THOMSON REUTERS
PRACTICAL LAW™

Drafting CCPA and CPRA Notices and Privacy Policies

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-019-6347**
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). This Note explains the requirements to provide California consumers with certain privacy notices when collecting, using, selling, sharing, disclosing, and retaining personal information. The Note also provides guidance and suggestions for aligning an organization's current privacy notice or privacy policy with the CCPA and CPRA's requirements.

California established the first US-based comprehensive consumer privacy law when it enacted the California Consumer Privacy Act (CCPA) on June 28, 2018 (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. However, businesses should continue to follow the CCPA and CCPA Regulations while they prepare for the CPRA's new requirements.

The CCPA and CPRA grant California residents enhanced rights regarding their personal information and impose various data protection duties on certain entities conducting business in California. They also establish specific public notification obligations for covered businesses that collect, share, or sell personal information about California residents. Given its broad reach, the CCPA and CPRA are likely to significantly impact entities both inside and outside California that collect and process California residents' personal information.

This Note details the CCPA and CPRA's privacy policy and other public notice requirements to help businesses review and adapt their current privacy policies or draft new notices to meet those standards.

For a broader discussion of the CCPA and CPRA, including which businesses must comply and how the laws define consumers as California residents, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).

For more on responding to individual requests to know and other consumer rights requests, see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests. For the full list of CCPA and CPRA resources, see California Privacy Toolkit (CCPA and CPRA).

For general considerations when drafting privacy notices, see Practice Note, Drafting Privacy Notices.

Preliminary Considerations

Amendments and Regulations

CCPA amendments and the CPRA temporarily exempt workforce-related personal information and personal information reflected in certain business-to-business (B2B) communications from most CCPA and CPRA provisions until January 1, 2023. However, employers must still provide the CCPA's notice at collection even though the workforce exception exempts employers from most other requirements (see Collection Notice). For more on these exceptions, see Practice Notes, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Temporary Exemptions and California Privacy Laws (CCPA and CPRA): Impact on Employers.

Regulations developed by the California Attorney General (California AG) establish detailed requirements that organize, operationalize, and provide context for the CCPA's different notice provision (CCPA Regulations) (Cal. Code Regs. tit. 11, §§ 7000 to 7102). For more on the CCPA Regulation's development, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): CCPA Regulations Development Timeline.

The CCPA currently allows businesses to seek the California AG's opinion or advice on any statutory compliance questions (Cal. Civ. Code § 1798.155(a)). However, the CPRA removed this direct guidance option. The CPRA also moves the California AG's rulemaking and guidance responsibilities to a newly created regulator, the California Privacy Protection Agency (Cal. Civ. Code §§ 1798.185(d), 1798.199.10(a), and 1798.199.40(b), (d), (e), (f)). For more on the newly formed Agency's rulemaking process and its progress on issuing new or amended regulations for the CPRA's different notice obligations, see CPRA Regulation Tracker.

For more on the CCPA and CPRA's history and ongoing amendments efforts, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): History of the CCPA and CPRA and California Privacy-Related Legislation Tracker.

General Application or Separate Notice for California Residents

As a state law, the CCPA and CPRA's coverage only extends to businesses operating within California's jurisdictional reach. The CCPA and CPRA also place additional thresholds on a covered business's size or personal information sales to limit its impact on small businesses (see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Covered Businesses). Further, only California residents are entitled to receive the CCPA and CPRA's required information disclosures (see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Protected Individuals).

Businesses with nationwide customer bases or operations face a choice between two different options:

- Only provide the CCPA and CPRA's consumer rights and disclosure requirements to consumers residing in California and develop separate privacy practices for consumers located elsewhere.
- Elevate the CCPA and CPRA's requirements to a company-wide standard and extend its protections to all US-based customers.

Opting to limit the CCPA and CPRA's protections to California residents may require the business to:

- Determine whether each customer or website visitor qualifies as a California resident.
- Change internal systems to track residential statuses, including processes for updating the status when individuals move.
- Provide California residents with:
  - separate websites; and
  - separate or supplemental privacy notices.
- Establish separate internal procedures and systems for handling California residents' personal information.

For a model privacy notice addendum for California Residents, see Standard Document, CCPA Privacy Policy for California Residents.

However, new consumer privacy laws in Colorado and Virginia that take effect in 2023 may increase the burden and difficulty of adopting state-by-state approaches (see Quick Comparison Chart (CPRA and VCDPA) and Legal Update, Colorado Enacts Privacy Act).

Businesses that adopt one common approach for all US customers should compare their current privacy notices to the CCPA and CPRA's requirements and make any required adjustments.

Data Maps

Accurately providing the CCPA and CPRA's required disclosures first requires a full understanding of exactly how the business collects, obtains, uses, stores, shares, sells, and protects personal information. To accomplish this, most organizations start by developing detailed data maps that track and visualize how information moves through the business's systems during the data lifecycle.

For more on developing data maps, see Practice Note, Drafting Privacy Notices: Preparing to Draft the Privacy Notice and Standard Document, Privacy Audit Questionnaire.

Required Notices

All covered businesses must publish several disclosures regarding their personal information practices and the consumer's rights under the CCPA. To help businesses understand their different disclosure obligations, the CCPA Regulations organize them into four distinct notice types:

- **A Privacy Policy**, which every covered business must provide (see Privacy Policy).

- **Collection Notices**, which covered businesses must provide whenever they collect personal information (see Collection Notice).
- **Opt-Out Right Notices**, which every covered business selling personal information must provide (see Opt-Out Right Notice).
- **Financial Incentive Notices**, which covered businesses must provide whenever they offer a financial incentive, price difference, or service difference related to the collection, retention, or sale of personal information (see Financial Incentive Notice).

(Cal. Code Regs. tit. 11, § 7010.)

The CPRA reorganizes and expands these public notice requirements but does not change the four primary notice types that the CCPA Regulations currently outline. However, businesses should expect the California Privacy Protection Agency to update or issue new regulations regarding each of these required notices (Cal. Civ. Code § 1798.185(6), (22); see CPRA Regulation Tracker).

Shared Presentation, Location, and Accessibility Requirements

The CCPA Regulations set out general presentation requirements that apply to all CCPA notices. They require the business to design and present the notice information in a way that is easy to read and understandable to an average consumer, 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.
- Ensuring consumers with disabilities can 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 308(a)(2)(A) to (D)).

The CCPA and CCPA Regulations also set unique presentation requirements for each notice type:

- For privacy policies, see Presentation Requirements.
- For collection notices, see Presentation Requirements.
- For opt-out right notices, see Placement and Links.
- For financial incentive notices, see Presentation Requirements.

CPRA Revisions: Shared Presentation, Location, and Accessibility Requirements

The CPRA does not materially change these presentation requirements and it charges the California Privacy Protection Agency with developing regulations to ensure that businesses provide the CPRA's required disclosures in a manner that is easily understood by average consumers, accessible to consumers with disabilities, and in the same language primarily used for consumer interactions (Cal. Civ. Code § 1798.185(a)(6)). It also directs the California Privacy Protection Agency to develop regulations that harmonize opt-out mechanisms and consumer notices to promote clarity and the CPRA's functionality (Cal. Civ. Code § 1798.185(a)(22)). For more on the regulation process and progress, see CPRA Regulation Tracker.

Privacy Policy

The CCPA's general consumer privacy notice obligations extend over several different sections that sometimes overlap or cross-reference each other. To help business comply with these obligations, the CCPA Regulations require all businesses to provide consumers with a privacy policy describing its online and offline business practices on personal information collection, use, disclosure, and sale, and the consumer's related rights (Cal. Code Regs. tit. 11, §§ 7001(p) and 7011).

The required elements in a CCPA-compliant privacy policy are:

- **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 Consumer Rights);
  - instructions for submitting a verifiable consumer request to know and links to any online request form or portal provided to make those requests (see Consumer Request Process);

  - a general description of the business's process for verifying consumer requests, including any information the consumer must provide (see Consumer Request Process);
  - 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 (see Personal Information Sources);
  - the business or commercial purpose for collecting or selling personal information (see Business or Commercial Purpose);
  - a statement on personal information disclosures for a business purpose (see Personal Information Disclosures for a Business Purpose); and
  - a statement on personal information sales disclosures (see Personal Information Sales and Opt-Out Links).
- **Right to deletion** disclosures, including an explanation of the right, submission instructions, and the verification process (see Consumer Rights and Consumer Request Process).
- **Right to opt-out** disclosures, including an explanation of the right, statements about sales, submission instructions, and the verification process (see Personal Information Sales and Opt-Out Links, Consumer Rights and Consumer Request Process).
- **Right to non-discrimination** disclosure, explaining the consumer's right not to receive discriminatory treatment by the business for exercising their CCPA consumer rights (see Consumer Rights).
- **Authorized agent** disclosure, describing how agents can make CCPA-related requests on the consumer's behalf (see Consumer Request Process).
- **Statistical metrics** on the business's response to consumer rights requests, if the business meets certain disclosure thresholds (see Consumer Rights Request Metrics).
- **Deidentified patient information** disclosures, if the business sells or discloses deidentified patient information (see Deidentified Patient Information).
- **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 (see Contact Information).
- **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).)

This rights-based listing of required privacy policy elements differs from the approach that many US-based privacy policies currently take, which often present each of these elements, but in a different order (see, for example, Standard Document, Website Privacy Policy).

