

## CCPA Privacy Policy for California Residents

by Practical Law Data Privacy & Cybersecurity, with Kenneth K. Dort, Drinker Biddle & Reath LLP

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

This document is published by Practical Law and can be found at: [us.practicallaw.tr.com/w-017-8754](https://us.practicallaw.tr.com/w-017-8754)

Request a free trial and demonstration at: [us.practicallaw.tr.com/practical-law](https://us.practicallaw.tr.com/practical-law)

A model website privacy policy or supplemental privacy policy for use by organizations that collect, store, use, share, sell, or disclose the personal information of California residents. This California-specific notice addresses requirements from the California Consumer Privacy Act of 2018 (CCPA) and other California privacy laws. This Standard Document has integrated notes with important explanations and drafting tips.

**Note:** On November 3, 2020, California voters approved the California Privacy Rights Act of 2020 (Proposition 24) (CPRA), which will amend and expand the CCPA on January 1, 2023. The CCPA remains in effect until the CPRA's operative date. For more on the CPRA's privacy notice changes, see [Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies](#). For more on the CPRA generally, see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\)](#) and [CPRA Regulation Tracker](#).

### DRAFTING NOTE: READ THIS BEFORE USING DOCUMENT

This Standard Document provides a California-specific privacy policy containing various disclosures required by the California Consumer Privacy Act of 2018 (CCPA) and the CCPA Regulations (Cal. Civ. Code §§ 1798.100 to 1798.199.95; Cal. Code Regs. tit. 11, §§ 7000 to 7102) (see [Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies: Privacy Policy](#)).

The CCPA grants consumers, defined as California residents, specific rights regarding their personal information, including information, deletion, and sales prevention rights (see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Consumer Rights](#)). Several different CCPA sections require businesses to make affirmative disclosures to consumers in privacy policies or other notices (see [Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies: CCPA Section-by-Section Notice Requirement Summary](#)).

The CCPA Regulations separate the CCPA's disparate notice requirements into four different notice types:

- A notice at collection.
- A privacy policy.
- A notice of right to opt out.
- A notice of financial incentive.

(Cal. Code Regs. tit. 11, §§ 7001(l), (m), (n), (p), and 7010.)

This Standard Document provides the CCPA privacy policy (Cal. Code Regs. tit. 11, §§ 7001(p) and 7011). A CCPA privacy policy differs from a notice at collection because it provides broader, comprehensive disclosures about the business's general practices rather than a specific disclosure tailored to the particular collection activities (Cal. Code Regs. tit. 11, §§ 7001(l) and 7012).

For more on the CCPA's different notice types, see [Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies](#).

Amended several times since its initial passage, the CCPA went into effect January 1, 2020 and regulatory enforcement began on July 1, 2020. On November 3, 2020, California voters approved a ballot initiative that will amend and expand the CCPA, the California Privacy Rights Act of 2020 (CPRA). Most of the CPRA's substantive CCPA amendments do not take effect until January 1, 2023, so businesses should continue to follow the CCPA and CCPA Regulations while they prepare for the CPRA's new requirements. For more on the CPRA, the CCPA, and their history, see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\)](#) and [Box, History of the CCPA and CPRA](#).

Regulations developed by the California Attorney General (California AG) implementing the CCPA became effective on August 14, 2020 and were amended on March 15, 2021 (Cal. Code Regs. tit. 11, §§ 7000 to 7102). The process of preparing implementing regulations for the CPRA is ongoing. For more on the regulations' progress, including possible revisions to the current CCPA Regulations, see [CPRA Regulation Tracker](#).

Given its expansiveness and broad reach, the CCPA is likely to significantly impact entities both inside and outside California that collect and process California residents' personal information. For a broader discussion of the CCPA, including which business must comply with it, see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\)](#). For the full list of CCPA resources, see [California Privacy Toolkit \(CCPA and CPRA\)](#).

### CCPA Privacy Policy Requirements

The CCPA privacy policy is a business's comprehensive statement 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), 7010(a), 7011(a)(1)). The CCPA and CCPA Regulations organize the required privacy policy disclosures as follows:

- **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 [Right to Know and Data Portability](#));
  - instructions for submitting a verifiable consumer request to know and links to any online request form or portal provided to make those requests (see [Exercising Your Rights to Know or Delete](#));
  - a general description of the business's process for verifying consumer requests, including any information the consumer must provide (see [Exercising Your Rights to Know or Delete](#));
  - the personal information categories collected about consumers in the preceding 12 months (see [Information We Collect](#));
  - the categories of sources from which the business collected personal information (see [Information We Collect](#));
  - the business or commercial purpose for collecting or selling personal information (see [Use of Personal Information](#));
  - a statement on personal information disclosures for a business purpose (see [Sharing Personal Information](#)); and
  - a statement on personal information sales disclosures (see [Sharing Personal Information](#)).
- **Right to deletion** disclosures, including an explanation of the right, submission instructions, and the verification process (see [Right to Delete and Exercising Your Rights to Know or Delete](#)).
- **Right to opt-out disclosures**, including an explanation of the right, statements about sales, submission instructions, and the verification process (see [Personal Information Sales Opt-Out and Opt-In Rights and Sharing Personal Information](#)).
- **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 [Non-Discrimination](#)).
- **Authorized agent disclosure**, describing how agents can make CCPA-related requests on the consumer's behalf (see [Exercising Your Rights to Know or Delete and Personal Information Sales Opt-Out and Opt-In Rights](#)).

- **Statistical metrics** on the business's response to consumer rights requests, if the business meets certain disclosure thresholds (see [CCPA 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 elements differs from the approach that many US-based privacy policies currently take, which typically present each of these elements in a different order (see, for example, [Standard Document, Website Privacy Policy](#)).

The California AG specifically notes that the CCPA Regulations provided the elements list to help clarify the privacy policy's 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.

To maintain consistency with other privacy policies, this Standard Document provides the CCPA Regulations' required elements within the prior organizational structure.

For a full overview of the CCPA's requirements, see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\)](#). For more on the CCPA's notice requirements, see [Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies](#).

For more on drafting privacy policies in general, see [Practice Note, Drafting Privacy Notices](#) and [Drafting a Privacy Notice Checklist](#).

### Regular Review Required

The businesses must review and update its CCPA privacy policy's content at least every 12 months

(Cal. Civ. Code § 1798.130(a)(5)). The business should also establish practices and procedures to ensure legal counsel learns when activities requiring a notice revision occur, such as:

- Collecting, disclosing, or selling new or different categories of personal information.
- Disclosing or selling personal information to new or different categories of third parties.
- Using, disclosing, or selling personal information for new or different purposes.
- Selling personal information for the first time.

