THOMSON REUTERS
PRACTICAL LAW™

Responding to CCPA and CPRA Consumer Rights Requests

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-027-1441**
Request a free trial and demonstration at: **us.practicallaw.tr.com/practical-law**

A Practice Note discussing the California Consumer Privacy Act of 2018 (CCPA), as amended by the voter-approved California Privacy Rights Act of 2020 (CPRA). The Note explains the requirements for receiving, verifying, and responding to CCPA and CPRA consumer rights requests. The Note also provides guidance and suggestions for setting up a CCPA and CPRA consumer rights response program.

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; 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 certain rights regarding their personal information and impose various data protection obligations on business that meet their jurisdictional thresholds. Businesses subject to the CCPA and CPRA must also enable California residents to exercise their personal information rights, including:

- The right to know, which encompasses both individualized personal information disclosures and data portability requirements.
- The right to delete personal information.
- Personal information sales opt-out and opt-in rights.

Once the CPRA becomes effective, consumers will also have rights to:

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

This Note discusses the CCPA and CPRA's requirements for enabling these rights and responding to consumer requests, including verification requirements, searching for responsive information, acting on the request, and responding to consumers. Given their broad reach, the CCPA and CPRA are likely to impact entities both inside and outside California that collect and process California residents' personal information.

For a broader discussion of the CCPA and CPRA, including which businesses must comply and how it defines consumers as California residents, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA). For the full list of CCPA and CPRA resources, see California Privacy Toolkit (CCPA and CPRA).

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 provisions until January 1, 2023. For more on these exceptions, see Practice Notes, California Privacy Laws (CCPA and CPRA): Impact on Employers and Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Temporary Exemptions.

Regulations developed by the California Attorney General (California AG) establish detailed requirements that organize, operationalize, and provide context for the

CCPA's different verification and response obligations to consumer right requests (CCPA Regulations) (Cal. Code Regs. tit. 11, §§ 7000 to 7102). For more on the CCPA Regulation's development process, 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 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 amendment 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.

Extending Rights to All Consumers or Limiting to California Residents

As a state law, the CCPA and CPRA's coverage only extends to businesses operating within California's jurisdictional reach. Only California residents are entitled to receive the CCPA and CPRA's protections and rights (see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Protected Individuals). The CCPA and CPRA also contain 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).

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

- Only provide the CCPA and CPRA's personal information rights 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 methods for submitting personal information rights requests.
- Establish separate internal procedures and systems for handling California residents' personal information, particularly to ensure the business can effectively honor sales opt-out requests.

However, new consumer privacy laws in Colorado and Virginia that take effect in 2023 will 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 practices to the CCPA and CPRA's requirements and make any required adjustments.

Data Maps

Accurately responding to a consumer's CCPA and CPRA rights request first requires a full understanding of exactly what personal information the business collects, obtains, uses, stores, shares, and sells about that individual and how to identify and access it. 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.

The business can then use the data maps to develop detailed guides that help employees responsible for responding to consumer rights requests know where to search for responsive information.

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

Consumer Rights Requests

The CCPA enables consumers to send covered businesses requests to exercise three different rights regarding their personal information:

- A right to know what personal information the business collected, sold, or disclosed about them, including the specific pieces of personal information held (see Request to Know Substantive Response).
- A right to make the business delete their personal information unless a statutory exception allowing its retention applies (see Deletion Request Substantive Response).
- A right to restrict sales of their personal information (see Responding to Sales Opt-Out and Opt-In Requests).

The CPRA will create three new personal information rights that consumers can exercise starting January 1, 2023:

- A right to make the business correct inaccurate personal information (see CPRA Revisions: Correction Request Substantive Response).
- A right to prevent the business from sharing their personal information with a third party for cross-context behavioral advertising purposes (see CPRA Revisions: Responding to Sharing Opt-Out and Opt-In Requests).
- A right to restrict how a business uses and discloses their sensitive personal information (see CPRA Revisions: Responding to Sensitive Personal Information Limitation Requests).

The CCPA and CPRA also protects consumers against waivers of these rights (Cal Civ. Code § 1798.192).