However, the California AG specifically notes that its regulations provided the list to help clarify the CCPA's privacy notice content requirements, not to prescribe how a business's privacy policy organizes and displays that information (CCPA ISOR at 14). This allows businesses to present each privacy policy element in their preferred order, addressing the following topics:

- Types of personal information (see Personal Information Categories).
- Sources of personal information (see Personal Information Sources).
- Business or commercial purposes (see Business or Commercial Purpose).
- Consumer rights description (see Consumer Rights).
- Consumer rights request process (see Consumer Request Process).
- Third-party sharing (see Third Party Categories).
- Business purpose disclosures (see Personal Information Disclosures for a Business Purpose).
- Personal information sales and opt-out links (see Personal Information Sales and Opt-Out Links).

For a section-by-section discussion of the different consumer notice requirements in the CCPA and CCPA Regulations, see Box, CCPA Section-by-Section Notice Requirement Summary.

CPRA Revisions: Privacy Policy

The CPRA retains the CCPA's scattershot approach that spreads its general consumer disclosure obligations out over several different, overlapping sections. Businesses should expect the California Privacy Protection Agency to issue regulations that similarly combine the CPRA's disparate notice requirements into one public privacy policy requirement (Cal. Civ. Code § 1798.185(a)(6), (22), (d); see CPRA Regulation Tracker). The CPRA's revised collection notice requirements include a new element that discloses the collected personal information's expected retention period (Cal. Civ. Code § 1798.100(a)(3) (effective January 1, 2023)). Consequently, a CPRA privacy policy should include a similar retention disclosure (see CPRA Revisions: New Retention Period Disclosure). This Note discusses CPRA revisions that may impact the other common privacy policy sections in-line below.

For a section-by-section discussion of the CPRA's different consumer notice requirements, see Box, CPRA Section-by-Section Notice Requirement Summary.

Personal Information Categories

A CCPA-compliant privacy policy must describe the categories of personal information the business collected about consumers during the past 12 months (Cal. Civ. Code §§ 1798.110(c)(1) and 1798.130(a)(5)(B); Cal. Code Regs. tit. 11, § 7011(c)(1)(D)).

The CCPA defines personal information as 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).)

Notably, the CCPA protects data even if it does not relate to a single individual, because it covers households and protects data even if the record does not contain a name. This means personal information under the CCPA includes items such as profiles associated with internet cookie identifiers or household television viewing profiles. The CCPA also clarifies that its provisions apply regardless of the data collection method used. It covers, for example, personal information collected electronically, recorded over the phone, entered on printed forms, or generated by an algorithm. (Cal. Civ. Code § 1798.175.)

The definition then provides 11 different categories with examples of data that could qualify as personal information, such as internet protocol (IP) addresses, when they identify or relate to a particular consumer or household. The CCPA directs the business to use and reference these 11 statutory categories for its privacy policy's personal information collection disclosure (Cal. Civ. Code §§ 1798.130(a)(5)(B) and 1798.130(c)). At a high level, those 11 categories are:

- Identifiers.
- California Customer Records' personal information categories (Cal. Civ. Code § 1798.80(e)).
- California or federal law protected classifications characteristics (see State Q&A, Anti-Discrimination Laws: California).
- Commercial information.
- Biometric information.
- Internet or other similar network, browsing, or search activity.
- Geolocation data.
- Audio, electric, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Non-publicly available educational information 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.

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

For a full list of the personal information category examples, see Box, Personal Information Category Descriptions.

When drafting the privacy policy's personal information category disclosures, a business should:

- Review its operations to ensure the privacy policy disclosures accurately reflect the types of personal information it collects (see Data Maps).
- Recognize that the CCPA's broader personal information and collection definitions may require reviewing business processes that obtain personal information from third parties or generate personal information by creating profiles.
- Match the personal information collected over the past 12 months to the closest CCPA personal information category.

The CCPA Regulations require the privacy policy to present the personal information category disclosures in a way that provides consumers with a meaningful understanding of what the business collects (Cal. Code

Regs. tit. 11, § 7011(c)(1)(D)). For example, to improve reader comprehension, a business could:

- Presenting this information in a table.
- Develop alternate infographic formats or icons.
- Use interactive forms that pop-up more information for each category when the reader hovers over the category name, including specific examples.

For a table example, see Standard Document, CCPA Privacy Policy for California Residents: Information We Collect.

Businesses must update the privacy notice's collected personal information category list at least once every 12 months (Cal. Civ. Code § 1798.135(a)(5)).

CPRA Revisions: Personal Information and Sensitive Personal Information Categories

The CPRA adds a new sensitive personal information category and broadens the privacy policy disclosures to include separate disclosures for any sensitive personal information categories collected (Cal. Civ. Code §§ 1798.100(a)(2), 1798.130(c), and 1798.140(v)(1)(L), (ae) (effective January 1, 2023)).

The CPRA also directs businesses to use and reference the 11 statutory personal information categories and the nine statutory sensitive personal information categories for their privacy policy's personal information collection disclosure (Cal. Civ. Code § 1798.130(c) (effective January 1, 2023)). At a high level, the nine sensitive personal information categories are:

- Government identifiers (social security, driver's license, state identification card, or passport number).
- Complete account access credentials (user names, account numbers, or card numbers combined with required access/security code or password).
- Precise geolocation.
- Racial or ethnic origin.
- Religious or philosophical beliefs.
- Union membership.
- Genetic data.
- Mail, email, or text messages contents.
- Unique identifying biometric information.
- Health, sex life, or sexual orientation information.

For the full sensitive personal information definition and examples, see Box, CPRA Revisions: New Sensitive Personal Information Categories.

However, the CPRA adds an important, but challenging qualifier to when personal information qualifies as sensitive. A business that collects or processes sensitive personal information **without** the purpose of inferring characteristics about a consumer can treat it as just regular personal information when complying with the CPRA's different requirements (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 § 1798.185(a)(19)(C)(iv); Cal. Civ. Code § 1798.121(d) (effective January 1, 2023); see CPRA Regulation Tracker).

Personal Information Sources

A CCPA-compliant notice must specifically describe the categories of sources from which the business collects personal information. It must identify these sources with enough particularity to provide consumers with a meaningful understanding. (Cal. Civ. Code § 1798.110(c)(2); Cal. Code Regs. tit. 11, §§ 7001(d) and 7011(c)(1)(E).)

A business collects personal information under the CCPA when it uses any means to obtain it, including:

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

(Cal. Civ. Code § 1798.140(e).)

Common means to collect personal information include:

- Actively from the consumer.
- Passively from clickstream data that website cookies gather.
- By observing the consumer's behavior.
- By purchasing information from data brokers.

While the CCPA does not establish specific source category types, as it does for personal information, businesses should remain mindful of the CCPA's broad collection definition when developing their category list. Generic, overly broad, or vague category descriptions may receive greater scrutiny.

Source category descriptions for the types of people and entities who provide personal information to the business may include:

- Customers, through direct interactions and form.
- Internet websites, through passive collection of information about a customer's interactions, including page clicks, time spent, or other automatically collected meta-data.
- Internet cookies.
- Advertising networks.
- Internet service providers.
- Data analytics providers.
- Operating systems and platforms.
- Observations from monitoring behavior, such as store video camera or surveillance systems.
- Search terms.
- Automated license plate readers.
- Data brokers or resellers.
- Social media services, like Twitter or Facebook.
- Government databases.
- Service providers.

When drafting the privacy notice, the business should:

- Describe the business's sources with sufficient detail to provide clear and meaningful disclosures about where acquired personal information originates.
- Avoid generic or overly broad language.
- Carefully review its personal information data flows to provide clear and accurate disclosures.

CPRA Revisions: Personal Information Sources

The CPRA does not substantively change this disclosure requirement (Cal. Civ. Code §§ 1798.110(c)(2), 1798.130(a)(5)(B)(ii), and 1798.140(f) (effective January 1, 2023)).

Business or Commercial Purpose

The CCPA privacy policy must identify the business or commercial purposes for collecting or selling personal information (Cal. Civ. Code §§ 1798.100(b) and 1798.110(c)(3); Cal. Code Regs. tit. 11, § 7011(c)(1)(F)). This general privacy policy disclosure is in addition to the notice a business must provide at or before the point of collection (see Collection Notice).

The CCPA restricts use of collected data to actions reasonably necessary for and proportionate to the notified purposes or another contextually compatible operational purpose (Cal. Civ. Code § 1798.100(b)). The business should therefore ensure that its privacy policy comprehensively describes all current and reasonably anticipated use cases to meet the CCPA's disclosure and purpose limitation requirements. The CCPA Regulations do not directly tie this disclosure to the last 12 months, as it does for personal information collections (see Personal Information Categories). However, as a best practice, drafters should ensure the privacy policy describes all the purposes for which the business actually used or sold collected personal information during the last 12 months.

Publishing clear, complete, and specific use purpose descriptions also benefits the business by providing transparency and lowering potential enforcement or compliance risks. For more on what qualifies as a business or commercial purpose, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Business Purposes and Commercial Purposes. For an example of a personal information use purpose disclosure, see Standard Document, CCPA Privacy Policy for California Residents: Use of Personal Information.

CPRA Revisions: Business or Commercial Purpose

The CPRA extends this disclosure requirement to cover sharing personal information for cross-context behavioral advertising (Cal. Civ. Code §§ 1798.110(c)(3), 1798.130(a)(5)(B)(iii), and 1798.140(ah) (effective January 1, 2023)).

It also slightly tweaks the CCPA's purpose limitation language. Under the CPRA the business must:

- 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).)