### Policy Presentation and Format

The CCPA does not establish a required form or format for compliant privacy policies. Rather, it allows each business to adopt a notice format that best fits its activities. However, it does direct covered businesses to:

- Adopt a format that is reasonably accessible to consumers.
- Make the required disclosures in either:
  - an online privacy policy, if the business has one;
  - in any California-specific description of consumer privacy rights, if provided; or
  - on its internet website, if the business does not maintain an online privacy policy or California-specific rights description.

(Cal. Civ. Code § 1798.130(a)(5); Cal. Code Regs. tit. 11, § 7011(a)(2), (b).)

The business must also make its CCPA privacy policy available in a printable format and conspicuously use the word "privacy" in online links (Cal. Code Regs. tit. 11, § 7011(a)(2)(E), (b)). The CCPA Regulations clarify that businesses without an internet website must make the privacy policy conspicuously available to consumers (Cal. Code Regs. tit. 11, § 7011(b)).

The CCPA Regulations also set out general privacy policy presentation requirements that apply to all CCPA notices. They require the business to design and present the notice information in a way that is understandable and easy for a consumer to read, including:

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

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

For more on the CCPA's privacy policy's format and location requirements, see [Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies: Presentation Requirements](#).

### Assumptions

This privacy policy for California residents assumes that:

- The CCPA applies to the business.
- The business shares personal information with entities that qualify as service providers or restricted third parties under the CCPA (see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Service Providers and Third Parties](#)).

- The business maintains a general privacy policy that links to/from this California-specific notice, such as [Standard Document, Website Privacy Policy](#).

### Other Considerations

To ensure the California-specific privacy policy accurately reflects the business's current and anticipated personal information uses and practices, ensure its review before publication by:

- Senior management.
- Business and technical employees responsible for operating the site and responding to CCPA rights requests.
- Operating units responsible for controlling access to and use of personal information collected from the site.
- Legal counsel.

The business should periodically audit compliance with the California-specific privacy policy. It should also periodically verify compliance with the outlined practices, particularly any choices and methods given to consumers for exercising their CCPA rights (for example, to opt-out of personal information sales). Failing to implement effective procedures and technology to comply with user opt-out requests exposes the business to potential liability.

### Bracketed Items

Complete bracketed items in ALL CAPS with the specific and relevant facts. Bracketed items in sentence case are either optional provisions or include alternative language choices that the drafting party should select, add, or delete in its discretion.

#### [COMPANY] Privacy Policy for California Residents

**Effective Date:** [DATE]

**Last [Updated/Reviewed] on:** [DATE]

This **Privacy Policy for California Residents** supplements the information contained in [COMPANY]'s [HYPERLINKED URL TO GENERAL PRIVACY POLICY] and applies solely to all visitors, users, and others who reside in the State of California ("consumers" or "you"). We adopt this notice to comply with the California Consumer Privacy Act of 2018 (CCPA) and any terms defined in the CCPA have the same meaning when used in this Policy.

[This Policy does not apply to workforce-related personal information collected from California-based employees, job applicants, contractors, or similar individuals (see [HYPERLINKED URL TO CALIFORNIA EMPLOYEE PRIVACY POLICY]).]

[Where noted in this Policy, the CCPA temporarily exempts personal information reflecting a written or verbal business-to-business communication ("**B2B personal information**") from some of its requirements.]

### DRAFTING NOTE: INTRODUCTION

#### Effective or Revision Date

The policy should identify the date it was last updated and optionally, the date it was last reviewed (Cal. Code Regs. tit. 11, § 7011(c)(7)).

The CCPA requires the business to review and update the privacy policy's content at least every 12 months (Cal. Civ. Code § 1798.130(a)(5)). If the annual review does not cause the business to change or alter the policy, it should use the alternate "last reviewed" language. This confirms that the required annual review took place but did not lead to changes requiring a new effective date.

#### Temporary Exclusions for Workforce and B2B Personal Information

The 2019 CCPA Amendments and the CPRA grant covered businesses temporary relief (until at least January 1, 2023) from most of the CCPA's requirements for certain:

- Workforce-related personal information.
- Personal information reflecting written or verbal business-to-business (B2B) communications or transactions.

(Cal. Civ. Code § 1798.145(h), (n); see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Temporary Exemptions.](#))

This section contains optional language for businesses that want to take advantage of these temporary exclusions and carve out coverage of them from the general privacy policy.

Importantly, the temporary employment-related exception still requires employers to provide the narrower notice at collection (Cal. Civ. Code §§ 1798.100(b) and 1798.145(h)(3); Cal. Code Regs. tit. 11, § 7012(f) to (g); see [Standard Document, CCPA Notice at Collection for California Employees and Applicants](#)). Businesses removing employment-related information from the notice's scope should provide a separate, tailored notice.

The B2B exception is also narrow in scope and does not apply to the personal information sales opt-out right. Businesses may find it difficult in practice to separate out which personal information collected from a business customer's employee qualifies.

For more on these temporary exceptions, see [Practice Note, California Privacy Laws \(CCPA and CPRA\): Impact on Employers.](#)

#### Information We Collect

[Our Website collects/We collect] information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer, household, or device ("**personal information**"). Personal information does not include:

- Publicly available information from government records.
- Deidentified or aggregated consumer information.
- [Information excluded from the CCPA's scope, like:

## CCPA Privacy Policy for California Residents

- health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA), clinical trial data, or other qualifying research data;
- personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver’s Privacy Protection Act of 1994.]

### DRAFTING NOTE: PERSONAL INFORMATION DEFINITION AND EXCEPTIONS

The notice’s personal information definition follows the broad language used by the CCPA (Cal. Civ. Code §§ 1798.140(o); see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Personal Information](#)). The CCPA also excludes certain categories of information from its personal information definition or coverage scope, including:

- Publicly available information from government records.
- Deidentified or aggregate consumer information.
- Certain personal information protected by other sector-specific federal or California statutes.

(Cal. Civ. Code §§ 1798.140(o)(2)–(3) and 1798.145(a)(5), (c)–(f).)

The CCPA provides specific definitions for what qualifies as “aggregate consumer information,” “deidentified” data, including deidentified patient data, and “publicly available” government records (Cal. Civ. Code §§ 1798.140 (a), (h), (o)(2) and 1798.146(a)(4)(A); see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Deidentified or Aggregated Consumer Information and Publicly Available Government Records](#)).

The sector based CCPA exceptions are very specific and limited. Businesses should carefully review their applicability before deciding to exclude those types of personal information from its policy definition (Cal. Civ. Code §§ 1798.145(c)–(f) and 1798.146; see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Preemption](#)).

For other statutes, including the California Online Privacy Protection Act (CalOPPA) and California Data Protection Act (CDPA), the CCPA resolves conflicts by allowing the law that affords the greatest privacy protections to control (Cal. Civ. Code § 1798.175; see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Conflict of Laws and Statutory Interpretation](#)). However, the CCPA also states that its obligations do not restrict a business’s ability to comply with other federal, state, or local laws, law enforcement requests, the defense or exercise of other legal claims, or to maintain an evidentiary privilege (Cal. Civ. Code § 1798.145(a)(1)–(4), (b)).