Once a business receives a consumer rights request, it must review, respond, verify, and act on that request within specific timeframes. To meet these CCPA and CPRA obligations, a covered business should establish internal procedures to:

- Enable consumers to submit rights requests (see Establish Methods to Receive Consumer Requests).
- Meet request response deadlines (see Response Timing and Frequency).
- Verify consumer identities (see Verifying Consumer Identities).
- Provide substantive responses for requests to know, delete, and correct (Request to Know Substantive Response, Deletion Request Substantive Response, and CPRA Revisions: Correction Request Substantive Response).
- Process personal information sales and sharing opt-out and opt-in requests (see Responding to Sales Opt-Out and Opt-In Requests and CPRA Revisions: Responding to Sharing Opt-Out and Opt-In Requests).
- Limit sensitive personal information use and disclosure (see CPRA Revisions: Responding to Sensitive Personal Information Limitation Requests).
- Manage service providers (see Service Provider Responsibility for Consumer Requests).
- Classify personal information transfers as sales or business purpose disclosures (see Distinguish Between Sales and Business Purpose Disclosures).
- Train employees and maintain required records (see Training and Recordkeeping Obligations).

For more on a business's other CCPA and CPRA obligations, such as providing public privacy notices and non-discrimination, see Practice Notes, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Consumer Rights and Drafting CCPA and CPRA Notices and Privacy Policies.

CPRA Revisions: New Exclusions

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

- To protect trade secrets (Cal, Civ. Code § 1798.185(a)(3); (Cal. Civ. Code §§ 1798.100(f) and 1798.145(a)(1) (effective January 1, 2023)).
- To protect free speech and press rights for noncommerical activities protected by California's Constitution (Cal. Civ. Code § 1798.145(l) (effective January 1, 2023)).
- To exempt certain commercial credit reporting agency actions from the deletion and opt-out rights (Cal. Civ. Code § 1798.145(o) (effective January 1, 2023)).
- To exempt household data from the business's right to know, deletion, and correction response obligations (Cal. Civ. Code § 1798.145(p) (effective January 1, 2023)).
- To exempt student grades, educational scores, or educational test results held for a local educational agency from the deletion right (Cal. Civ. Code § 1798.145(q) (effective January 1, 2023)).
- To exempt educational standardized assessments, including specific responses, from the right to know's disclosure requirements when disclosure could jeopardize its validity or reliability (Cal. Civ. Code § 1798.145(q) (effective January 1, 2023)).
- To exempt physical items containing personal information from the deletion and opt-out rights, such as the consumer's photograph, if the consumer previously consented to the item's creation and other circumstances apply (Cal. Civ. Code § 1798.145(r) (effective January 1, 2023)).

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

Establish Methods to Receive Consumer Requests

Businesses must establish designated contact methods consumers can use to submit CCPA-related requests. The CCPA and CCPA Regulations outline different, but related submission methods and requirements for:

- Requests to know (see Request to Know Submission Methods).
- Requests to delete (see Request to Delete Submission Methods).
- Requests to opt-out (see Opt-Out Request Submission Methods).

(Cal. Civ. Code §§ 1798.130(a) and 1798.135(a); Cal. Code Regs. tit. 11, § 7020; California AG Final Statement of Reasons for CCPA Regulations (CCPA FSOR) at 21 to 23 and California AG Initial Statement of Reasons for CCPA Regulations (CCPA ISOR) at 14 to 16.)

Businesses cannot require consumers to open accounts to submit CCPA-related requests. However, they can require existing account holders to submit requests using their account. (Cal. Civ. Code § 1798.130(a)(2).)

The CCPA Regulations also direct businesses to avoid erecting procedural barriers to consumer rights requests. When consumers submit requests incorrectly, the business must either:

- Inform the consumer about the correct way to submit the request or remedy any deficiencies.
- Treat deficient requests as if the consumer followed the business's process when submitting them.

(Cal. Code Regs. tit. 11, § 7020(e).)

The business's privacy policy must describe the submission method it establishes. For more on CCPA privacy policies, see Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies and Standard Document, CCPA Privacy Policy for California Residents.

Request to Know Submission Methods

The required submission method for requests to know depends on the type of business. A business can provide consumers with just an email address if it both:

- Only operates online.
- Has a direct relationship with its consumers.

(Cal. Civ. Code § 1798.130(a)(1)(A); Cal. Code Regs. tit. 11, § 7020(a).)

All other businesses must provide consumers with both:

- A toll-free telephone number.
- A second submission method of its choice, such as a dedicated email address, online portal, or printed form.

(Cal. Civ. Code § 1798.130(a)(1)(A); Cal. Code Regs. tit. 11, § 7020(a).)

While the CCPA also requires a business to let consumers submit requests to know on its internet site if it operates one, the CCPA Regulations do not mention this requirement (Cal. Civ. Code § 1798.130(a)(1)(B)).

Request to Delete Submission Methods

All businesses must provide at least two submission methods of their choice for requests to delete (Cal. Code Regs. tit. 11, § 7020(b)). The CCPA Regulations do not mandate a particular format, although they do require businesses to consider adopting methods that match or follow methods they typically use to communicate with consumers (Cal. Code Regs. tit. 11, § 7020(c)).