Third Party Categories

A CCPA-compliant privacy notice must also disclose the categories of third parties with which the business shares personal information (Cal. Civ. Code §§ 1798.110(c)(4) and 1798.130(a)(5)). The CCPA Regulations clarify that the business should disclose these categories as part of their required policy statements on personal information sales and business purpose disclosures (Cal. Code Regs. tit. 11, §§ 7001(e) and 7011(c)(1)(G); see Personal Information Disclosures for a Business Purpose and Personal Information Sales and Opt-Out Links).

While not specifically defined, the concept of sharing generally includes any disclosure of personal information and it does not require a sale. It may, for example, include granting a third party access to the business's internal systems containing personal information.

The CCPA does not establish specific categories describing the different types of third parties. However, the CCPA Regulations define the categories of third parties as meaningful descriptions of the third parties with whom a business shares personal information (Cal. Code Regs. tit. 11, § 7001(e)). Examples include:

- Service providers.
- Data brokers or aggregators.
- Advertisers.
- Affiliates.
- Partners.
- Parent or subsidiary organizations.
- Social media companies.
- Internet cookie information recipients, like Google.

Businesses should keep the CCPA's purpose of providing reasonable and accessible disclosures in mind when developing their third party category list. As with personal information source categories, generic, overly broad, or vague third-party category descriptions may receive greater scrutiny. For more on the CCPA and third parties, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Service Providers and Third Parties.

When drafting the privacy notice, the business should:

- Select descriptive category names that provide clear and meaningful disclosures about personal information sharing and the different types of third parties that:
  - receive;
  - view;
  - obtain; or
  - access personal information from the business.
- Avoid generic or overly broad language.
- Carefully review its personal information data flows to provide clear and accurate disclosures.

CPRA Revisions: Third Party Categories

Because the CPRA adds a new, but narrow definition for the term "shares," the CPRA slightly tweaks the language in this section so it requires the notice to list the categories of third parties to whom the business discloses personal information (Cal. Civ. Code §§ 1798.110(c)(4), 1798.130(a)(5)(B)(iv), and 1798.140(ah) (effective January 1, 2023)). However, this change should not substantively alter the current disclosure requirements.

Personal Information Disclosures for a Business Purpose

A CCPA-compliant notice must contain a statement about personal information the business disclosed for a business purpose during the preceding 12 months that either:

- States that no disclosures occurred.
- Lists the categories of personal information disclosed:
  - using the CCPA's personal information categories that most closely describe the personal information (see Personal Information Categories); and
  - provides, for each personal information category identified, the categories of third parties to whom personal information was disclosed (see Third Party Categories)

(Cal. Civ. Code §§ 1798.115(c)(2) and 1798.130(a)(5)(C)(ii); Cal. Code Regs. tit. 11, § 7011(c)(1)(G).)

The business should carefully review the types of personal information it discloses for a business purpose to identify which categories it should list in the privacy notice. Sharing personal information with service providers will usually fall under this disclosure requirement. For more on the CCPA's service provider requirements, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Service Providers and Third Parties.

The business must also update this personal information disclosures list at least once every 12 months (Cal. Civ. Code § 1798.130(a)(5)).

To understand when sharing personal information constitutes a business purpose disclosure, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Distinguishing Between Sales and Business Purposes Disclosures.

CPRA Revisions: Personal Information Disclosures for a Business Purpose

The CPRA does not substantively change this notice requirement, but it does change the business purpose definition (Cal. Civ. Code §§ 1798.115(c)(2), 1798.130(a)(5)(C)(ii), (c) and 1798.140(e) (effective January 1, 2023)). For more on how the CPRA defines a business purpose, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): CPRA Revisions: Business Purposes.

The CPRA also alters how it defines service providers, adding a new, but similar entity called contractors (Cal. Civ. Code § 1798.140(j), (ag), (ai) (effective January 1, 2023)). The business's personal information disclosures to both service providers and contractors will likely fall under this disclosure requirement. For more on service providers and contractors under the CPRA, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): CPRA Revisions: Service Provider, Contractor, Third Party Definitions.

Finally, the CPRA adds a new personal information category for sensitive personal information that businesses should include in this disclosure (Cal. Civ. Code §§ 1798.130(c) and 1798.140(v), (ae) (effective January 1, 2023); see CPRA Revisions: Personal Information and Sensitive Personal Information Categories).

Personal Information Sales and Opt-Out Links

Under the CCPA, the privacy policy for a business that sells personal information must:

- State whether or not the business sells personal information.
- State whether the business has actual knowledge that it sells the personal information of minors under age 16.
- Inform consumers about their personal information sales restriction rights (see Consumer Rights).
- Provide the business's opt-out right notice content or a link to its location (see Opt-Out Right Notice).
- List the categories of personal information it sold during the preceding 12 months, if applicable:
  - using the CCPA's personal information categories that most closely describe the personal information (see Personal Information Categories); and
  - provide, for each personal information category identified, the categories of third parties to whom personal information was sold (see Third Party Categories).

(Cal. Civ. Code §§ 1798.115(c)(1), 1798.120(b), 1798.130(a)(5)(C)(i), and 1798.135; Cal. Code Regs. tit. 11, § 7011(c)(1)(G).)

The CCPA requires two separate personal information category lists for sales and business purpose disclosures (Cal. Civ. Code § 1798.130(a)(5)(C); see Personal Information Disclosures for a Business Purpose). However, the CCPA Regulations discuss these two personal information category lists as one element and combine it with the CCPA's required disclosure of the categories of third parties with whom the business shared personal information, which does not require distinguishing between sales and business purpose disclosures (Cal. Civ. Code § 1798.110(c)(4); Cal. Code Regs. tit. 11, § 7011(c)(1), (g)(1) to (2); see Third Party Categories).

While there are several ways a business could present these different disclosures, providing separate sales and business purpose disclosures that identify which categories of third parties received each personal information category provides clearer and more transparent consumer disclosures. It may also help the business respond to consumer request to know that do require separate lists (see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests: Individualized Privacy Notice).

The business must update its personal information category list disclosures at least once every 12 months (Cal. Civ. Code § 1798.130(a)(5)).

For more on the CCPA's sale opt-out rights, see Practice Notes, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Sale Opt-Out and Opt-In Rights and Responding to CCPA and CPRA Consumer Rights Requests.

CPRA Revisions: Personal Information Sales or Sharing and Opt-Out Links

The CPRA expands the consumer's opt-out right, and the corresponding notice requirements outlined above, to include sharing personal information for cross-context behavioral advertising purposes (Cal. Civ. Code §§ 1798.100(a)(1), (2), 1798.115(c)(1), 1798.120(b), 1798.130(a)(5)(C)(i), and 1798.135 (effective January 1, 2023)). The CPRA's personal information disclosures should also include the new sensitive personal information categories (Cal. Civ. Code §§ 1798.130(c) and 1798.140(v), (ae) (effective January 1, 2023); see CPRA

Revisions: Personal Information and Sensitive Personal Information Categories).

The CPRA also allows the California Privacy Protection Agency to create a user-directed, opt-out preference signal standard that business can use as an alternative to the opt-out right notice links (Cal. Civ. Code §1798.135(b) (effective January 1, 2023); see CPRA Revisions: Consumer Preference Signal Exception and CPRA Regulation Tracker). Once that standard is established, a business opting to use it can replace the privacy policy's opt-out notice links with a statement that it will honor the consumer's opt-out preference signals (Cal. Civ. Code §1798.135(c)(2) (effective January 1, 2023)).

For more on the CPRA's sales and sharing opt-out rights, see Practice Notes, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): CPRA Revisions: Sharing Opt-Out and Opt-In Rights and Responding to CCPA and CPRA Consumer Rights Requests: CPRA Revisions: Responding to Sharing Opt-Out and Opt-In Requests.

Resales of Personal Information

The CCPA restricts third-party sale recipients from reselling the personal information unless the consumer receives explicit notice of the potential resale and an opportunity to opt-out (Cal. Civ. Code §§ 1798.115(d)). For more on collection and opt-out right notices, see Collection Notice and Opt-Out Right Notice.

CPRA Revisions: Resales of Personal Information

The CPRA retains the CCPA's resale restriction and expands it to include personal information about a consumer shared with a third party for cross-context behavioral advertising purposes (Cal. Civ. Code §§ 1798.115(d) and 1798.140(ah) (effective January 1, 2023)).

CPRA Revisions: Sensitive Personal Information Use and Disclosure Limitation Links

The CPRA requires the business's privacy policy to:

- Disclose that consumers have the right to limit the use or disclosure of their sensitive personal information to just actions necessary to perfom specific purposes listed in the statute.
- State whether the business uses, or discloses to a service provider or contractor, sensitive personal information for purposes other than what the CPRA specifically allows after a consumer exercises their limitation right and specify the additional purposes.
- Inform consumers about their senstive personal information limitation rights and how to exercise them.
- Provide the business's limitation notice content or a link to its location. Once the California Privacy Protection Agency establishes an opt-out prefernce signal standard, the business could alternatively provide a statement that it will honor the consumer's opt-out preference signals. (See CPRA Revisions: Sharing Opt-Out and Sensitive Personal Information Limitation Right Notices, CPRA Revisions: Consumer Preference Signal Exception, and CPRA Regulation Tracker.)

(Cal. Civ. Code §§ 1798.121(a), 1798.130(a)(5)(A), 1798.135(c)(2) (effective January 1, 2023).)

The CPRA specifically identifies the following purposes for which the business may continue using or disclosing sensitive personal information after receiving a consumer's limitation request:

- To perform services or provide goods that an average consumer requesting those goods or services would reasonably expect.
- To help ensure security and integrity, if that use is reasonably necessary and proportionate.
- To perform short-term, transient uses, 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.
- To 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.
- To verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business.
- To improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

- To perform other actions that CPRA regulations authorize.