For more on these exclusions, see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Coverage Exceptions and Extraterritorial Application](#).

In particular, [our Website has/we have] collected the following categories of personal information from consumers within the last twelve (12) months:

Category	Examples	Collected
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver’s license number, passport number, or other similar identifiers.	[YES/NO]

## CCPA Privacy Policy for California Residents

Category	Examples	Collected
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.  Some personal information included in this category may overlap with other categories.	[YES/NO]
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	[YES/NO]
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	[YES/NO]
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to 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.	[YES/NO]
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	[YES/NO]
G. Geolocation data.	Physical location or movements.	[YES/NO]
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	[YES/NO]
I. Professional or employment-related information.	Current or past job history or performance evaluations.	[YES/NO]
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	[YES/NO]
K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	[YES/NO]

### DRAFTING NOTE: PERSONAL INFORMATION CATEGORIES

When disclosing the personal information categories that the business collects about consumers, the CCPA expects the privacy policy to reference and use the 11 categories listed in its personal information definition that most closely describe the personal information collected (Cal. Civ. Code §§ 1798.110(c)(1) and 1798.130(c)). Placing those categories in a chart, where the business affirmatively states whether it has or has not collected that type of personal information provides the required information in a clear, easy-to-understand format. It also helps the business comply with the requirement to produce individualized lists by category on request (see [Practice Note, Understanding](#)

[the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Individual Right to Know](#)). A business should carefully review and categorize the personal information it collects to complete the chart.

For more on the CCPA's personal information definition, see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Personal Information](#). For more on describing personal information categories, see [Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies: Personal Information Categories](#).

[Our Website obtains/We obtain] the categories of personal information listed above from the following categories of sources:

- [Directly from you. For example, from forms you complete or products and services you purchase.]
- [Indirectly from you. For example, from observing your actions on our Website.]
- [[OTHER SOURCE CATEGORY].]

### DRAFTING NOTE: SOURCE CATEGORY IDENTIFICATION

The CCPA requires the business to identify the categories of sources from which it collects personal information (Cal. Civ. Code §§ 1798.110(c)(2)). While CCPA does not elaborate on or provide examples of the source categories a business should use, the CCPA Regulations define "category of sources" as the types or groups of people or entities:

- From which a business collects personal information about consumers.
- Described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity.
- That may include:
  - the consumer directly;
  - advertising networks;
  - internet service providers;

- data analytic providers;
- government entities;
- operating systems and platforms;
- social networks; or
- data brokers.

(Cal. Code Regs. tit. 11, § 7001(d)).

The business should:

- Carefully review its personal information data flows to provide clear and accurate disclosures.
- Describe the categories with enough detail to provide clear and meaningful disclosures about where acquired personal information originates.

For more on describing source categories, see [Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies: Personal Information Sources](#).



### Use of Personal Information

We may use, [sell,] or disclose the personal information we collect for one or more of the following purposes:

- To fulfill or meet the reason you provided the information. For example, if you share your name and contact information to request a price quote or ask a question about our products or services, we will use that personal information to respond to your inquiry. If you provide your personal information to purchase a product or service, we will use that information to process your payment and facilitate delivery. We may also save your information to facilitate new product orders or process returns.
- [To provide, support, personalize, and develop our Website, products, and services.]
- [To create, maintain, customize, and secure your account with us.]
- [To process your requests, purchases, transactions, and payments and prevent transactional fraud.]
- [To provide you with support and to respond to your inquiries, including to investigate and address your concerns and monitor and improve our responses.]
- [To personalize your Website experience and to deliver content and product and service offerings relevant to your interests, including targeted offers and ads through our Website, third-party sites, and via email or text message (with your consent, where required by law).]
- [To help maintain the safety, security, and integrity of our Website, products and services, databases and other technology assets, and business.]
- [For testing, research, analysis, and product development, including to develop and improve our Website, products, and services.]
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- As described to you when collecting your personal information or as otherwise set forth in the CCPA.
- **[[OTHER PURPOSES].]**
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by us about our [Website users/consumers] is among the assets transferred.

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

### **DRAFTING NOTE: USE OF PERSONAL INFORMATION**

The business's CCPA privacy policy must identify its 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)). The policy must describe the use purposes in a manner that provides consumers with a meaningful understanding of why the business collects or sells personal information (Cal. Code Regs. tit. 11, § 7011(c)(1)(F)).

This section provides optional clauses describing several common commercial or business purposes for using personal information. However, the business

should carefully review how and why it uses the personal information it collects to provide clear and accurate disclosures.

To increase transparency, the business may consider tying the listed use purposes back to each personal information category (see Drafting Note, Personal Information Categories).

The CCPA's purpose limitation clause prohibits using collected personal information for purposes not listed in the privacy policy or uses unrelated to those purposes (Cal. Civ. Code § 1798.100(b)). Therefore,

the business should ensure that the provided list comprehensively describes both current and reasonably anticipated use cases.

### Commercial Purpose and Business Purpose Definitions

While the CCPA's Section 1798.100(b) notice requirement requires disclosure of all use purposes, other CCPA sections, like Section 1798.110(c), separate out the use purpose concept into the defined terms of commercial purposes or business purposes.

The CCPA broadly defines commercial purposes as uses that advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. Importantly, the commercial purpose definition explicitly excludes uses with the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism. (Cal. Civ. Code § 1798.140(f).)

However, the CCPA strictly defines the business purpose term to mean uses that are reasonably necessary and proportionate to achieve either:

- The business's operational or notified purpose for collecting the personal information.
- Purposes compatible with the context in which the business collected the information.

(Cal. Civ. Code § 1798.140(d).)

The definition goes on to identify the following seven specific types of permitted business purposes:

- Performing services on behalf of a CCPA-covered business or its service provider, such as customer service, order fulfillment, payment processing, financing, and advertising, marketing, or analytic services.
- Auditing the interaction with the consumer and concurrent transactions, including counting ad impressions and verifying quality of ad impressions.
- Detecting or preventing security incidents or other illegal activity and prosecuting the responsible parties.

- Debugging.
- Verifying or maintaining quality or safety or improving or upgrading a service or device owned, manufactured, or controlled by or for the business.
- Short-term, transient use if the personal information is not:
  - disclosed to another third party; or
  - used to build a profile or otherwise alter an individual consumer's experience outside the current interaction.
- Undertaking internal research for technological development and demonstration.

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

While those listed activities clearly qualify as business purposes under the statute, it is unclear whether the list merely provides examples of business purposes or restricts the term to just those activities. This ambiguity is one of many generated by the CCPA's hasty adoption and inconsistent phrasing (see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): History of the CCPA and CPRA](#)). The CCPA Regulations do not directly address this ambiguity. However, California AG comments on the CCPA Regulations discuss the business purpose definition in the broader context and do not indicate an intention to limit the term to just the seven listed items (see [CCPA ISOR](#) at 21 to 23).