For example, a business that typically communicates with consumers in person should consider providing an in-person method for submitting requests. Other acceptable submission methods may include:

- A toll-free telephone number.
- A dedicated email address.
- An interactive form or similar website-based submission method.
- A printed form that consumers can submit using the mail or in person at a retail location.
- An in-store tablet or computer portal consumers can use to submit an interactive form.

(Cal. Code Regs. tit. 11, § 7020(a) to (c).)

A business may present consumers with choices to only delete portions of their personal information if it also presents a global option to delete all personal information more prominently than the partial deletion options (Cal. Code Regs. tit. 11, § 7022(h)).

CPRA Revisions: Submission Methods for Requests to Know, Delete, and Correct

The CPRA harmonizes the submission methods and requirements for requests to know, delete, and correct. It follows the current request to know approach that allows online businesses with direct consumer relationships to only provide an email address for submitting all three requests but requires all other businesses to offer a toll-free telephone number along with at least one other submission method. (Cal. Civ. Code § 1798.130(a)(1), (2)(A) (effective January 1, 2023); see Request to Know Submission Methods.)

However, businesses should not alter or reduce their current deletion request submission methods unless and until the California Privacy Protection Agency changes the related CCPA Regulations that provide stricter requirements (see Request to Delete Submission Methods and Amendments and Regulations; see also CPRA Regulation Tracker).

Opt-Out Request Submission Methods

A business that sells personal information must provide at least two methods for submitting personal information sales opt-out right requests:

- An internet page titled "Do Not Sell My Personal Information" containing an interactive submission form, accessible from clear and conspicuous links using the title posted to the business's website or mobile application. All businesses must provide this method.
- A second submission method of its choice that reflects how it primarily interacts with consumers, considering:
  - the methods it normally uses to interact with consumers;
  - how it sells personal information to third parties;
  - available technology; and
  - the consumer's ease of use.

(Cal. Civ. Code § 1798.135(a); Cal. Code Regs. tit. 11, § 7026(a), (b).)

The vast majority of businesses should incorporate the required online submission form as part of its required opt-out right notice (Cal. Civ. Code § 1798.135; Cal. Code Regs. tit. 11, § 7013(b)(2); see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Opt-Out Right Notice). However, the CCPA Regulations do allow a business that does not operate a website to establish, document, and comply with another method to inform consumers about their personal information sales opt-out rights (Cal. Code Regs. tit. 11, § 7013(b)(2)).

Potential second submission methods include:

- The same methods used for requests to know or delete (see Request to Know Submission Methods and Request to Delete Submission Methods).
- User enabled global privacy controls that communicate or signal the consumer's personal information sales opt-out choice, which businesses collecting information online must honor (see Extra Submission Requirement for Online Personal Information Collection). Global privacy controls may include:
  - a browser plug-in;
  - device settings;
  - privacy center settings; or
  - other similar mechanisms.

(Cal. Code Regs. tit. 11, § 7026(a) to (c).)

The business cannot require consumers to create an account to submit opt-out rights requests or use personal information collected during the opt-out right submission process for any other purpose (Cal. Civ. Code § 1798.135(a)(1), (6)).

The CCPA Regulations also:

- Require the selected opt-out method to be easy for consumers to execute and use minimal steps. Specifically, opt-out methods should not require consumers to take more steps than the process for opting back in to personal information sales.
- Prohibit methods designed with the purpose of, or that have the substantial effect of, subverting or impairing a consumer's opt-out choices, including:
  - using confusing language in opt-out notices, such as double negatives like don't not sell my personal information;
  - requiring consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request, unless specifically permitted under the CCPA Regulations (see Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies: Financial Incentive Notice);
  - requiring consumers to provide personal information that is not necessary to implement the opt-out request; and

- requiring consumers to search or scroll through the text of a privacy policy or similar document or webpage to locate the opt-out request mechanism after clicking on a "Do Not Sell My Personal Information" link.

(Cal. Code Regs. tit. 11, § 7026(h).)

Similar to deletion requests, the CCPA Regulations allow businesses to present opt-out choices for a subset of personal information sales, if they also present a global opt-out option for all sales more prominently than other options (Cal. Code Regs. tit. 11, § 7026(d)).

Importantly, a business can **avoid** posting an opt-out submission form if it:

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

(Cal. Code Regs. tit. 11, § 7013(d).)

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

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 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.