(Cal. Civ. Code §§ 1798.121(a) and 1798.140(e)(2), (4), (5), (8).)

For more on the CPRA's right to limit senstive personal information use and disclosure, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): CPRA Revisions: New Right to Restrict Sensitive Personal Information Processing and Responding to CCPA and CPRA Consumer Rights Requests: CPRA Revisions: Responding to Sensitive Personal Information Limitation Requests.

Consumer Rights

The CCPA establishes several new consumer rights regarding personal information, including:

- An individualized right to know:
  - what personal information a business collected, sold, or disclosed about them, including the categories of third parties who purchased or received their data; and
  - the specific pieces of personal information held (data portability right).
- Deletion rights.
- Personal information sale prevention rights.
- Freedom from discrimination.

(Cal. Civ. Code §§ 1798.105(b), 1798.110(c)(5), 1798.120(b), 1798.125(b)(2), (3), and 1798.135(a)(2).)

A CCPA-compliant privacy notice must describe these personal information rights to consumers (Cal. Civ. Code § 1798.130(a)(5)(A); Cal. Code Regs. tit. 11, § 7011(c)(1)(A), (2)(A), (3)(A), (4)(A)). A business must also update this rights description at least once every 12 months (Cal. Civ. Code § 1798.135(a)(5)).

For a full discussion of these rights, see Practice Notes, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Consumer Rights and Responding to CCPA and CPRA Consumer Rights Requests. For a model privacy policy description of these rights, see Standard Document, CCPA Privacy Policy for California Residents: Your Rights and Choices.

CPRA Revisions: Consumer Rights

The CPRA adds new consumer rights to:

- Correct inaccurate personal information.
- Opt-out of sharing personal information for cross-context behavioral advertising purposes.
- Restrict sensitive personal information processing.

(Cal. Civ. Code §§ 1798.106, 1798.120, 1798.121 and 1798.140(ah) (effective January 1, 2023).)

A CPRA-compliant privacy notice must also describe these new personal information rights to consumers (Cal. Civ. Code § 1798.130(a)(5)(A) (effective January 1, 2023)).

For a full discussion of these new rights, see Practice Notes, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) and Responding to CCPA and CPRA Consumer Rights Requests.

Consumer Request Process

A CCPA-compliant privacy notice must also inform consumers how to exercise their personal information rights. It should:

- Provide instructions for submitting verified consumer requests to know and delete.
- Provide links to any online request form or portal for making the requests, if offered.
- Generally describe the process the business will use to verify the consumer's request, including any information the consumer must provide.
- Explain how a consumer may designate an authorized agent to make requests on their behalf.
- If the business has actual knowledge that it sells personal information about consumers under 16 years old a description of the process for:
  - opting into personal information sales; and
  - submitting verified consumer requests to know and delete for minors.

(Cal. Code Regs. tit. 11, § 7011(c)(1)(B), (1)(C), (2)(B), (2)(C), (5), (9).)

The CCPA Regulations clarify that the privacy policy disclosure requirements related to consumers under 16 apply even if the business only targets consumers under 13 or only targets consumers between 13 and 15 (Cal. Code Regs. tit. 11, §§ 7070, 7071, and 7072(a)).

For more on the CCPA's consumer rights submission and response requirements, see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests.

The business must also update this customer request description at least once every 12 months (Cal. Civ. Code § 1798.135(a)(5)).

CPRA Revisions: Consumer Request Process

A CPRA-complaint privacy notice should include similar disclosures but expand them to include the same information for the CPRA's new consumer rights (Cal. Civ. Code §§ 1798.130(a)(1)(A), (5)(A) and 1798.135(c)(2) (effective January 1, 2023); see CPRA Revisions: Consumer Rights). For more on the CPRA's consumer rights submission and response requirements, see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests.

Consumer Rights Request Metrics

The CCPA Regulations require the privacy notice for large businesses to disclose specific metrics on its receipt of and response to verified consumer rights requests (Cal. Code Regs. tit. 11, § 7011(c)(8)). A large business is one that knows or should know that it, alone or jointly, buys, receives, sells, or shares personal information for commercial purposes from more than 10 million consumers in a calendar year (Cal. Code Regs. tit. 11, § 7102). For more on the new metrics requirements, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Metrics for Large Businesses.

Deidentified Patient Information

The CCPA generally excludes deidentified patient information from its coverage scope (Cal. Civ. Code § 1798.146(a)(4)). However, it does prohibit reidentification and requires specific privacy notice disclosures and contract provisions when businesses sell, license, or disclose it (Cal. Civ. Code. §§ 1798.130(a)(5)(D) and 1798.148).

Patient information is deidentified 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);
  - 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).)

If the business sells or discloses deidentified patient information exempt from the CCPA, the privacy policy must include a statement disclosing whether:

- It sells or discloses deidentified patient information.
- 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)).

(Cal. Civ. Code § 1798.130(a)(5)(D).)

For more on deidentified patient information, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Deidentified Patient Information.

CPRA Revisions: Deidentified Patient Information

The CPRA's effect on this deidentified patient information disclosure requirement remains unclear. Because it was not added to the CCPA until September 25, 2020, 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); AB 713 (2019-2020)). The CPRA's provisions prevail over any conflicting legislation enacted after January 1, 2020, however legislation does not conflict if it is consistent with CPRA and furthers its purposes (Section 25(d), CA Prop. 24 (2020)). Assuming that this deidentified patient information notice requirement does not conflict with the CPRA, it remains intact.

CPRA Revisions: New Retention Period Disclosure

The CPRA requires that a business disclose, at or before the point of collection, the length of time it intends to retain each personal information and sensitive personal information category. If providing the exact retention period is not possible, the business may instead describe the criteria it will use to determine how long it plans to retain that personal information or sensitive personal information category. When setting the retention period, the business should remember that the CPRA prohibits it from retaining a consumer's personal information for longer than is reasonably necessary to achieve the disclosed collection and use purposes. (Cal. Civ. Code § 1798.100(a)(3) (effective January 1, 2023).)

Contact Information

The business's privacy policy must tell consumers who to contact if they have questions or concerns about its privacy policies and practices (Cal. Code Regs. tit. 11, § 7011(c)(6)). Privacy policies often list the business's chief privacy officer or data protection officer as the primary contact point.

However, the CCPA Regulations also require the business to use a contact method that reflects how it primarily interacts with consumers (Cal. Code Regs. tit. 11, § 7011(c)(6)). Businesses should consider if or how they may integrate privacy questions or complaints into their regular customer service process.

Presentation Requirements

The CCPA and CCPA Regulations do not establish a required form or format for compliant privacy notices. Rather, they allow each business to adopt a notice format that best fits its activities. However, they do direct businesses to:

- Adopt a form that is reasonably accessible to consumers and easily understood.
- Uses a format that makes the policy readable on smaller screens, if applicable.
- Provide a format that allows consumers to print it out as a single document.

(Cal. Civ. Code §1798.130(a); Cal. Code Regs. tit. 11, § 7011(a)(2)(A) to (E)).

The policy should also meet the CCPA Regulation's language and accessibility requirements applicable to all notices (see Shared Presentation, Location, and Accessibility Requirements).

The business must make its privacy policy available:

- Online through a conspicuous link using the word "privacy" on the business's website homepage, unless it does not operate a website.
- On a mobile app's download or landing pages, and optionally, in the app's settings menu.
- In any California-specific description of consumer's privacy rights.
- Conspicuously to consumers when the business does not operate a website.

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

For general information on privacy notice formats and drafting considerations, see Practice Note, Drafting Privacy Notices: Different Privacy Notice Approaches and Formats.

CPRA Revisions: Presentation Requirements

The CPRA does not substantively change these presentation requirements.

Collection Notice

The CCPA requires a business to disclose, before or at the point of collection, both:

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

(Cal. Civ. Code § 1798.100(b).)

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 CCPA Regulations operationalize these provisions 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). A notice at collection must provide:

- A list of the personal information categories collected (see Personal Information Categories).
- The business or commercial purpose for which the categories of personal information will be used (see Business or Commercial Purpose).
- A link or website address to the business's opt-out right notice, if applicable (see Opt-Out Right Notice).
- A link or website address to the business's privacy policy (Privacy Policy).

(Cal. Code Regs. tit. 11, § 7012(b).)

For a model collection notice, see Standard Document, Notice at Collection (CCPA and CPRA).

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 Practice Note, California Privacy Laws (CCPA and CPRA): Impact on Employers). For a model workforce collection notices, see Standard Documents, CCPA Notice at Collection for California Employees and Applicants and CCPA Notice at Collection for California Independent Contractors.

CPRA Revisions: Collection Notice

The CPRA rephrases and expands the CCPA's collection notice requirements to include:

- The personal information categories the business will collect, including any sensitive personal information categories.
- The purposes for which it collects or uses the personal information and sensitive personal information categories.
- Whether it sells or shares the personal information and sensitive personal information categories.
- The intended retention period for each personal information or sensitive personal information category, 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)).

Presentation Requirements

The business must provide a notice of collection whenever and wherever it collects personal information, including in offline situations such as collecting information from a paper form or by observing a consumer's physical behavior (Cal. Code Regs. tit. 11, § 7012(a)). The CCPA does not allow businesses to collect personal information surreptitiously.

Depending on how and where a business collects personal information, internet-based collection notices on their own may not suffice. The CCPA specifically states that it applies to the collection and sale of **all** personal information collected by a business from customers, not just to electronic or internet collections (Cal. Civ. Code § 1798.175). This includes, for example, personal information collected from consumers using:

- Phone interviews.
- Postal mail.
- Written forms.
- Observations to create an individual profile.

