthcare Providers, HIPAA Covered Entities, HIPAA Business Associates, Deidentified Patient Information, and Clinical Research Purposes
Cal. Civ. Code § 1798.148	Deidentified Patient Information: Restrictions on Reidentification and Required Contract Provisions for Sales or Licenses
Cal. Civ. Code § 1798.150	Penalties for Data Breaches Reasonable Security Procedures Right to Cure Violations Private Right to Action Statutory Damages
Cal. Civ. Code § 1798.155	Regulatory Actions Right to Cure Violations Civil Penalties Consumer Privacy Fund

Section	Topic
Cal. Civ. Code § 1798.160	Consumer Privacy Fund
Cal. Civ. Code § 1798.175	Supplementation of Existing Law
Cal. Civ. Code § 1798.180	Preemption of Local Law
Cal. Civ. Code § 1798.185	California Attorney General Rulemaking Authority
Cal. Civ. Code § 1798.192	Prohibition on Contractual Limitation on CCPA Applicability
Cal. Civ. Code § 1798.196	Supplementation of Federal and State Law
Cal. Civ. Code § 1798.198	Operative Date
Cal. Code Regs. tit. 11, § 7000	Title and Scope
Cal. Code Regs. tit. 11, § 7001	Definitions
Cal. Code Regs. tit. 11, § 7010	Overview of Required Notices
Cal. Code Regs. tit. 11, § 7011	Privacy Policy
Cal. Code Regs. tit. 11, § 7012	Notice at Collection of Personal Information
Cal. Code Regs. tit. 11, § 7013	Notice of Right to Opt-Out of Sale of Personal Information
Cal. Code Regs. tit. 11, § 7016	Notice of Financial Incentive
Cal. Code Regs. tit. 11, § 7020	Methods for Submitting Requests to Know and Requests to Delete
Cal. Code Regs. tit. 11, § 7021	Timelines for Responding to Requests to Know and Requests to Delete
Cal. Code Regs. tit. 11, § 7022	Requests to Delete
Cal. Code Regs. tit. 11, § 7024	Requests to Know
Cal. Code Regs. tit. 11, § 7026	Requests to Opt-Out
Cal. Code Regs. tit. 11, § 7028	Requests to Opt-In After Opting-Out of the Sale of Personal Information
Cal. Code Regs. tit. 11, § 7031	Requests to Know or Delete Household Information
Cal. Code Regs. tit. 11, § 7051	Service Providers
Cal. Code Regs. tit. 11, § 7060	General Rules Regarding Verification
Cal. Code Regs. tit. 11, § 7061	Verification for Password-Protected Accounts
Cal. Code Regs. tit. 11, § 7062	Verification for Non-Account Holders
Cal. Code Regs. tit. 11, § 7063	Authorized Agent
Cal. Code Regs. tit. 11, § 7070	Consumers Under 13 Years of Age
Cal. Code Regs. tit. 11, § 7071	Consumers 13 to 15 Years of Age
Cal. Code Regs. tit. 11, § 7072	Notices to Consumers Under 16 Years of Age
Cal. Code Regs. tit. 11, § 7080	Discriminatory Practices
Cal. Code Regs. tit. 11, § 7081	Calculating the Value of Consumer Data

Section	Topic
Cal. Code Regs. tit. 11, § 7100	Training
Cal. Code Regs. tit. 11, § 7101	Record-Keeping
Cal. Code Regs. tit. 11, § 7102	Requirements for Businesses Collecting Large Amounts of Personal Information

CPRA Provision Index

Topic to Section

Topic	Sections
Administrative Fines	Cal. Civ. Code §§ 1798.155(a) and 1798.199.55(a)(2)
Anti-Avoidance	Cal. Civ. Code § 1798.190
Authorized Agents	Cal. Civ. Code § 1798.185(a)(7)
California Privacy Protection Agency	Cal. Civ. Code § 1798.199.10 to 1798.199.100
Civil Penalties	Cal. Civ. Code § 1798.199.90(a)
Consent	Cal. Civ. Code § 1798.140(h)
Consumer Privacy Fund	Cal. Civ. Code §§ 1798.155(b) and 1798.160
Contractor: Definition, Contract Requirements, and Liability Waiver	Cal. Civ. Code §§ 1798.100(d), 1798.135(g), 1798.140(j)(1), and 1798.145(i)(1)
Contractor: Direct Obligations	Cal. Civ. Code §§ 1798.105(c)(3), (d), 1798.121(c), 1798.130(a)(3)(A), 1798.140(j)(2), and 1798.145(j)
Contract Requirements for Selling, Sharing, or Disclosing Personal Information to Third Parties, Contractors, or Service Providers	Cal. Civ. Code §§ 1798.100(d) and 1798.140(j)(1), (ag)(1)
Data Minimization	Cal. Civ. Code §§ 1798.100(c)
Data Portability	Cal. Civ. Code §§ 1798.110(a)(5), (b), 1798.130(a)(3)(B)(iii), 1798.145(k), and 1798.185(a)(14)
Definitions	Cal. Civ. Code § 1798.140
Disclosure of Deletion Rights	Cal. Civ. Code § 1798.105(b)
Exceptions to Deletion Requirement	Cal. Civ. Code § 1798.105(d)
Exclusions and Exceptions to CPRA Compliance	Cal. Civ. Code § 1798.145. Although not enacted by the CPRA, Cal. Civ. Code § 1798.146 also provides exceptions.