Extra Submission Requirement for Online Personal Information Collection

Businesses that collect personal information from consumers online must treat user-enabled global privacy controls as a valid opt-out request submission method for that browser, device, or if known, the actual consumer (Cal. Code Regs. tit. 11, § 7026(c)). The California AG indicated that it added this requirement with the intent to support innovation for privacy services and ensure businesses do not ignore or reject consumer choice tools (CCPA FSOR at 36 to 39, CCPA ISOR at 24).

Lack of clear browser-based controls and technology standards, like do not track (DNT) signals, initially made compliance with this requirement to honor browser-based global privacy settings difficult. However, a consortium of businesses working together have now issued a Global Privacy Control (GPC) specification that businesses can use to interpret browser-based consumer do-not-sell requests.

CCPA FAQs issued by the California AG now directly reference the new GPC technical standard and indicate that covered business must honor those GPC signals as a valid consumer request to stop the sale of personal information (see OAG: CCPA FAQ B.7 and B.8).

The CCPA Regulations also clarify that:

- The business only needs to honor global privacy control signals that clearly communicate the consumer's personal information sales opt-out request.
- When discrepancies arise between a global privacy control signal and a business-specific privacy setting, such as a consumer's participation in a business's financial incentive program, the business must respect the global privacy control setting unless:
  - it notifies the consumer about the conflict; and
  - the consumer chooses to confirm the business-specific setting or financial incentive program participation.

(Cal. Code Regs. tit. 11, § 7026(c)(1), (2).)

Subsequently, the California AG announced a $1.2 million settlement with Sephora USA, Inc. over CCPA violations that included allegations the company did not honor user-generated GPC signals to opt consumers out of personal information sales (see Legal Update, California AG Announces $1.2 Million Settlement with Sephora for CCPA Personal Information Sales Violations). The California AG press release about the settlement reminded businesses that they must treat opt-out requests made by user-enabled global privacy controls the same as requests made by users who have clicked the "Do Not Sell My Personal Information" links, and announced it had sent several enforcement notices to businesses about honoring GPC signals (see OAG: Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act).

CPRA Revisions: Opt-Out Request Submission Methods

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)). Conversely, the CPRA creates a mirrored set of requirements for the 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).)

However, the CPRA also provides business with an important alternative to using webpage links. 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 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.)

The CPRA retains, but moves, the CCPA's prohibition on requiring consumers to create an account to exercise their opt-out rights or using personal information collected during the opt-out right submission process for any other purpose (Cal. Civ. Code § 1798.135(c)(1), (6) (effective January 1, 2023)). It also prohibits businesses from asking consumers for more information than what is necessary to execute the opt-out request (Cal. Civ. Code § 1798.135(c)(1) (effective January 1, 2023)).

Common Response Requirements for Requests to Know or Delete

Once the business receives a consumer's request to know or delete, it must:

- Reply to the requestor within specific timeframes (see Response Timing and Frequency).
- Verify the requestor's identity (see Verifying Consumer Identities).
- Prepare a substantive response to the request (see Request to Know Substantive Response and Deletion Request Substantive Response).
- Provide the response and requested information free of charge, unless the request is manifestly unfounded or excessive.

(Cal. Civ. Code §§ 1798.100(c) to (d), 1798.105(c), 1798.110(b), 1798.115(b), 1798.130(a), 1798.140(y), and 1798.145(i); Cal. Code Regs. tit. 11, §§ 7021 to 7031 and 7060 to 7063.)

Unless it is the business's usual practice to do so, responding to consumer requests does not require a business to:

- Retain information collected for a single transaction.
- Link de-identified information to personal information.

(Cal. Civ. Code §§ 1798.100(e) and 1798.110(d).)

CPRA Revisions: Common Response Requirements for Requests to Know, Delete, or Correct

The CPRA extends the CCPA's right to know and deletion response timing and verification requirements to the consumer's new correction right (Cal. Civ. Code §§ 1798.130(a)(2), 1798.145(h) (effective January 1, 2023)). It also establishes specific requirements for substantively responding to correction requests (see CPRA Revisions: Correction Request Substantive Response).

The CPRA also clarifies that the business's response obligation does not apply to personal information about a consumer that belongs to another natural person or that the business maintains for another natural person (Cal. Civ. Code § 1798.145(k) (effective January 1, 2023)).

Response Timing and Frequency

Confirming Receipt

A business must confirm receipt of a consumer's request to know or delete within ten business days (Cal. Code Regs. tit. 11, § 7021(a)). The receipt must inform the consumer about the business's process for responding to requests, including:

- Generally describing the business's verification process.
- Providing an expected response timeframe, unless the business already granted or denied the request.