A business should therefore carefully review how it collects personal information to ensure it provides consumers with the appropriate notices.

Businesses must make the notice readily available where the consumers will encounter it at or before the point of collection (Cal. Code Regs. tit. 11, § 7012(a)(3)). While the CCPA Regulations recognize that the best presentation method will depend on how and when the business collects personal information, they do provide specific guidelines for the following common situations:

- Online collections may:
  - post a conspicuous link to the collection notice on each webpage that collects personal information and, on the website's, introductory page; or
  - embed the notice in its online privacy policy **if** the website collection point provides a direct link to the specific section containing the collection notice's required disclosures.
- Mobile applications may provide links to the notice on its download page and on the app's settings menu or similar internal location.
- Mobile applications that collect personal information a consumer would not reasonably expect, such as a flashlight app collecting real-time geolocation

information, must also provide **just-in-time pop-up notices** at the collection point that:

  - summarize the personal information categories collected; and
  - provide a link to the full collection notice.

- Offline collections may:
  - provide the notice directly on printed forms that collect personal information;
  - provide the notice as a separate paper document; or
  - post prominent signs displaying the notice or its online location.
- Telephone or in person conversations collecting personal information may provide the notice orally.

(Cal. Code Regs. tit. 11, § 7012(a)(3) to (4), (c).)

For more on the CCPA Regulation's general presentation and delivery requirements, see Shared Presentation, Location, and Accessibility Requirements.

Exceptions

The notice at collection is separate and independent from the business's privacy policy. However, a business collecting personal information online may provide the collection notice in its privacy policy **if** the website collection point:

- Provides a direct link to that specific privacy policy section.
- The section describes the specific information that the website collects in the manner required for a compliant notice of collection.

(Cal. Code Regs. tit. 11, § 7012(c).)

Businesses that do not collect any consumer personal information directly from consumers are exempt from the collection notice requirement if they either:

- Do not sell 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 the registration submission (see OAG: Data Broker Registration and OAG: Data Broker Registry).

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

CPRA Revisions: Third Party Collection Notices

All businesses covered by the CPRA that control the collection of a consumer's personal information must provide a specific notice before or at the collection point (Cal. Civ. Code § 1798.100(b) (effective January 1, 2023)). Providing these collection notices can prove difficult when the business does not have a direct relationship with the consumer whose information is collected or when the business collects personal information indirectly, such as by observing consumer behavior. Recognizing this tension, the CPRA allows a covered business that acts as a third party when it controls the collection of a consumer's personal information to meet its collection notice obligation by prominently and conspicuously providing the required information on its internet website's homepage (Cal. Civ. Code § 1798.100(b) (effective January 1, 2023)).

However, if that personal information collection occurs on the business's premises, including in a vehicle, the business acting as a third party must also provide the consumer with an additional notice that:

- Occurs:
  - at the collection location;
  - in a clear and conspicuous manner; and
  - at or before the point of collection.
- Informs the consumer about:
  - the personal information categories it will collect;
  - the use purposes for the collected personal information categories; and
  - whether it sells that personal information.

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

Under the CPRA's revised definitions, a business acts as third party when:

- The consumer is not intentionally interacting with the business.
- The business is not:
  - collecting the information as part of the consumer's current interaction with it;
  - a service provider to another business with whom the consumer intentionally interacts and who collects the personal information as part of the consumer's current interaction with that business; or
  - a contractor.

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

For more on service providers, contractors, and third parties under the CPRA, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Definitions for Third Party, Restricted Third Party, and Service Provider.

Opt-Out Right Notice

Consumers who are at least 16 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. To help consumers exercise this right, a business that sells personal information must provide consumers with a specific opt-out right notice that contains:

- A description of the consumer's right to opt-out of personal information sales.
- An interactive form that enables a consumer to submit an opt-out request online using the title "Do Not Sell My Personal Information," 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 §§ 1798.120(b) and 1798.135; Cal. Code Regs. tit. 11, § 7013(c).)

For more on the required opt-out submission methods, see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests: Opt-Out Request Submission Methods.

A business that shares personal information with service providers should also include a statement disclosing that practice to qualify for the CCPA's service provider exception to personal information sales (Cal. Civ. Code § 1798.140(t)(2)(C)(i)). For more on this exception and the difference between sales and business purpose disclosures, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Distinguishing Between Sales and Business Purposes Disclosures and Qualifying for the Service Provider Sales Exception.

Importantly, a business cannot:

- Sell personal information collected when it did not post an opt-out right notice unless it obtains the consumer's affirmative consent.
- Require a consumer to create an account to exercise their opt-out rights.
- Ask a consumer opting out to reauthorize personal information sales for at least 12 months after the request.
- Use personal information collected in an opt-out request for any other purpose.

(Cal. Civ. Code § 1798.135(a)(1), (5) to (6); Cal. Code Regs. tit. 11, § 7013(e)).

For a detailed discussion of the CCPA's sale opt-out right, see Practice Notes, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Sale Opt-Out and Opt-In Rights and Responding to CCPA and CPRA Consumer Rights Requests.

CPRA Revisions: Sharing Opt-Out and Sensitive Personal Information Limitation Right Notices

The CPRA extends all of the CCPA's sales opt-out submission method requirements to the new right to opt out of sharing personal information for cross-context behavioral advertising purposes (Cal. Civ. Code §§ 1798.120(b) and 1798.135(a)(1) (effective January 1, 2023)). It also creates a mirrored series of notice obligations for the consumer's new right to limit a business's use or disclosure of sensitive personal information (Cal. Civ. Code § 1798.135(a)(2) (effective January 1, 2023)).

Under the CPRA, businesses must:

- Change the sales opt-out link's title to "Do Not Sell or Share My Personal Information" and enable consumers to also opt-out of sharing personal information on the linked webpage.
- Provide a second opt-out link titled "Limit the Use of My Sensitive Personal Information" that links to a webpage where consumers or their authorized agents can submit opt-out requests.
- Alternatively, utilize a single, clearly labeled link on its internet homepages if that link easily allows a consumer to exercise all three of their opt-out rights.

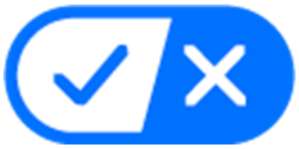
(Cal. Civ. Code § 1798.135(a)(1), (2), (3) (effective January 1, 2023).)

Businesses should expect the California Privacy Protection Agency to issue regulations that further describe what information its CPRA opt-out right notice must provide (Cal. Civ. Code § 1798.185(a)(4)(A), (6), (22); see CPRA Regulation Tracker).

For more on the CPRA's new sales opt-out and sensitive personal information limitation rights, see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests.

Uniform Opt-Out Icon

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 as 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.

Placement and Links

The CCPA expects businesses to post the right to opt-out notice as a publicly available internet webpage (Cal. Civ. Code §1798.135(a)(1)). The opt-out right notice's exact location depends on the business's operation methods. For example, a business that:

- Operates a website should place the notice on the internet webpage where it sends consumers who click on a "Do Not Sell My Personal Information" link.
- Operates a mobile app should place the notice text on its download or landing page or to an internet webpage where it sends consumers who click on a "Do Not Sell My Personal Information" from those locations.
- Provides all the opt-out right notice's required elements, including the interactive submission form, in a single, separate section of its privacy policy may provide direct links to that section.
- Operates a separate homepage dedicated to California consumers and takes reasonable steps to ensure that California consumers are directed to that homepage may place the opt-out right notice text and links there instead of on its general public website.
- Does not operate a website must establish, document, and follow another delivery method that informs consumers of their right to opt-out.

(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)). Examples of offline notices include:

- For personal information collected in a brick-and-mortar store:
  - printing the notice on paper forms that collect the personal information; or
  - posting signs where the business collects personal information directing consumers to the online notice location.
- For personal information collected in telephone calls, providing the notice orally during the phone call.

(Cal. Code Regs. tit. 11, § 7013(b)(3).)

Under the CCPA, a covered business must also:

- Clearly and conspicuously link to the opt-out right notice webpage from either its:
  - public internet homepage; or
  - a California-specific public internet homepage, if it takes reasonable steps to direct all California consumers to that California homepage instead of the general one.
- Include a separate link to the opt-out right notice's webpage in:
  - any online privacy policies; and
  - any California-specific description of consumers' privacy rights.

(Cal. Civ. Code § 1798.135.)

The CCPA broadly defines the term "homepage" to include:

- The introductory page of an internet Web site.
- Any internet webpage that collects personal information.
- In the case of an online service, such as a mobile application:
  - the application's platform page or download page;
  - a link within the application, such as from the application configuration, "About," "Information," or settings page; and

  - any other location that allows consumers to review the opt-out right notice, including, but not limited to, before downloading the application.

(Cal. Civ. Code § 1798.140(l).)

Based on this broad definition of homepage and common technology practices that may cause every page of a website to collect personal information, businesses should consider including the "Do Not Sell My Personal Information" opt-out right notice links as part of its website footer information, so it appears on every webpage.

The opt-out right notice must meet the same general readability and accessibility requirements as the CCPA's other notices (see Shared Presentation, Location, and Accessibility Requirements).

CPRA Revisions: Placement and Links

The CPRA does not substantively change the CCPA's link posting requirements, it just expands them to cover the CPRA's new sharing opt-out and sensitive personal information limitation rights and creates a new exception for consumer-directed preference signals (see CPRA Revisions: Sharing Opt-Out and Sensitive Personal Information Limitation Right Notices and CPRA Revisions: Consumer Preference Signal Exception).