Topic	Sections
Financial Incentives for Consumers	Cal. Civ. Code §§ 1798.125(b), 1798.135(a)(4), and 1798.185(a)(6)
Household Information Rights Exclusion and Definition	Cal. Civ. Code §§ 1798.140(q) and 1798.145(p)
Methods for Submitting Requests to Know, Correct, and Delete	Cal. Civ. Code § 1798.130(a)(1)
Non-Discrimination (Right of No Retaliation)	Cal. Civ. Code § 1798.125(a)
Notice of Right to Opt-Out and Limit Use	Cal. Civ. Code § 1798.135(a) to (c)
Notice of Financial Incentive	Civ. Code § 1798.125(b)(2), (3)
Public Notice Requirements	Cal. Civ. Code §§ 1798.100(a), (b), 1798.105(b), 1798.106(b), 1798.110(b), (c), 1798.115(c), 1798.120(b), 1798.121(a), 1798.130(a)(5), 1798.135(a), (b), (c)(2), (d), and 1798.140(ad)(2)(C), (ah)(2)(C)
Operative Date	CPRA Ballot Initiative, Section 31
Opt-In Rights and the Sale or Sharing of Minor's Personal Information	Cal. Civ. Code § 1798.120(c), (d) and 1798.135(c)(5)
Opt-Out Rights for the Sale or Sharing of Personal Information	Cal. Civ. Code §§ 1798.120(a) and 1798.135(c)(4), (6)
Personal Information Definition	Cal. Civ. Code § 1798.140(v)
Preemption of Local Law	Cal. Civ. Code § 1798.180
Privacy Policy	Cal. Civ. Code § 1798.130(a)(5)
Private Right of Action for Data Breaches	Cal. Civ. Code § 1798.150(a), (b)
Prohibition on Contractual Limitation on CCPA Rights	Cal. Civ. Code § 1798.192
Purpose Limitation	Cal. Civ. Code § 1798.100(c)
Reasonable Security Procedures	Cal. Civ. Code §§ 1798.100(e), 1798.140(ac), and 1798.150(a)(1)
Regulations	Cal. Civ. Code § 1798.185
Right to Cure Violations	Cal. Civ. Code §§ 1798.150(b) and 1798.199.50
Right to Correct	Cal. Civ. Code § 1798.106(a)
Right to Delete	Cal. Civ. Code § 1798.105(a)

Topic	Sections
Right to Know (Access and Individualized Information)	Cal. Civ. Code § 1798.110(a), 1798.115(a), 1798.130(a), and 1798.140(ad)(2)(C), (ah)(2)(C)
Right to Limit Sensitive Personal Information Use and Sharing	Cal. Civ. Code §§ 1798.121 and 1798.140(ae)
Sale, Sharing, or Disclosure for Business Purposes Requirements	Cal. Civ. Code §§ 1798.100(d), 1798.115(a) to (c), 1798.120, 1789.121, and 1798.135(a)
Sensitive Personal Information Definition	Cal. Civ. Code § 1798.140(ae)
Service Provider: Definition, Contract Requirements, and Liability Waiver	Cal. Civ. Code §§ 1798.100(d), 1798.135(g), 1798.140(ag)(1), and 1798.145(i)(1)
Service Provider: Direct Obligations	Cal. Civ. Code §§ 1798.105(c)(3), (d), 1798.121(c), 1798.130(a)(3)(A), 1798.140(ag)(2), and 1798.145(j)
Statutory Damages	Cal. Civ. Code § 1798.150(a), (b)
Subcontracting	Cal. Civ. Code § 1798.140(ag)(2)
Supplementation of Existing Law	Cal. Civ. Code §§ 1798.175 and 1798.196
Trade Secrets Exception	Cal. Civ. Code § 1798.100(f) and 1798.185(a)(3), (15)
Third Party: Definition, Contract Requirements, and Liability Waiver	Cal. Civ. Code § 1798.100(d), 1798.135(g), 1798.140(ai), 1798.145(i)(2)
Third Party: Direct Obligations and Sales/ Sharing Restrictions	Cal. Civ. Code § 1798.100(b), 1798.115(d), 1798.140(ad)(2)(C), (ah)(2)(C), and 1798.190(a)
Training and Recordkeeping Requirements	Cal. Civ. Code §§ 1798.130(a)(6) and 1798.135(a)(3)
Verifiable Consumer Requests	Cal. Civ. Code §§ 1798.105(c), 1798.106(c), 1798.110(b), 1798.115(b), 1798.130(a)(2) to (4), and 1798.140(ak)