(Cal. Code Regs. tit. 11, § 7021(a).)

A business may provide the confirmation response in the same manner that it received the request. For example, a business receiving requests on its toll-free telephone number can provide the confirmation orally during the call as part of its intake process script. (Cal. Code Regs. tit. 11, § 7021(a).)

Guidance provided by the California AG further explains that businesses can automate this initial response to lessen the cost and burden and that requirement's purpose is to improve transparency about the process and set appropriate expectations (CCPA FSOR at 23, CCPA ISOR at 16 to 17).

Substantive Response Deadlines

A business has 45 calendar days from the date it receives a consumer's request to know or delete to provide its substantive response. Time spent verifying the requestor's identity does not stay or extend the substantive response deadline.

The business may extend this response period for another 45 calendar days if necessary. However, the business must first notify the consumer about its reasons for extending the response period within the original 45-day deadline. The maximum total response period, including any extensions, is 90 calendar days.

(Cal. Civ. Code § 1798.130(a)(2); Cal. Code Regs. tit. 11, § 7021(b); CCPA FSOR at 24, CCPA ISOR at 17.)

The CPRA retains these same response deadlines, also applying them to a consumer's correction request (Cal. Civ. Code §§ 1798.130(a)(2) and 1798.145(h)(1) (effective January 1, 2023)).

Frequency

The CCPA's right to know only allows consumers to make two requests to a business within any 12-month period. A business can deny more frequent requests, but it can also decide to honor additional requests as a customer service. (Cal. Civ. Code § 1798.100(d).)

There are no similar limits on the number of deletion requests. However, the business can deny or charge a fee for manifestly unfounded or excessive deletion requests. Any fee charged must consider the administrative costs for the deletion requests and the business bears the burden for proving that the request was manifestly unfounded or excessive. (Cal. Civ. Code § 1798.145(i)(3).)

The CRPA retains these same frequency and fee requirements (Cal. Civ. Code §§ 1798.130(b) and 1798.145(h)(3) (effective January 1, 2023)). As with deletion requests, the CPRA does not directly limit the number of correction requests a consumer may make. However, it does direct the California Privacy Protection Agency to establish regulations on how often, and under what circumstances, a consumer may request a correction (Cal. Civ. Code § 1798.185(a)(8); see CPRA Regulation Tracker).

Verifying Consumer Identities

The CCPA vaguely defines a verifiable consumer request as one that:

- A consumer or someone legitimately acting on the consumer's behalf makes.
- The business can reasonably verify is from the person about whom it collected personal information, by following the processes established in the CCPA Regulations (see Amendments and Regulations).

(Cal. Civ. Code § 1798.140(y).)

The CCPA Regulations define the term verify as determining that:

- The consumer making a request to know or request to delete is the consumer about whom the business has collected information.
- The person making a request to know or request to delete for personal information about a consumer under age 13 is that consumer's parent or legal guardian.

(Cal. Code Regs. tit. 11, § 7001(x).)

To help businesses operationalize their obligation to verify a consumer's identity before providing a substantive response to their request, the CCPA Regulations provide general verification guidelines (see General Verification Considerations). The CCPA Regulations also provide specific verification requirements that depend on whether the requestor:

- Has a password-protected account (see Verifying Using Password-Protected Accounts).
- Is a non-account holder or unnamed person (see Verifying Non-Account Holder Identities).
- Is an authorized agent (see Verifying Requests from Authorized Agents).
- Seeks household level information (see Verifying Household Consumer Requests).
- Seeks information from a minor under age 13 (see Verifying Parental Consent).

(Cal. Code Regs. tit. 11, §§ 7060 to 7063.)

Verifying requests should not require a business to take the following actions, unless it already does so in its normal course of operations:

- Retain information collected for a single transaction.
- Link de-identified information to personal information.
- Re-identify individual data.

(Cal. Civ. Code §§ 1798.100(e) and 1798.110(d); Cal. Code Regs. tit. 11, § 7060(f).)

The CCPA permits businesses to deny consumer requests to know or delete that they cannot verify (Cal. Civ. Code § 1798.140(y); Cal. Code Regs. tit. 11, §§ 7021(b), 7024(a), (b), 7022(a), and 7062(f)). However, the CCPA Regulations still require that the business confirm receipt of those requests and provide alternative responses in specific situations (see Confirming Receipt and Responding to Non-Verified Requests).

CPRA Revisions: Verifying Consumer Identities

The CPRA adds a qualifier to the verifiable consumer request definition so it requires a business to use commercially reasonable methods to verify a consumer's identity (Cal. Civ. Code § 1798.140(ak) (effective January 1, 2023)). It also specifically allows someone acting as a conservator for the consumer or with the person's power of attorney to make a verifiable consumer request (Cal. Civ. Code § 1798.140(ak) (effective January 1, 2023)).