Exceptions

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

- It does not sell personal information.
- Its privacy policy affirmatively states that it does not sell personal information (see Personal Information Sales and Opt-Out Links).

(Cal. Code Regs. tit. 11, § 7013(d).)

The CCPA Regulations also provide a narrow exception for business that exclusively focus on children and do not collect personal information from consumers age 16 or older. Those business can avoid posting the opt-out right notice and "Do Not Sell My Personal Information" links if it both:

- Exclusively and directly targets consumers under 16.
- Only sells personal information with affirmative, opt-in consent.

(Cal. Code Regs. tit. 11, § 7072(b).)

For more on obtaining opt-in consent from minors, see Practice Note, Responding to CCPA and CPRA Consumer Rights Requests: Obtaining Opt-In Consent for Minors.

CPRA Revisions: Consumer Preference Signal Exception

The CPRA provides business with an important alternative to using webpage links that connect to an online submission form. It allows the California Privacy Protection Agency to develop technical specifications for a browser- or platform- based opt-out preference signal system where consumers can directly exercise all three of their opt-out rights (Cal. Civ. Code § 1798.185(a)(19), (20); Cal. Civ. Code § 1798.135(b)(1) (effective January 1, 2023); see CPRA Regulation Tracker). Once established, a business that honors those consumer opt-out preference signals can forgo the webpage opt-out links (Cal. Civ. Code § 1798.135(b)(3) (effective January 1, 2023)).

The California Privacy Protection Agency's technical specification should also include an exception process that allows a business to override the consumer's general opt-out signal if they receive the consumer's informed consent through a web page notice that:

- Makes it as easy to revoke the consent as it is to grant it.
- Does not degrade the consumer's intended browsing experience and has a similar look, feel, and size relative to other links on the same web page.
- Meets all other regulatory requirements.

(Cal. Civ. Code § 1798.135(b)(2) (effective January 1, 2023); see CPRA Regulation Tracker.)

Financial Incentive Notice

The CCPA does not allow businesses to discriminate against consumers who exercise their CCPA rights, such as opting out of personal information sales (Cal. Civ. Code § 1798.125(a)(1)). However, financial incentive offers represent one notable exception to the CCPA's non-discrimination provision. These offers permit businesses to pay or otherwise compensate consumers for the collection, sale, or retention of their personal information if they meet specific requirements, including:

- Notifying consumers of the program's material terms.
- Obtaining consumers' prior opt-in consent.

- Allowing consumers to revoke their participation or consent at any time.

(Cal. Civ. Code § 1798.125(b).)

The financial incentive notice's purpose is to provide consumers with an explanation of the program's material terms that enables them to make informed decisions about participating in the program (Cal. Code Regs. tit. 11, § 7016(a)(1)). To further that purpose, the financial incentive notice must contain:

- A succinct summary of the financial incentive or price or service difference offered (collectively, incentive).
- The incentive's material terms, including the categories of personal information that the incentive may impact and the value of the consumer's data.
- How the consumer can opt-in to the incentive.
- A statement on the consumer's right to withdraw from the incentive at any time, and instructions for exercising that right.
- An explanation of how the incentive reasonably relates to the value of the consumer's data, 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.

(Cal. Code Regs. tit. 11, § 7016(b).)

The business should also consider describing the consequences if the consumer decides not to participate, withdraws their participation, or revokes their consent. It should also include any other material information necessary for a consumer to decide whether to accept the incentive.

An investigation sweep into the customer loyalty programs of several major corporations in the retail, home improvement, travel, and food service industries conducted by the California AG in January 2022 resulted in several CCPA violation 30-day cure notices. The California AG's announcement about the sweep contained important reminders for drafting compliant financial incentive notices, including that:

- Customer loyalty programs that collect personal information and grant gifts, discounts, points, or other loyalty rewards are financial incentives.
- Offline actions can create financial incentives, just as online actions can. For example, in-store data collections for customer loyalty programs, such as when a customer enters their telephone number at a grocery store to receive a discount or a brick-and-mortar store provides free gifts or redeemable points after in-store customer purchases, are financial incentives.
- California businesses operating loyalty programs should 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.)

The CCPA Regulations define:

- A financial incentive as a program, benefit, or other offering related to the collection, deletion, or sale of personal information, including payments to consumers.
- A price or service difference as any difference in:
  - the price or rate charged for any good or service to any consumer related to the collection, retention, or sale of personal information, including through the use of discounts, financial payments, or other benefits or penalties; or
  - the level or quality of any good or service offered to any consumer related to the collection, retention, or sale of personal information, including the denial of goods or services to the consumer.

(Cal. Code Regs. tit. 11, § 7001(j), (o).)

For more on the CCPA's non-discrimination requirements, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Freedom from Discrimination and Establish Financial Incentive and Anti-Discrimination Programs.

CPRA Revisions: Financial Incentive Notice

The CPRA expands the non-discrimination 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)). It also explicitly clarifies that the anti-discrimination right 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)). The CPRA does not otherwise materially change the financial notice's content requirements.

Presentation Requirements

Consumers must encounter the financial incentive notice before opting into the program and the business must use a format that draws the consumer's attention to the notice

(Cal. Code Regs. tit. 11, § 7016(a)(2)(B), (E)). This might require using different fonts or colors, providing it in an offline format, or presenting the notice on a separate sign up page, similar to terms of use.

As with collection notices, a business offering financial incentives online may provide the notice by linking to a specific privacy policy section **if** it provides all of the notice's required content. (Cal. Code Regs. tit. 11, § 7016(a)(2)(E), (3); see Privacy Policy.) For more on the CCPA Regulation's general presentation and delivery requirements, see Shared Presentation, Location, and Accessibility Requirements.

CPRA Revisions: Presentations Requirements

The CPRA adds a clarification that a business must present a financial incentive notice anytime it responds to a consumer's opt-out or limitation request by informing them of a charge to use the business's product or service (Cal. Civ. Code § 1798.135(a)(4) (effective January 1, 2023)).

Enforcement and Sanctions

The CCPA rests primary enforcement authority with the California AG (Cal. Civ. Code § 1798.155). It permits the California AG to file civil actions for injunctive relief and monetary penalties for any violations of the CCPA's provisions, with maximum fines of either:

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

(Cal. Civ. Code § 1798.155(b).)

While unclear, these "per violation" civil penalties likely extend to each affected individual and may result in large aggregate fines. Before initiating an action for a CCPA violation, the California AG must give the offender notice of the alleged violation and at least 30 days to cure it.

The CCPA's consumer private right of action currently only applies to certain data breaches, not to notice violations (see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Private Right of Action for Data Breaches).

CPRA Revisions: Enforcement and Sanctions

The CPRA shifts the primary regulatory and enforcement responsibilities to the new California Privacy Protection Agency, although the California AG remains empowered to investigate and prosecute CPRA violations (Cal. Civ. Code §§ 1798.155(a), 1798.199.45, 1798.199.55, and 1798.199.90(a)). The potential administrative fine or penalty amounts remain unchanged, as does the application of the CPRA's consumer private right of action to certain data breaches and not to consumer notice violations. For more on enforcement under CPRA, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): CPRA Revisions: Enforcement and CPRA Revisions: Private Right of Action for Data Breaches.

Personal Information Category Descriptions

The personal information definition provides a list of 11 personal information categories with examples, highlighting that the examples only qualify as personal information the data meets the underlying criteria for 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 makes clear 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.
- Through an algorithm.

(Cal. Civ. Code § 1798.175.)

CPRA Revisions: New Sensitive Personal Information Categories

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 § 1798.185(a)(19)(C)(iv); Cal. Civ. Code § 1798.121(d) (effective January 1, 2023); see CPRA Regulation Tracker).

California AG Rulemaking Authority for Notices

The California AG's rulemaking responsibilities related to general consumer privacy notices include:

- Addressing changes in technology, data collection practices, obstacles to implementation, and privacy concerns by updating, as needed:
  - the enumerated personal information categories; and
  - unique identifiers definition.
- Establishing rules and procedures for processing and complying with a consumer's personal information sale opt-out request, including a uniform opt-out logo or button.
- Establishing rules, procedures, and any necessary exceptions to ensure that businesses provide all required notices and information, including financial incentive offerings, in a manner:
  - easily understood by the average consumer;
  - accessible to consumers with disabilities; and
  - available in the language primarily used to interact with the consumer.
- Establishing rules and procedures to further the purposes of the CCPA sections establishing a consumer's:
  - right to information when a business collects personal information about the consumer (Cal. Civ. Code § 1798.110);
  - right to information when a business sells the consumer's personal information or discloses it for a business purpose (Cal. Civ. Code § 1798.115); and
  - ability to request and obtain that information (Cal. Civ. Code § 1798.130).

(Cal. Civ. Code § 1798.185(a)(1), (2), (4), (6), (7).)

CPRA Revisions: Rulemaking Authority for Notices

The CPRA transfers rulemaking authority to the California Privacy Protection Agency (Cal. Civ. Code §§ 1798.185(d) and 1798.199.10(a)). It also increases the consumer notice related rulemaking responsibilities to include:

- Further defining and adding to the CPRA's business purpose definition, including describing other notified purposes for which businesses, service providers, and contractors may use consumers' personal information.
- Harmonizing regulations on opt-out mechanisms, consumer notices, and other operational mechanisms to promote clarity and CPRA's functionality.

(Cal. Civ. Code § 1798.185(10), (11), (22).)

For more on the California Privacy Protection Agency's rulemaking authority and progress, see CPRA Regulation Tracker.