These Standard Clauses follow a statutory interpretation that does not limit business purposes to the seven listed items because:

- The language introducing the list does not indicate those are the only permitted purposes.
- Allowing the term to include other qualifying operational or notified purposes gives meaning to both sentences in business purpose definition.

However, businesses taking a conservative approach may choose to separate out their CCPA business purposes from the other commercial purposes that the notice discloses.

For more on the CCPA's business purpose definition, see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Business Purposes](#).

## CCPA Privacy Policy for California Residents

### Sharing Personal Information

We may share your personal information by disclosing it to a third party for a business purpose. We only make these business purpose disclosures under written contracts that describe the purposes, require the recipient to keep the personal information confidential, and prohibit using the disclosed information for any purpose except performing the contract. In the preceding twelve (12) months, Company [has/ has not] disclosed personal information for a business purpose[ to the categories of third parties indicated in the chart below].

[We do not sell personal information./We may also share your personal information by selling it to third parties, subject to your right to opt-out of those sales. Our personal information sales [do/do not] include information about individuals we know are under age 16.] In the preceding twelve (12) months, Company [has not sold/has sold the following categories of] personal information[ to the categories of third parties indicated in the chart below]. For more on your personal information sale rights, see Personal Information Sales Opt-Out and Opt-In Rights.

Personal Information Category	Category of Third-Party Recipients	
	Business Purpose Disclosures	Sales
A: Identifiers.	[None/[THIRD-PARTY CATEGORIES]]	[None/[THIRD-PARTY CATEGORIES]]
B: California Customer Records personal information categories.	[None/[THIRD-PARTY CATEGORIES]]	[None/[THIRD-PARTY CATEGORIES]]
C: Protected classification characteristics under California or federal law.	[None/[THIRD-PARTY CATEGORIES]]	[None/[THIRD-PARTY CATEGORIES]]
D: Commercial information.	[None/[THIRD-PARTY CATEGORIES]]	[None/[THIRD-PARTY CATEGORIES]]
E: Biometric information.	[None/[THIRD-PARTY CATEGORIES]]	[None/[THIRD-PARTY CATEGORIES]]
F: Internet or other similar network activity.	[None/[THIRD-PARTY CATEGORIES]]	[None/[THIRD-PARTY CATEGORIES]]
G: Geolocation data.	[None/[THIRD-PARTY CATEGORIES]]	[None/[THIRD-PARTY CATEGORIES]]
H: Sensory data.	[None/[THIRD-PARTY CATEGORIES]]	[None/[THIRD-PARTY CATEGORIES]]
I: Professional or employment-related information.	[None/[THIRD-PARTY CATEGORIES]]	[None/[THIRD-PARTY CATEGORIES]]
J: Non-public education information.	[None/[THIRD-PARTY CATEGORIES]]	[None/[THIRD-PARTY CATEGORIES]]
K: Inferences drawn from other personal information.	[None/[THIRD-PARTY CATEGORIES]]	[None/[THIRD-PARTY CATEGORIES]]

### DRAFTING NOTE: SHARING PERSONAL INFORMATION

A business's privacy policy must disclose the categories of third parties with whom it shares personal information (Cal. Civ. Code § 1798.110(c)(4); Cal. Code Regs. tit. 11, §7011(c)(1)(G)). The concept

of sharing includes any disclosure of personal information and does not require a sale. Whenever a business shares personal information with a third party, it should determine if that action resulted in a:

- Disclosure for a business purpose (see Drafting Note, Business Purpose Disclosures).
- Sale (Drafting Note, Sales of Personal Information).

To understand when sharing personal information constitutes a sale or 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](#).

The privacy policy must contain different disclosures for each type of sharing. While there are several ways a business could present these different disclosures, this policy presents them in a matrix-type chart, where the business separately identifies sales and business purpose disclosures for each personal information category. For more on other formatting options, see [Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies: Personal Information Sales and Opt-Out Links](#).

### Business Purpose Disclosures

The CCPA privacy policy must provide a statement on personal information disclosures made for a business purpose during the preceding 12 months that either:

- States that no disclosures occurred.
- Provides:
  - the personal information categories disclosed, using the 11 categories listed in the personal information definition that most closely describe the personal information (see Drafting Note, Personal Information Categories); and
  - for each personal information category, the categories of third parties that received those disclosures (see Drafting Note, Categories of Third Parties).

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

The business should carefully review the types of personal information it discloses for a business purpose and fill out the chart by selecting the correct alternate clauses. For more on what activities meet the business purposes definition, see Drafting Note, Commercial Purpose and Business Purpose

Definitions and [Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies: Personal Information Disclosures for a Business Purpose](#).

### Sales of Personal Information

A business that sells personal information must notify consumers about those potential sales and their right to opt-out of them (Cal. Civ. Code §§ 1798.120(b)).

The privacy policy 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 16 years of age.
- Inform consumers about their personal information sales restriction rights (see Personal Information Sales Opt-Out and Opt-In Rights).
- Provide the business's opt-out right notice content or a link to its location (see Personal Information Sales Opt-Out and Opt-In Rights).
- 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 Drafting Note, Personal Information Categories); and
  - provide, for each personal information category identified, the categories of third parties to whom personal information was sold (see Drafting Note, Categories of Third Parties).

(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).)

Businesses that sell personal information should select the alternate language accurately disclosing those sales. The business should also carefully review the types of personal information it sold and fill out the chart by selecting the correct alternate clauses. For more, see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Personal Information Sales](#).

### Categories of Third Parties

The CCPA Regulations define categories of third parties as the types or groups of third parties with whom the business shares personal information (Cal. Code Regs. tit. 11, § 7001(e); see [CCPA FSOR](#) at 2, [CCPA ISOR](#) at 4).

The business should describe the recipient categories with enough detail to provide clear and meaningful disclosures about the type of recipients that receive personal information from the business. Category examples provided in the draft CCPA Regulations include.

- Advertising networks.
- Internet service providers.
- Data analytic providers.
- Government entities.

- Operating systems and platforms.
- Social networks.
- Data brokers or aggregators.

(Cal. Code Regs. tit. 11, § 7001(e).)

Other third-party category types may include:

- Service providers.
- Affiliates.
- Partners.
- Parent or subsidiary organizations.
- Internet cookie data recipients, like Google Analytics.

The business should carefully review its personal information data flows to provide clear and accurate disclosures.

### **[Reselling Personal Information]**

[The CCPA prohibits a third party from reselling personal information unless you have received explicit notice and an opportunity to opt-out of further sales. The following businesses purchase personal information from us and may resell that information. To opt-out of those sales, please [visit that business's opt-out notice at link provided below/[OTHER INSTRUCTIONS]].