The CPRA also moves and alters the section describing what type of actions a business does not need to take when responding to request. The revised section clarifies that, unless a business already does so in the normal course of business, the CPRA will not require it to:

- Reidentify or otherwise link information that is not ordinarily maintained as personal information.
- Retain personal information about a consumer that it would not normally retain.
- Maintain information in an identifiable, linkable, or associable form so that the business can link or associate a verifiable consumer request with personal information.

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

The CPRA does not change a business's ability to deny rights requests when it cannot verify the consumer's identity (Cal. Civ. Code § 1798.140(ak) (effective January 1, 2023)).

Many of the current consumer verification requirements and guidance come from the CCPA Regulations, which the California Privacy Protection Agency may eventually revise expand (Cal. Civ. Code § 1798.185(a)(7), (8), (14); see CPRA Regulation Tracker).

General Verification Considerations

Verifying a requestor's identity is a difficult task, with many different roads to compliance. Recognizing this, the California AG embraced a flexible approach that emphasizes the need for each business to establish, document, and follow a reasonable verification process that fits its unique circumstances and uses reasonable security measures to detect fraudulent activity and prevent unauthorized access or deletion (Cal. Code Regs. tit. 11, § 7060(a), (e); CCPA FSOR at 46, CCPA ISOR at 29 and 30).

The CCPA Regulations adopt a matrix approach for determining how far a business must go to verify a requestor's identity that considers:

- The type, sensitivity, and value of the personal information involved in the request, with a presumption of sensitivity for personal information protected by the California Data Protection Act (see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Private Right of Action for Data Breaches).
- The potential harm a consumer may face from unauthorized access or deletion of personal information involved in the request.

- The likelihood that fraudulent or malicious actors would seek the personal information involved in the request.
- Whether personal information the consumer provides to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated.
- How the business typically interacts with the consumer.
- Available technology for verification.

(Cal. Code Regs. tit. 11, § 7060(b)(3); CCPA ISOR at 29 to 30.)

Requests involving:

- Sensitive or valuable personal information or a greater potential for consumer harm or fraudulent activity, all warrant a more stringent verification process (Cal. Code Regs. tit. 11, § 7060(b)(3)(A) to (C)).
- Personal information from a child under age 13 also requires the business to verify that the requestor is the child's parent or guardian (Cal. Code Regs. tit. 11, § 7070(c)).
- Deletion may use a two-step verification process where the individual first submits the verified request, then separately confirms they want their personal information deleted to prevent accidental and irrevocable deletion requests and to assure businesses that the individual made a clear choice to exercise their deletion rights (Cal. Code Regs. tit. 11, § 7020(d); CCPA FSOR at 22, CCPA ISOR at 16).

While businesses can ask a requestor for personal information to verify identity, the CCPA Regulations also caution them:

- To avoid collecting sensitive personal information.
- To avoid collecting new personal information not already in the business's possession.
- If colleting new information is necessary:
  - to only use it for identity purposes; and
  - to delete it as soon as practical after processing the request and to comply with recordkeeping obligations (see Training and Recordkeeping Obligations).

(Cal. Code Regs. tit. 11, § 7060(b)(2), (c).)

When no reasonable method to verify a requestor's identity to the appropriate degree of certainty exists, the CCPA Regulations do permit denial of the request if the business:

- Explains exactly why it has no reasonable method to verify the requestor's identity in its response.
- Provides that explanation in its privacy policy when the problem exists for all consumers.
- Revaluates and documents whether it can establish a reasonable verification process at least once every 12 months.

(Cal. Code Regs. tit. 11, § 7062(g); CCPA FSOR at 48, CCPA ISOR at 33.)

Documenting the business's unique process and the related analysis that justifies its adoption is a critical step in complying with the CCPA's required identity verification (see CCPA ISOR at 29). What is reasonable can also change over time, as hackers and other bad actors adopt new tactics and technology evolves. Therefore, businesses should also regularly review and update their verification procedures.

The CCPA Regulations also require that businesses transparently describe their verification process, including any information the requestor must provide, and avoid placing unnecessary roadblocks that prevent consumers from exercising their CCPA rights (Cal. Code Regs. tit. 11, §§ 7011(c)(1)(C), (2)(C), 7020(e), and 7021(a); CCPA FSOR at 22 and 23).