CCPA Section-by-Section Notice Requirement Summary

The following chart identifies and summarizes the primary statute sections relating to the CCPA's generalized notice or disclosure requirements. For a chart summarizing all the CCPA's sections, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): CCPA Provision and Regulation Index.

CCPA Section	General Notice or Information Disclosure Summary
Cal. Civ. Code § 1798.100(b)	Must inform consumers, before or at the point of collection: • What personal information categories a business collects. • Its intended use purposes. Prohibits collection of additional personal information categories or using collected personal information for additional purposes without providing this required notice. See also, Enforcement and Sanctions.
Cal. Civ. Code § 1798.105(b)	Must disclose the consumer's deletion right. Cross-references Section 1798.130 for the disclosure requirement.
Cal. Civ. Code § 1798.110(c)	A business that collects personal information about a consumer must disclose: • The personal information categories collected about consumers. • The source categories for the personal information collected. • The business or commercial purposes for collecting or selling personal information. • The categories of third parties with whom the business shares personal information. • That a consumer has the right to request the specific pieces of personal information the business has collected about that consumer (access rights). Cross-references Section 1798.130(a)(5)(B) for the disclosure requirement.
Cal. Civ. Code § 1798.115(c)	A business must separately: • Disclose the personal information categories it sold or include a statement that it has not sold personal information. • Disclose the personal information categories it disclosed for a business purpose or include a statement that it has not disclosed personal information. Cross-references Section 1798.130(a)(5)(C) for the disclosure requirement.
Cal. Civ. Code § 1798.115(d)	A third party cannot resell a consumer's personal information that another business sold to it unless that consumer receives explicit notice and an opportunity to opt-out. Cross-references Section 1798.120 establishing the consumer's personal information sales opt-out and opt-in rights.

CCPA Section	General Notice or Information Disclosure Summary
Cal. Civ. Code § 1798.120(b)	If a business sells personal information to third parties, it must provide notice to consumers that: • It may sell their information. • Consumers have the right to opt-out of these sales. Cross-references Section 1798.135(a) for notice requirements.
Cal. Civ. Code § 1798.125(b)(2), (3)	If a business offers financial incentives for personal information collections, sales, or deletions, it must notify consumers of the financial incentives and clearly describe material terms. Cross-references Section 1798.130 for notice requirements.
Cal. Civ. Code § 1798.130	Primary section discussing both general and specific notice requirements. Cross-references: • Section 1798.100 (statute introduction and general establishment of information rights). • Section 1798.105 (deletion right). • Section 1798.110 (disclosures for business that collects personal information). • Section 1798.115 (disclosures for business that sells personal information or discloses personal information for a business purpose). • Section 1798.125 (non-discrimination rights). Subsections related to general or public disclosures and notices described below.
Cal. Civ. Code § 1798.130(a)(1)	Must make available two or more designated methods for submitting verified consumer requests for information disclosures required under: • Section 1798.110 (disclosures for business that collects personal information). • Section 1798.115 (disclosures for business that sells personal information or discloses personal information for a business purpose). Contact methods must include, at minimum: • Toll-free telephone number. • Website address, if the business maintains an internet website. However, businesses that operate exclusively online with direct consumer relationships only need to provide an email address.

CCPA Section	General Notice or Information Disclosure Summary
Cal. Civ. Code § 1798.130(a)(5)	Must disclose the following information: • A description of the following consumer rights and one or more methods for submitting consumer requests: – Section 1798.100 (disclosures at collection); – Section 1798.105 (deletion right) – Section 1798.110 (disclosures for business that collects personal information); – Section 1798.115 (disclosures for business that sells personal information or discloses personal information for a business purpose); and – Section 1798.125 (non-discrimination rights and financial incentive notices). • A list of the personal information categories the business collected in the preceding 12 months. • A list of the personal information categories the business sold in the preceding 12 months or a statement that no sales took place. • A list of the personal information categories the business disclosed for a business purpose in the preceding 12 months or a statement that no disclosures took place. • If the business sells or discloses deidentified patient information not subject to the CCPA: – whether the business sells or discloses deidentified from patient information; and – whether that patient information was deidentified pursuant to one or more deidentification method commonly known as the HIPAA expert determination method or HIPAA safe harbor method. The personal information lists must use the 11 categories enumerated in the personal information definition in Section 1798.140(o) that most closely describe the personal information. Disclosure must occur: • In the business's online privacy policy, if it exists. • In any California-specific description of consumer's privacy rights, if it exists. • On its internet website, if the business does not maintain an online privacy policy or California-specific description of rights. Must update this information at least once every 12 months.
Cal. Civ. Code § 1798.135	Disclosures and operational requirements for the consumer's sale opt-out and opt-in rights, established in Section 1798.120. Subsections related to general or public disclosures and notices described below.

CCPA Section	General Notice or Information Disclosure Summary
Cal. Civ. Code § 1798.135(a)(1)	If a business sells personal information, it must provide a clear and conspicuous link on the business's internet homepage to a webpage titled "Do Not Sell My Personal Information," that enables the consumer or authorized representative to opt-out of personal information sales, in a form reasonably accessible to consumers. Must not require consumers to create an account to exercise their opt-out rights.
Cal. Civ. Code § 1798.135(a)(2)	If a business sells personal information, it must include a description of the consumer's opt-out/opt-in right under Section 1798.120 and a link to the "Do Not Sell My Personal Information" webpage in: • Any online privacy policies that exist. • Any California-specific description of consumer's privacy rights that exist.
Cal. Civ. Code § 1798.135(b)	Gives businesses the option of providing the "Do Not Sell My Personal Information" notice and links required by this section on a separate and additional California-specific website homepage, instead of the general public homepage, if the business takes reasonable steps to ensure California consumers land on the California homepage instead of the general homepage.
Cal. Civ. Code § 1798.140(d)	Business purpose definition.
Cal. Civ. Code § 1798.140(e)	Collects definition.
Cal. Civ. Code § 1798.140(f)	Commercial purposes definition.
Cal. Civ. Code § 1798.140(i)	Designated methods for submitting requests definition.
Cal. Civ. Code § 1798.140(l)	Homepage definition.
Cal. Civ. Code § 1798.140(o)	Personal information definition, including the 11 enumerated categories.
Cal. Civ. Code § 1798.140(t)	Sales definition.
Cal. Civ. Code § 1798.185	Establishes the California Attorney General's rulemaking authority, including for the CCPA's different notice requirements.
Cal. Code Regs. tit. 11, § 7001(d)	Categories of sources definition
Cal. Code Regs. tit. 11, § 7001(e)	Categories of third parties definition
Cal. Code Regs. tit. 11, § 7001(j)	Financial incentive definition
Cal. Code Regs. tit. 11, § 7001(k)	Household definition
Cal. Code Regs. tit. 11, § 7001(l)	Notice at collection definition
Cal. Code Regs. tit. 11, § 7001(m)	Notice of right to opt-out definition
Cal. Code Regs. tit. 11, § 7001(n)	Notice of financial incentive definition
Cal. Code Regs. tit. 11, § 7001(p)	Price or service definition
Cal. Code Regs. tit. 11, § 7001(p)	Privacy policy definition

CCPA Section	General Notice or Information Disclosure Summary
Cal. Code Regs. tit. 11, § 7001(w)	Value of the consumer's data definition
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, § 7072	Privacy Policy disclosure of personal information sales opt-in process for consumers under 16. The disclosure requirements apply even when the business only targets consumers under 13 or only targets consumers between 13 and 15.

CPRA Section-by-Section Notice Requirement Summary

The following chart identifies and summarizes the primary statute sections relating to the CPRA's generalized notice or disclosure requirements. For a chart summarizing all the CPRA's sections, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): CPRA Provision Index.

CPRA Section	General Notice or Information Disclosure Summary
Cal. Civ. Code § 1798.100(a)	A business that controls the collection of a consumer's personal information must inform consumers, before or at the point of collection: • What personal information categories and, if applicable, sensitive personal information categories the business will collect. • The purposes for collecting and using the disclosed personal information or sensitive personal information categories. • Whether the collected personal information or sensitive personal information is sold or shared. • The intended retention period for each of personal information and sensitive personal information category collected. If the business cannot provide a finite time period, it may disclose the criteria used to determine the retention period. The business cannot select a retention period which lasts longer than what is reasonably necessary for the disclosed collection and use purpose. Without providing the consumer with this required notice, the business cannot: • Collect additional personal information or sensitive personal information categories. • Use collected personal information or sensitive personal information for additional purposes incompatible with the disclosed collection purpose.

CPRA Section	General Notice or Information Disclosure Summary
Cal. Civ. Code § 1798.100(b)	A business that acts as a third party when it controls the collection of personal information about a consumer may meet its Section 1798.100(a) notice obligation by prominently and conspicuously providing the required information on its internet website's homepage. However, if that personal information collection occurs on the business's premises, including in a vehicle, the business acting as a third party must also provide consumers with an additional notice that: • Occurs: – at the collection location; – in a clear and conspicuous manner; and – at or before the point of collection. • Informs consumers about: – the personal information categories it will collect; – the use purposes for the collected personal information categories; and – whether it sells that personal information. A business acts as third party when: • The consumer is not intentionally interacting with it. • It is not collecting the information as part of the consumer's current interaction with the business. • It is not a service provider to another business with whom the consumer intentionally interacts and that collects the personal information as part of the consumer's current interaction with that business. • It is not a contractor. (Cal. Civ. Code § 1798.140(ai) (effective January 1, 2023).)
Cal. Civ. Code § 1798.105(b)	Must disclose the consumer's deletion right. Cross-references Section 1798.130 for the disclosure requirement.
Cal. Civ. Code § 1798.106(b)	Must disclose the consumer's correction right. Cross-references Section 1798.130 for the disclosure requirement.