- [COMPANY NAME]: [OPT-OUT LINK OR INSTRUCTION].]

### **DRAFTING NOTE: RESELLING PERSONAL INFORMATION**

The CCPA restricts third-party sale recipients from reselling that personal information unless the consumer receives explicit notice of the potential resale and an opportunity to opt-out (Cal. Civ. Code § 1798.115(d)).

The CCPA and CCPA Regulations do not define explicit notice or set specific requirements for providing explicit notice of personal information resales. This optional section may help businesses meet that requirement by:

- Explicitly identifying the third parties that may resell personal information purchased from the business.

- Providing a direct link to the third party's personal information sales opt-out notice.

While it remains unclear whether a privacy policy disclosure alone can provide consumers with explicit notice, a business that want to help its customers meet this reseller requirement should consider including this optional section.

Third-party resellers may also need to register in California as a data broker (see [Practice Note, California Privacy and Data Security Law: Overview: Data Broker Registration](#)).

### **[Deidentified Patient Information]**

[We [do/do not ][sell ][and/or ][disclose] deidentified patient information exempt from the CCPA to third parties. [To deidentify the patient information, we followed [the HIPAA expert determination method] [and/or,] [the HIPAA safe harbor method] [and/or] [OTHER METHOD DESCRIPTION].]]

#### **DRAFTING NOTE: DEIDENTIFIED PATIENT INFORMATION**

The CCPA generally excludes deidentified patient information from its coverage scope (Cal. Civ. Code § 1798.146(a)(4)). However, the privacy policy of a business that sells or discloses it 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).)

Businesses selling or disclosing deidentified patient information must include this optional section. While not directly required, to provide clarity and transparency businesses that do not sell or disclose deidentified patient information should also consider including this optional section, affirmatively stating it they do not.

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](#).

### **Your Rights and Choices**

The CCPA provides consumers (California residents) with specific rights regarding their personal information. This section describes your CCPA rights and explains how to exercise those rights.

#### **DRAFTING NOTE: YOUR RIGHTS AND CHOICES**

The CCPA privacy policy must describe the consumers' rights regarding their personal information and explain how to exercise those rights (Cal. Civ. Code §§ 1798.105(b), 1798.120(b), 1798.130(a)(5)(A), and 1798.135(a); Cal. Code Regs. tit. 11, § 7011(c)(1)(A), (2)(A), (3)(A), (4)(A)). Those rights include:

- 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, 1798.110, 1798.115, 1798.120, and 1798.125.)

For a full discussion of the CCPA's consumer rights, see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Consumer Rights](#). For more on responding to consumer rights requests, see [Practice Note, Responding to CCPA and CPRA Consumer Rights Requests](#).

### ***Right to Know and Data Portability***

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months (the “right to know”). Once we receive your request and confirm your identity (see [Exercising Your Rights to Know or Delete](#)), we will disclose to you:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting or selling that personal information.
- The categories of third parties with whom we share that personal information.
- If we sold or disclosed your personal information for a business purpose, two separate lists disclosing:
  - sales, identifying the personal information categories that each category of recipient purchased; and
  - disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.
- The specific pieces of personal information we collected about you (also called a data portability request).

[We do not provide a right to know or data portability disclosure for B2B personal information.]

### **DRAFTING NOTE: RIGHT TO KNOW AND DATA PORTABILITY**

#### **Individualized Disclosures**

The CCPA grants consumers an individualized right to know about the business’s collection and use of their specific personal information. The CCPA spreads a business’s obligations and response requirements for this right out among several different sections (Cal. Civ. Code §§ 1798.100(a), (c), 1798.110(a), (b), 1798.115(a), (b), and 1798.130; Cal. Code Regs. tit. 11, §§ 7001(r) and 7024).

This policy section pulls requirements from those different sections together to provide a clearer description of the consumer’s right to know.

The initial CCPA section establishing the consumer’s right to know about personal information business purpose disclosures does not specifically require matching the personal information categories to the third-party recipient categories, like the section on sales does (see Cal. Civ. Code § 1798.115(a)(3) for disclosures and Cal. Civ. Code § 1798.115(a)(2) for sales). However, the CCPA section implementing those individualized disclosure rights and the CCPA Regulations both require it (Cal. Civ. Code § 1798.130(a)(4)(C); Cal. Code Regs. tit. 11, § 7024(j)).

To learn more about this individualized disclosure right, see [Practice Notes, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Individual Right to Know](#) and [Practice Note, Responding to CCPA and CPRA Consumer Rights Requests: Individualized Privacy Notice](#).

#### **Data Portability Rights**

The CCPA’s requirements to provide the specific pieces of personal information the business has collected in a readily useable format creates what many refer to as a data portability right (Cal. Civ. Code §§ 1798.100(a), (d), 1798.110(a)(5), (b), (c)(5), and 1798.130(a)(2); Cal. Code Regs. tit. 11, § 7024). To learn more about the scope of this right, see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Data Portability](#) and [Practice Note, Responding to CCPA and CPRA Consumer Rights Requests: Data Portability Responses](#).

#### **B2B Personal Information**

The 2019 CCPA Amendments and CPRA provide a temporary B2B personal information exception

for compliance with right to know requests until January 1, 2023 (Cal. Civ. Code § 1798.145(n); see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights](#)

[Act \(CPRA\): Temporary Exemptions](#)). Businesses that plan to exclude B2B personal information when responding to verified consumer access requests should include the optional disclaimer.

### **Right to Delete**

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions (the “right to delete”). Once we receive your request and confirm your identity (see [Exercising Your Rights to Know or Delete](#)), we will review your request to see if an exception allowing us to retain the information applies. We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

1. Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, or otherwise perform our contract with you.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Debug products to identify and repair errors that impair existing intended functionality.
4. Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
5. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 et. seq.).
6. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information’s deletion may likely render impossible or seriously impair the research’s achievement, if you previously provided informed consent.
7. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
8. Comply with a legal obligation.
9. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

We will delete or deidentify personal information not subject to one of these exceptions from our records and will direct our service providers to take similar action.

[We do not provide these deletion rights for B2B personal information.]

### **DRAFTING NOTE: DELETION REQUEST RIGHTS**

The CCPA notice must disclose the consumers’ right to request deletion of their personal information (Cal. Civ. Code §§ 1798.105(b) and 1798.130(a)(5)(A)). This right requires a business to delete personal information from its records after receiving a verifiable consumer request, unless one of nine statutory exceptions allow the business to retain it (Cal. Civ. Code § 1798.105(c), (d)).

The business must also instruct its service providers to delete any information that the CCPA requires it to delete under this consumer right (Cal. Civ. Code § 1798.105(c)).