Verification Fees

Businesses cannot charge consumers or their authorized agents a fee to verify their request. They also cannot set requirements, like notarization, that result in additional fees unless the business compensates the consumer for the costs. (Cal. Code Regs. tit. 11, § 7060(d); CCPA FSOR at 46.)

Verifying Using Password-Protected Accounts

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)). While a business cannot require a consumer to create an account to make a CCPA or a CPRA rights request, it may require preexisting account holders to make rights requests using their accounts (Cal. Civ. Code § 1798.130(a)(2); Cal. Civ. Code § 1798.130(a)(2)(A) (effective January 1, 2023)).

A business that wants to verify consumers' identities using their password-protected accounts must first review and evaluate the system's current authentication practices to ensure they meet the CCPA Regulations' general standards. It must also require the consumer to re-authenticate before acting on the request. (Cal. Code Regs. tit. 11, § 7061(a); CCPA ISOR at 30 to 31.)

Any indications or suspicions of fraudulent or malicious activity on the consumer's password-protected account require the business to suspend reliance on this verification method and use other procedures to confirm that the consumer's request is authentic (Cal. Code Regs. tit. 11, § 7061(b); CCPA ISOR at 30 to 31).

Verifying Non-Account Holder Identities

For non-account holders, the CCPA Regulations set verification standards along a sliding scale from:

- A **reasonable degree of certainty** for requests to know categories of personal information or to delete non-sensitive information with a low risk of harm, which may require:
  - matching at least two data points the requestor provides with information the business holds; and
  - a determination by the business that the information matched is reliable for verification purposes.
- A **reasonably high degree of certainty** for disclosure of specific pieces of personal information or deletion of sensitive information with a high risk of harm, which may require:
  - matching at least three pieces of personal information the requestor provides with information the business holds;
  - a determination by the business that the information matched is reliable for verification purposes; and
  - a signed declaration under penalty of perjury from the requestor stating that the personal information requested is about the requestor. A business using this method must maintain all signed declarations as part of its recordkeeping obligations (see Training and Recordkeeping Obligations).

(Cal. Code Regs. tit. 11, § 7062(a) to (d); CCPA FSOR at 46 and 47, CCPA ISOR at 31 to 33.)

As an example, the CCPA Regulations suggest that when a business maintains personal information associated with a named individual, it may verify a requestor's identity to a reasonable degree of certainty by requiring the person to identify or match:

- Recently purchased items.
- The dollar amounts of recent purchases.

(Cal. Code Regs. tit. 11, § 7062(e)(1).)

For unnamed individuals, such as a mobile application that does not require an account but tracks individual device-level data, the business may verify the requestor's identity by:

- Asking for information only the application user was likely to know.
- Requiring the consumer's response to a device notification.

(Cal. Code Regs. tit. 11, § 7062(e)(2).)

However, the best verification techniques for each business must, by necessity, remain highly fact or situation dependent.

Verifying Requests from Authorized Agents

When a consumer authorizes an agent to make verified requests on its behalf, the CCPA Regulations allow the business to require:

- The authorized agent to provide proof that the consumer gave the agent signed permission to submit the request.
- The consumer to verify their own identity directly with the business.
- The consumer to directly confirm that they provided the authorized agent permission to submit the request.

(Cal. Code Regs. tit. 11, § 7063(a).)

The additional agent verification requirements do not apply when the agent holds a valid power of attorney under the California's Probate Code (Cal. Code Regs. tit. 11, § 7063(b)).

Authorized agents must:

- Implement and maintain reasonable security procedures and practices to protect the consumer's information.
- Only use a consumer's personal information, and any information collected from or about the consumer, to fulfill the consumer's request, confirm identities, or for fraud prevention.

(Cal. Code Regs. tit. 11, § 7063(c), (d).)

Authorized agents cannot make requests on behalf of children under age 13 (Cal. Code Regs. tit. 11, § 7070(c); CCPA FSOR at 50).

Verifying Household Consumer Requests

Businesses should deny household-based data portability requests or deletion requests unless:

- For non-password protected accounts:
  - all household members jointly request the access; and
  - the business verifies each household member's identity and confirms the person is a current household member (see Verifying Non-Account Holder Identities).
- For password-protected accounts, the request meets the same verification practices and requirements used for individual accounts (see Verifying Using Password-Protected Accounts).
- For households that contain minors under age 13, the business obtains verifiable parental consent (see Verifying Parental Consent).

(Cal. Code Regs. tit. 11, § 7031; see Data Portability Responses and Deletion Request Substantive Response.)

Household-based requests to know that just seek an individualized privacy disclosure do not require any additional verification steps (see Individualized Privacy Notice).