CPRA Section	General Notice or Information Disclosure Summary
Cal. Civ. Code § 1798.110(b)	Allows a business to meet its request to know consumer response obligation by pointing to its privacy notice if the individualized disclosures required under Section 1798.110(a)(1) to (4) for that consumer exactly match the general privacy notice disclosure required under Section 1798.110(c)(1) to (4).
Cal. Civ. Code § 1798.110(c)	A business that collects personal information about a consumer must disclose: • The personal information categories collected about consumers. • The source categories for the personal information collected. • The business or commercial purposes for collecting, selling, or sharing personal information. • The categories of third parties to whom the business discloses personal information. • That a consumer has the right to request the specific pieces of personal information the business has collected about that consumer (access rights). Cross-references Section 1798.130(a)(5)(B) for the disclosure requirement.
Cal. Civ. Code § 1798.115(c)	A business must separately: • Disclose the personal information categories it sold or shared or include a statement that it has not sold or shared personal information. • Disclose the personal information categories it disclosed for a business purpose or include a statement that it has not disclosed personal information for a business purpose. Cross-references Section 1798.130(a)(5)(C) for the disclosure requirement.
Cal. Civ. Code § 1798.115(d)	A third party cannot resell or reshare a consumer's personal information that another business sold to or shared with it unless that consumer receives explicit notice and an opportunity to opt-out. Cross-references Section 1798.120 establishing the consumer's personal information sales opt-out and opt-in rights.
Cal. Civ. Code § 1798.120(b)	A business that sells or shares personal information to or with third parties must notify consumers that: • It may sell or share their information. • Consumers have the right to opt-out of the sale or sharing of their personal information. Cross-references Section 1798.135(a) for notice requirements.

CPRA Section	General Notice or Information Disclosure Summary
Cal. Civ. Code § 1798.121(a)	A business that uses or discloses sensitive personal information for purposes other than those listed in this section must notify consumers that: • The business may use their sensitive personal information or disclose it to a service provider or contractor for additional, specified purposes. • The consumer has a right to limit the use or disclosure of their sensitive personal information. The section lists the following use or disclosure purposes, which do not require an additional disclosure: • Perform services or provide goods that an average consumer requesting those goods or services would reasonably expect. • Help ensure security and integrity, if that use is reasonably necessary and proportionate. • Perform short-term, transient uses, 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. • Verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business. • Improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business. • Perform other actions that CPRA regulations authorize. Cross-references Section 1798.135(a) for notice requirements and Section 1798.140(e)(2), (4), (5), (8) for listed use and disclosure purposes.
Cal. Civ. Code § 1798.125(b)(2), (3)	A business that offers financial incentives for personal information collections, sales, or deletions must notify consumers about the financial incentives and clearly describe the material terms. Cross-references Section 1798.130 for notice requirements.

CPRA Section	General Notice or Information Disclosure Summary
Cal. Civ. Code § 1798.130	Primary section discussing both general and specific notice requirements. Cross-references: • Section 1798.100 (general business duties). • Section 1798.105 (deletion right). • Section 1798.106 (correction right). • Section 1798.110 (right to know what personal information is being collected and right to access personal information). • Section 1798.115 (right to know what personal information is sold or shared and to whom). • Section 1798.125 (non-discrimination rights). Subsections related to general or public disclosures and notices described below.
Cal. Civ. Code § 1798.130(a)(1)	Must make available two or more designated methods for submitting verified consumer requests for information disclosures required under: • Section 1798.105 (deletion right). • Section 1798.106 (correction right). • Section 1798.110 (right to know what personal information is being collected and right to access personal information). • Section 1798.115 (right to know what personal information is sold or shared and to whom). Contact methods must include, at minimum: • Toll-free telephone number. • Website address, if the business maintains an internet website. However, businesses that operate exclusively online with direct consumer relationships only need to provide an email address.
Cal. Civ. Code § 1798.130(a)(5)	Must disclose the following information: • A description of the following consumer rights: – Section 1798.100 (disclosures at collection); – Section 1798.105 (deletion right) – Section 1798.106 (correction right). – Section 1798.110 (right to know what personal information is being collected and right to access personal information); – Section 1798.115 (right to know what personal information is sold or shared and to whom); and – Section 1798.125 (non-discrimination rights and financial incentive notices).

CPRA Section	General Notice or Information Disclosure Summary
	• Two or more methods for submitting consumer rights requests unless the businesses only needs to provide an email address because it operates exclusively online with direct consumer relationships. • A list of the personal information categories the business collected in the preceding 12 months. • The source categories for the personal information collected. • The business or commercial purposes for collecting, selling, or sharing personal information. • The categories of third parties to whom the business discloses personal information. • A list of the personal information categories the business sold or shared in the preceding 12 months or a prominent statement that no sales or sharing took place. • A list of the personal information categories the business disclosed for a business purpose in the preceding 12 months or a statement that no disclosures took place. The personal information lists must use the category that most closely describes the personal information, following the specific terms for those categories that appear in the CPRA's personal information and sensitive information definitions in Sections 1798.140(v)(A) to (K) and 1798.140(ae)(1) to (9). Disclosure must occur: • In the business's online privacy policy, if it exists. • In any California-specific description of consumer's privacy rights, if it exists. • On its internet website, if the business does not maintain an online privacy policy or California-specific description of rights. Must update this information at least once every 12 months. CCPA amendments enacted after January 1, 2020 but before the CPRA's approval also required the privacy notice to disclose: • Whether the business sells or discloses deidentified from patient information. • If it does, whether that patient information was deidentified pursuant to one or more deidentification method commonly known as the HIPAA expert determination method or HIPAA safe harbor method. However, CPRA may overwrite this disclosure requirement because the corresponding CPRA section approved by the voters did not contain new language (Cal. Civ. Code § 1798.130(a)(5)(D); Cal. Civ. Code § 1798.130(a)(5) (effective January 1, 2023)). 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)).

CPRA Section	General Notice or Information Disclosure Summary
Cal. Civ. Code § 1798.135	Disclosures and operational requirements for the consumer's sale and sharing opt-out and opt-in rights, established in Section 1798.120, and sensitive personal use and sharing limitation rights, established in Section 1798.121. Subsections related to general or public disclosures and notices described below.
Cal. Civ. Code § 1798.135(a)(1))	If a business sells or personal information, it must provide a clear and conspicuous link on the business's internet homepage to a webpage titled "Do Not Sell or Share My Personal Information," that enables the consumer or authorized representative to opt-out of personal information sales, in a form reasonably accessible to consumers.
Cal. Civ. Code § 1798.135(a)(2)	If a business uses or discloses consumers' sensitive personal information for purposes other than those authorized in Section 1798.121(a), it must provide a clear and conspicuous link on the business's internet homepage to a webpage titled "Limit the Use of My Personal Information," that enables the consumer or authorized representative to limit personal information use and disclosure to just the authorized purposes.
Cal. Civ. Code § 1798.135(a)(3)	Allows a business to use a single, clearly labeled link on the business's internet homepage instead of the separate links that Section 1798.135(a)(1), (2) require, if the link easily allows the consumer to opt out of sales, opt out of sharing, and limit sensitive personal information use and disclosure.
Cal. Civ. Code § 1798.135(a)(4)	Requires the business to provide a financial incentive notice if it response to an opt-out or limitation request by informing the consumer of a charge to use any product or service.
Cal. Civ. Code § 1798.135(b)	Establishes an option to use consumer-driven opt-out preference signals instead of website links and notices, once further regulations establish a technical specification.
Cal. Civ. Code § 1798.135(c)(2)	A business that sells or shares personal information, or uses sensitive personal information for purposes other than what Section 1798.121(a) lists, must include a description of the consumer's opt-out/opt-in/limitation rights and links to the webpage or webpages where consumers can exercise them in: • Any online privacy policies that exist. • Any California-specific description of consumer's privacy rights that exist.
Cal. Civ. Code § 1798.135(d)	Gives businesses the option of providing the "Do Not Sell My Personal Information" notice and links required by this section on a separate and additional California-specific website homepage, instead of the general public homepage, if the business takes reasonable steps to ensure California consumers land on the California homepage instead of the general homepage.

CPRA Section	General Notice or Information Disclosure Summary
Cal. Civ. Code § 1798.140(a)	Advertising and marketing definition.
Cal. Civ. Code § 1798.140(e)	Business purpose definition.
Cal. Civ. Code § 1798.140(f)	Collects definition.
Cal. Civ. Code § 1798.140(g)	Commercial purposes definition.
Cal. Civ. Code § 1798.140(k)	Cross-context behavioral advertising
Cal. Civ. Code § 1798.140(l)	Dark pattern definition.
Cal. Civ. Code § 1798.140(n)	Designated methods for submitting requests definition.
Cal. Civ. Code § 1798.140(l)	Homepage definition.
Cal. Civ. Code § 1798.140(s)	Intentionally interacts definition.
Cal. Civ. Code § 1798.140(v)	Personal information definition, including the 11 enumerated categories.
Cal. Civ. Code § 1798.140(w)	Precise geolocation definition.
Cal. Civ. Code § 1798.140(z)	Profiling definition.
Cal. Civ. Code § 1798.140(ad)	Sales definition.
Cal. Civ. Code § 1798.140(ae)	Sensitive personal information definition.
Cal. Civ. Code § 1798.140(ah)	Shares definition.
Cal. Civ. Code § 1798.185	Establishes the California Privacy Protection Agency's rulemaking authority, including for the CCPA and CPRA's different notice requirements.