For more on this right, see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Deletion Rights](#) and [Practice Note, Responding to CCPA and CPRA Consumer Rights Requests: Deletion Request Substantive Response](#). For a model deletion response letter, see [Standard Document, Deletion Request Response Letter \(CCPA and CPRA\)](#).



### **B2B Personal Information**

The 2019 CCPA Amendments and CRPA provide a temporary B2B personal information exception for compliance with deletion requests until January 1, 2023 (Cal. Civ. Code § 1798.145(n); see [Practice Note, Understanding the California Consumer Privacy Act](#)

(CCPA) and the California Privacy Rights Act (CPRA): [Temporary Exemptions](#)). Businesses that plan to exclude B2B personal information when responding to verified consumer deletion requests should include the optional disclaimer.

### ***Exercising Your Rights to Know or Delete***

To exercise your rights to know or delete described above, please submit a request by either:

- [Calling us at [TOLL-FREE NUMBER].]
- [Emailing us at [EMAIL ADDRESS].]
- [Visiting [WEBSITE ADDRESS].]
- [[PASSWORD PROTECTED ACCOUNT INSTRUCTIONS].]
- [[OTHER METHOD].]

Only you, or someone legally authorized to act on your behalf, may make a request to know or delete related to your personal information. [To designate an authorized agent, [INSTRUCTIONS].]

You may also make a request to know or delete on behalf of your child by [INSTRUCTIONS].

You may only submit a request to know twice within a 12-month period. Your request to know or delete must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative, which may include:
  - [VERIFICATION REQUIREMENTS].
  - [[PARENT OR GUARDIAN VERIFICATION REQUIREMENTS].]
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you.

You do not need to create an account with us to submit a request to know or delete. [However, we do consider requests made through your password protected account sufficiently verified when the request relates to personal information associated with that specific account.]

We will only use personal information provided in the request to verify the requestor's identity or authority to make it.

For instructions on exercising your sale opt-out or opt-in rights, see [Personal Information Sales Opt-Out and Opt-In Rights](#).

### **DRAFTING NOTE: EXERCISING YOUR RIGHTS TO KNOW OR DELETE**

#### **Submission Methods**

Businesses must provide consumers with at least two methods for making verifiable requests to exercise

these rights and the specific submissions methods required depends on how the business interacts with its consumers. For example, most businesses need to provide consumers with a toll-free telephone number

and an online form to submit requests. However, some business that directly interact with consumers online may only need to provide an email address. Also, while businesses can require existing account holders to submit requests through their account, they cannot require a consumer to create an account in order to make a CCPA rights request (Cal. Civ. Code § 1798.130(a)(1), (2), (5)(A).)

For more on the specific submissions requirements for different business types, see [Practice Note, Responding to CCPA and CPRA Consumer Rights Requests: Establish Methods to Receive Consumer Requests](#).

The business should select or describe the actual methods it provides to receive CCPA rights requests using the optional clauses provided.

The CCPA also limits the number of right to know requests a consumer may make to two in a 12-month period (Cal. Civ. Code §§ 1798.100(d) and 1798.130(b)). While it does not specifically limit the number of deletion requests, a business may refuse consumer requests that are manifestly unfounded or excessive, in particular because of their repetitive character (Cal. Civ. Code § 1798.145(i)(3)).

The CCPA prohibits using personal information collected to verify a consumer's request for any purpose other than the verification (Cal. Civ. Code § 1798.130(a)(7)).

### Verifying Consumer Identities

The CCPA only requires a business to honor a consumer's request to know or delete if it can reasonably verify the requester's identity (Cal. Civ. Code §§ 1798.100(c), (d), 1798.105(c), 1798.110(b), 1798.115(b), 1798.130(a)(2), and 1798.140(y)). The business may disregard a request that it cannot verify (Cal. Civ. Code § 1798.140(y)).

The privacy policy must:

- 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.
- Describe the process the business will use to verify the consumer's request, including any information the consumer must provide.
- Provide instructions describing how an authorized agent can make requests on a consumer's behalf.
- If the business has actual knowledge that it sells the personal information of consumers under age 16, describe the process that parents or legal guardians should use to verify their identity and submit requests to know, delete, and opt into personal information sales.

(Cal. Code Regs. tit. 11, §§ 7011(c)(1)(B) to (C), (2)(B) to (C), (5), (9) and 7072(a).)

The verification process disclosure requirements for 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, § 7072(a)).

The CCPA Regulations provide detailed guidance on how to reasonably verify a request and ensure the business only shares personal information with the consumer to which the personal information relates (Cal. Code Regs. tit. 11, §§ 7060 to 7063). For a detailed discussion of these verification requirements, see [Practice Note, Responding to CCPA and CPRA Consumer Rights Requests: Verifying Consumer Identities](#).

Businesses should review these guidelines to determine their unique submission and verification process, then ensure the privacy policy section accurately describes that process to consumers.

The CCPA provides that a request made using a consumer's password protected account with the business is a verifiable consumer request (Cal. Civ. Code § 1798.185(a)(7)). If the business permits consumers to make verifiable consumer requests using their password protected accounts, it should add that method to the submission list and include the optional clause regarding password protected accounts.

### Response Timing and Format

We will confirm receipt of your request within ten (10) business days. If you do not receive confirmation within the 10-day timeframe, please [contact [CONTACT] / [OTHER ACTION]].

We endeavor to substantively respond to a verifiable consumer request within forty-five (45) days of its receipt. If we require more time (up to another 45 days), we will inform you of the reason and extension period in writing.

If you have an account with us, we will deliver our written response to that account. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option.

Any disclosures we provide will only cover the 12-month period preceding our receipt of your request. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance[, specifically [EXPECTED FORMAT DESCRIPTION]].

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

### DRAFTING NOTE: RESPONSE TIMING AND FORMAT

#### Timing

The CCPA sets strict deadlines for responding to verifiable consumer requests. It expects the business to provide request to know or delete responses with 45 calendar days of receipt, extendable by 45 calendar days if necessary. The maximum response time for any request to know or delete is 90 calendar days. (Cal. Civ. Code §§ 1798.130(a)(2) and 1798.145(i)(1); Cal. Code Regs. tit. 11, § 7021(b).)

Time spent verifying the requestor's identity does not delay the beginning of the 45-day response period (Cal. Civ. Code § 1798.130(a)(2)).

Businesses must also confirm receipt of requests within 10 business days of receipt (Cal. Code Regs. tit. 11, § 7021(a)).

For more on responding to requests, see [Practice Note, Responding to CCPA and CPRA Consumer Rights Requests: Response Timing and Frequency](#).

#### Delivery Format and Content

The CCPA and CCPA Regulations also establish clear and detailed expectations on the response format and content (Cal. Civ. Code § 1798.130; Cal. Code Regs. tit. 11, §§ 7021 to 7024 and 7031).

Particularly, consumers with accounts should receive request to know responses to that account, while consumers without accounts can choose between mail or electronic delivery. It also requires provision

of electronic information "in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance." (Cal. Civ. Code §§ 1798.100(d) and 1798.130(a)(2).)