Section to Topic

Section	Topic
Cal. Civ. Code § 1798.100	General Duties of Businesses that Collect Personal Information • Consumer Notices • Purpose Limitation and Data Minimization • Contract Requirements • Reasonable Security Requirements

Section	Topic
Cal. Civ. Code § 1798.105	Consumer's Right to Delete Personal Information
Cal. Civ. Code § 1798.106	Consumer's Right to Correct Inaccurate Personal Information
Cal. Civ. Code § 1798.110	Consumers' Right to Know What Personal Information is Being Collected; Right to Access Personal Information
Cal. Civ. Code § 1798.115	Consumers' Right to Know What Personal Information is Sold or Shared and to Whom
Cal. Civ. Code § 1798.120	Consumers' Right to Opt Out of Sale or Sharing of Personal Information • Minor's Right to Opt-In
Cal. Civ. Code § 1798.121	Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information
Cal. Civ. Code § 1798.125	Consumers' Right of No Retaliation Following Opt Out or Exercise of Other Rights • Financial Incentives for Consumers
Cal. Civ. Code § 1798.130	Notice, Disclosure, Correction, and Deletion Requirements
Cal. Civ. Code § 1798.135	Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information
Cal. Civ. Code § 1798.140	Definitions
Cal. Civ. Code § 1798.145	Exemptions
Cal. Civ. Code § 1798.146	Additional Exclusions to CCPA Compliance for Medical and Health Information, CMIA Healthcare Providers, HIPAA Covered Entities, HIPAA Business Associates, Deidentified Patient Information, and Clinical Research Purposes
Cal. Civ. Code § 1798.148	Deidentified Patient Information: Restrictions on Reidentification and Required Contract Provisions for Sales or Licenses
Cal. Civ. Code § 1798.150	Personal Information Security Breaches (Private Right of Action)
Cal. Civ. Code § 1798.155	Administrative Enforcement
Cal. Civ. Code § 1798.160	Consumer Privacy Fund
Cal. Civ. Code § 1798.175	Conflicting Provisions
Cal. Civ. Code § 1798.180	Preemption
Cal. Civ. Code § 1798.185	Regulations
Cal. Civ. Code § 1798.190	Anti-Avoidance
Cal. Civ. Code § 1798.192	Prohibition on Contractual Limitation on CPRA Applicability
Cal. Civ. Code §§ 1798.199.10 to 1798.199.100	California Privacy Protection Agency

CCPA Regulations Development Timeline

- **October 10, 2019:** The California AG releases its first draft CCPA Regulations and its Initial Statement of Reasons (ISOR) for the proposed adoption of the CCPA Regulations for public comments (see OAG: Proposed Text of Regulations and OAG: ISOR).
- **February 7 and 10, 2020**: After reviewing the large volume of comments, the California AG proposes numerous modifications to its initial draft CCPA Regulations (see OAG: Redline Text of Modified Regulations and Legal Update, Revised CCPA Regulations Draft Released for Comment).
- **March 11, 2020:** The California AG releases a second modified version of the proposed CCPA Regulations (see OAG: Redline Text of Second Modifications and Legal Update, Second Revised CCPA Regulations Draft Released for Comment).
- **June 1, 2020:** The California AG submits final proposed CCPA regulations to the California Office of Administrative Law (OAL) for approval (see OAG: Final Text of Regulations, OAG: FSOR, and Legal Update, California AG Submits Final Proposed CCPA Regulations to OAL for Approval)).
- **August 14, 2020:** After the California AG withdraws four provisions and accepts various non-substantive revisions for accuracy, consistency, and clarity, the OAL approves the final CCPA Regulations with immediate effect and files them with the Secretary of State (see OAG: OAL Notice of Approval in Part and Withdrawal in Part, OAG: Final Text of Regulations, OAG: Addendum to FSOR, and Legal Update, Final CCPA Regulations Approved).
- **October 12, 2020:** The California AG releases a third set of proposed modifications to the CCPA Regulations (see Notice of Third Set of Proposed Modifications to Text of Regulations, Text of Modified Regulations, and Legal Update, Third Set of Proposed Modifications to CCPA Regulations Released for Comment).
- **December 10, 2020**: The California AG releases a fourth set of proposed modifications to the CCPA Regulations (see Notice of Fourth Set of Proposed Modifications to Text of Regulations, Text of Modified Regulations, and Legal Update, Fourth Set of Proposed Modifications to CCPA Regulations Released for Comment).
- **March 15, 2021**: The OAL approved modifications to the CCPA Regulations, with some additional revisions (see Final Regulation Text and Legal Update, California OAL Approves Additional CCPA Regulations). The regulations took immediate effect on March 15, 2021.

For more on the California AG's prior rulemaking process, including the public comments received, see OAG: CCPA Regulations.

For more on the development of CPRA Regulations, see CPRA Regulation Tracker.