When the consumer's request seeks the specific pieces of personal information collected, the readily useable and transferable delivery requirements combine to create the data portability right (see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Data Portability](#)). The business can choose any delivery format meeting the CCPA's requirements. If the business knows the specific format it intends to use, it should disclose this information to increase transparency and set appropriate expectations using the optional clause provided.

The CCPA does temper these disclosure requirements by limiting the response scope to only personal information collected, sold, or disclosed in the past 12 months (Cal. Civ. Code § 1798.130(a)(2)).

For more on responding to consumer requests, see [Practice Note, Responding to CCPA and CPRA Consumer Rights Requests](#).

#### Fees

The business generally cannot charge a fee to process or respond to a consumer's request (Cal. Civ. Code §§ 1798.100(d), 1798.130(a)(2)). The CCPA only permits charging a reasonable fee if consumer requests are

manifestly unfounded or excessive, in particular because of their repetitive character. The fee amount must reflect the administrative costs of providing the information or communication or taking the requested action requested. (Cal. Civ. Code § 1798.145(i)(1).) The

CCPA Regulations also prohibit charging authorized agents fees or setting verification requirements like notarization, that result in additional fees unless the business compensates the consumer for the costs (Cal. Code Regs. tit. 11, § 7060(d)).

### **Personal Information Sales Opt-Out and Opt-In Rights**

If you are age 16 or older, you have the right to direct us to not sell your personal information at any time (the “right to opt-out”). We do not sell the personal information of consumers we actually know are less than 16 years old, unless we receive affirmative authorization (the “right to opt-in”) from either the consumer who is between 13 and 15 years old, or the parent or guardian of a consumer less than 13 years old]. Consumers who opt-in to personal information sales may opt-out of future sales at any time.

To exercise the right to opt-out, you (or your authorized representative) may submit a request to us by visiting the following Internet Web page link:

[



]

**[HYPERLINKED URL with the title “Do Not Sell My Personal Information”]**

Once you make an opt-out request, we will wait at least twelve (12) months before asking you to reauthorize personal information sales. However, you may change your mind and opt back in to personal information sales at any time by:

**[OPT-IN INSTRUCTIONS OR URL LINK]**

You do not need to create an account with us to exercise your opt-out rights. We will only use personal information provided in an opt-out request to review and comply with the request.

### **DRAFTING NOTE: PERSONAL INFORMATION SALES OPT-OUT AND OPT-IN RIGHTS**

The right to opt-out of personal information sales (or opt-in for minors) is one of the CCPA’s significant changes (Cal. Civ. Code § 1798.120; Cal. Code Regs. tit. 11, §§ 7013, 7026 and 7028). A minor’s opt-in right applies to consumers under 16 years old and consumers at least 13 but less than 16 years old may exercise that right directly (Cal. Civ. Code § 1798.120(c); Cal. Code Regs. tit. 11, §§ 7070 to 7072).

The business’s privacy policy must:

- Explain the consumer’s personal information sales opt-out and opt-in rights.
- State whether or not the business sells personal information (see Drafting Note, Sales of Personal Information).

- If the business:

- sells personal information, provide a link to the “Do Not Sell My Personal Information” opt-out right notice or directly include the opt-out right notice’s complete contents (see [Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies: Opt-Out Right Notice](#));
- knowingly sells personal information about consumers under age 16, describe the verification process used before opting minors into such sales (Cal. Code Regs. tit. 11, § 7011(c)(9)).

(Cal. Civ. Code § 1798.135; Cal. Code Regs. tit. 11, §§ 7011(c)(3), 7070, 7071, 7072(a).)

The opt-in process disclosure requirements for 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, § 7072(a)).

Businesses must also make the opt-out request submission method easy for consumers to use and take minimal steps (Cal. Code Regs. tit. 11, § 7026(h); see also [Practice Note, Responding to CCPA and CPRA Consumer Rights Requests: Opt-Out Request Submission Methods](#)).

The business cannot:

- Require a consumer to create an account to exercise their opt-out rights (Cal. Civ. Code § 1798.135(a)(1)).
- Ask a consumer opting out to reauthorize personal information sales for at least 12 months after the request (Cal. Civ. Code § 1798.135(a)(5)).
- Use personal information collected in an opt-out request for any other purpose (Cal. Civ. Code § 1798.135(a)(6)).

For a detailed discussion of these rights, see [Practice Note, Understanding the California Consumer Privacy](#)

[Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Sale Opt-Out and Opt-In Rights and Practice Note, Responding to CCPA and CPRA Consumer Rights Requests: Responding to Sales Opt-Out and Opt-In Requests](#).

For more on drafting opt-out right notices, see [Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies: Opt-Out Right Notice](#).

### Uniform Opt-Out Icon

To supplement the opt-out notice, businesses may use the uniform opt-out icon approved in the CCPA Regulations (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](#).

### Non-Discrimination

We will not discriminate against you for exercising any of your CCPA rights. Unless permitted by the CCPA, we will not:

- Deny you goods or services.
- Charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties.
- Provide you a different level or quality of goods or services.
- Suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

However, we may offer you certain financial incentives permitted by the CCPA that **can result** in different prices, rates, or quality levels. Any CCPA-permitted financial incentive we offer will reasonably relate to your personal information’s value and contain written terms that describe the program’s material aspects. Participation in a financial incentive program requires your prior opt-in consent, which you may revoke at any time. [We currently provide the following financial incentives:

[FINANCIAL INCENTIVE NAME, HYPERLINKED TO THE DISCLOSURE DOCUMENT]]

## DRAFTING NOTE: NON-DISCRIMINATION

The privacy policy must explain the consumer’s right not to receive discriminatory treatment (Cal. Civ. Code §§ 1798.125, 1798.130(a)(5)(A); Cal. Code Regs. tit. 11, § 7011(c)(4)). While the CCPA does prohibit discriminating against consumers exercising their CCPA rights, including charging different prices or changing the good or service quality, it also expressly allows a business to offer certain financial incentives that may result in price or service differences under specific circumstances, including providing clear notice and opt-in consent from the consumer (Cal. Civ. Code § 1798.125(a)(2), (b)(1)–(4); Cal. Code Regs. tit. 11, §§ 7080 to 7081). To learn more about this right and the tension between the CCPA’s somewhat contradictory requirements, see [Practice Note, Understanding the California Consumer Privacy Act \(CCPA\) and the California Privacy Rights Act \(CPRA\): Freedom from Discrimination and Distinguishing Between Discriminatory Practices and Financial Incentive Offers](#).

A business that offers financial incentives must provide a notice with specific content requirements

that consumers must encounter before opting into the program (Cal. Code Regs. tit. 11, §§ 7001(n), 7010(d), and 7016). While the CCPA Regulations do not require that these notices appear directly in the business’s privacy policy:

- Providing financial incentive notice links improves transparency and provides clarity on how the business meets its non-discrimination obligations.
- Online financial incentive offers may provide the required notice by directly linking to a privacy policy section containing the required information (Cal. Code Regs. tit. 11, § 7016(a)(3)).

A business that offers CCPA-compliant financial incentives should include the optional clause that links to the required disclosure documents and opt-in pages.

For more on preparing financial incentive notices, see [Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies: Financial Incentive Notice](#).

### [CCPA Rights Request Metrics]

[Metrics regarding the consumer rights requests we received from [all individuals/California residents] from January 1, [YEAR] to December 31, [YEAR] appear in the following chart:

Request Type	Received	Granted (in whole or in part)	Denied	[Median/Mean] Days to Respond
Requests to Know	[NUMBER]	[NUMBER]	[[TOTAL NUMBER]	[DAYS]
<b>OR</b>				
Unverifiable: [NUMBER].				
Not by a [consumer/California resident]: [NUMBER].				
Called for information exempt from disclosure: [NUMBER].				
Denied on other grounds: [NUMBER].]				

## CCPA Privacy Policy for California Residents

Request Type	Received	Granted (in whole or in part)	Denied	[Median/Mean] Days to Respond
Requests to Delete	[NUMBER]	[NUMBER]	[[TOTAL NUMBER] OR Unverifiable: [NUMBER]. Not by a consumer: [NUMBER]. Called for information exempt from disclosure: [NUMBER]. Denied on other grounds: [NUMBER].]	[DAYS]
Requests to Opt-Out of Personal Information Sales	[NUMBER]	[NUMBER]	[[TOTAL NUMBER] OR Unverifiable: [NUMBER]. Not by a consumer: [NUMBER]. Called for information exempt from disclosure: [NUMBER]. Denied on other grounds: [NUMBER].]	[DAYS]

]

### DRAFTING NOTE: CCPA RIGHTS REQUEST METRICS

The CCPA Regulations require the privacy policy 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](#).

By July 1 of each calendar year, the large business must compile and publish in its privacy policy metrics for the prior calendar year that disclose:

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

(Cal. Code Regs. tit. 11, § 7102(a).)

Optionally, the large businesses may:

- Break the metrics on denials down into requests denied in whole or part because they:
  - were not verifiable;
  - were not made by a consumer;
  - called for information exempt from disclosure; or
  - were denied on other grounds.

- Compile and disclose the metrics on requests received from all individuals instead of just California residents, provided its disclosure identifies how the metrics were calculated and, if requested, the business can provide California-only CRR Metrics to the California AG.

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

Businesses meeting the large business threshold should include this optional section.

### **[Other California Privacy Rights]**

[California's "Shine the Light" law (Civil Code Section § 1798.83) permits users of our Website that are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. To make such a request, please send an email to [EMAIL ADDRESS][ or write us at: [MAILING ADDRESS]].]

### **DRAFTING NOTE: OTHER CALIFORNIA PRIVACY RIGHTS**

The CCPA does not preempt all other California laws providing privacy rights. Instead, it carves out exceptions for certain personal information and activities protected by other sector-specific laws, but then expressly states that is meant to supplement, not replace, existing consumer protection laws, specifically identifying as complementary laws:

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

It also requires that in case of any conflicts with California laws, the law affording the greatest privacy protections controls (Cal. Civ. Code § 1798.175). As a result, businesses that must comply with the California "Shine the Light" law should retain their current compliance programs. For more on preemption, see [Practice Note, Understanding the California Consumer](#)

#### **Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Preemption and Conflict of Laws and Statutory Interpretation.**

Under the "Shine the Light" law, a covered business that shares certain types of a California resident's personal information with third parties for their own direct marketing purposes must, subject to certain exceptions, provide those California residents with either:

- A list of the personal information categories disclosed to third parties for their marketing purposes during the preceding calendar year, with the names and addresses of those third parties.
- A privacy statement giving those California residents a cost-free means to opt out of information sharing.

A business that provides a cost-free means to opt-out of information sharing or is not covered by California's Shine the Light law does not need to include this optional section. For more on California's Shine the Light law, see [Practice Note, California Privacy and Data Security Law: Overview: Shine the Light](#).



## CCPA Privacy Policy for California Residents

### Changes to Our Privacy Policy

We reserve the right to amend this privacy policy at our discretion and at any time. When we make changes to this privacy policy, we will post the updated notice on the Website and update the notice's effective date. **Your continued use of our Website following the posting of changes constitutes your acceptance of such changes.**

#### **DRAFTING NOTE: CHANGES TO OUR PRIVACY POLICY**

The privacy policy should specify how the site operator notifies users of changes made to the policy. The business should archive or keep all versions of the privacy policy on file so that it has a clear record

of what version was in effect at a particular time. It should also post the prior version so that consumers can understand what changes were made.

### Contact Information

If you have any questions or comments about this notice, the ways in which [COMPANY] collects and uses your information described here [and in the [Privacy Policy](#)], your choices and rights regarding such use, or wish to exercise your rights under California law, please do not hesitate to contact us at:

**Phone:** [TOLL-FREE PHONE NUMBER]

**Website:** [WEBSITE CONTACT URL]

**Email:** [EMAIL ADDRESS]

**Postal Address:**

[COMPANY]

Attn: [CONTACT NAME/DEPARTMENT]

[PHYSICAL ADDRESS]

[[**OTHER CONTACT METHOD**]: [CONTACT INSTRUCTIONS]]

If you need to access this Policy in an alternative format due to having a disability, please contact [COMPANY EMAIL ADDRESS] [and] [COMPANY PHONE NUMBER].

#### **DRAFTING NOTE: CONTACT INFORMATION**

The policy must contain contact information that enables users to ask questions or raise concerns regarding the site operator's privacy policy or information practices (Cal. Code Regs. tit. 11, § 7011(c)(6)). A business adopting a contact method not listed, such as by contacting a third-party

dispute resolution service, should describe it using the optional clause provided.

The CCPA also requires the business to provide consumers with at least two methods for making verifiable requests to exercise certain CCPA rights (see Drafting Note, Exercising Your Rights to Know or Delete).

## CCPA Privacy Policy for California Residents

To help ensure consumers with disabilities can access the policy, this section also includes specific contact information for alternate format requests (see Drafting Note, Policy Presentation and Format). Business

should ensure that any online publications meet the Web Content Accessibility Guidelines published by the World Wide Web Consortium (see [W3C: Web Content Accessibility Guidelines \(WCAG\) Overview](#)).

### About Practical Law

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at [legalsolutions.com/practical-law](https://legalsolutions.com/practical-law). For more information or to schedule training, call 1-800-733-2889 or e-mail [referenceattorneys@tr.com](mailto:referenceattorneys@tr.com).