The CCPA Regulations define a household as a person or group all:

- Residing at the same address.
- Sharing a common device or the business's service.
- Using the same group account or unique identifier.

(Cal. Code Regs. tit. 11, § 7001(k).)

CPRA Revisions: Verifying Household Consumer Requests

The CPRA specifically excludes household data from the business's obligation to provide consumers with the rights to know, delete, and correct (Cal. Civ. Code § 1798.145(p) (effective January 1, 2023)). As a result, the CCPA Regulations on consumer verification will eventually become moot for those requests. However, this household data exclusion does not go into effect until January 1, 2023.

The CPRA also defines a household as group of consumers who cohabitate with one another at the same residential address and share use of common devices or services (Cal. Civ. Code § 1798.140(q) (effective January 1, 2023)).

Verifying Parental Consent

Only a parent or legal guardian can make requests to know or delete personal information about a consumer under age 13 or provide consent for a personal information sales opt-in request. Under the CCPA Regulations, a business must adopt and document verification methods reasonably calculated to ensure this requirement is met. (Cal. Code Regs. tit. 11, § 7070(c); CCPA FSOR at 50.)

When selecting a method, the business can use the verifiable parental consent methods approved under the Children's Online Privacy Protection Act of 1998 (COPPA), such as requiring the parent or guardian to:

- Sign and return a consent form to the business.
- Use a credit card, debit card, or other online payment system that notifies the primary account holder of each discrete transaction.
- Use a toll-free telephone number, video conference, or otherwise communicate in person with trained personnel.
- Produce a form of government-issued identification to compare against databases of that information.

(Cal. Code Regs. tit. 11, § 7070(a)(2); CCPA FSOR at 50, CCPA ISOR at 34.)

For more on obtaining verifiable parental consent, see Practice Note, Children's Online Privacy: COPPA Compliance: Verifiable Parental Consent.

Responding to Anonymous or Pseudonymous Consumer Requests

The CCPA Regulations clearly state that a business does not need to provide or delete deidentified consumer information in response to a consumer request. The business also does not need to reidentify individual data to verify a consumer request. (Cal. Code Regs. tit. 11, § 7060(f); CCPA FSOR at 46, CCPA ISOR at 30.) However, ambiguity about the scope of this exemption remains and how it may apply to real-world situations using anonymous or pseudonymous data, like online behavioral advertising (OBA) profiles.

The CCPA's definition of deidentified information is narrow, specific, and does not apply if the "deidentified" information is reasonably capable of directly or indirectly being associated with or linked to a particular consumer (see Box, Deidentified or Aggregated Consumer Information). The CCPA also explicitly includes unique personal and online identifiers and consumer profiles reflecting behavior as personal information. Given this, strong arguments exist that unique but "anonymous" profiles do not qualify for the deidentified consumer information exceptions (Cal. Civ. Code §§ 1798.140(o)(1)(A) to (K), and 1798.140(x); see Box, Personal Information Categories).

The CCPA Regulations do not clearly address this dichotomy. One of the verification examples provided involves personal information not associated with a named actual person, but with a non-account based mobile application. The example required the business to verify the requestor's identity using other facts and circumstances, such as asking for information only the application user was likely to know or requiring the consumer's response to a device notification (Cal. Code Regs. tit. 11, § 7062(e)(2); CCPA FSOR at 47, CCPA ISOR at 32 to 33).

Businesses holding unique and individualized profiles should carefully consider what methods they can technically use to provide the CCPA's access and deletion rights to those profiled individuals. However, when no reasonable method to verify a requestor's identity to the appropriate degree of certainty truly exists, the CCPA Regulations do permit denial of the request (see General Verification Considerations).

Responding to Non-Verified Requests

While a business must deny requests to know or delete when it cannot verify the requestor's identity, it must still respond to the consumer and describe the reasons for denying the request (Cal. Code Regs. tit. 11, § 7024(a), (b) and 7022(a)).

The CCPA Regulations also establish several fallback positions when the business cannot verify a request to the required standard (see General Verification Considerations). A business must:

- Evaluate data portability requests that do not meet the higher verification standard as a request to know categories of information (Cal. Code Regs. tit. 11, § 7024(a)) (see Data Portability Responses and Individualized Privacy Notice).
- Direct submitters of unverified requests to know categories of information to its general privacy policy (Cal. Code Regs. tit. 11, § 7024(b)) (see Individualized Privacy Notice and Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies: Privacy Policy).
- If it denies a deletion request and also sells personal information, ask requestors if they want to exercise their personal information sales opt-out right and provide the opt-out notice content or link as part of the response (Cal. Code Regs. tit. 11, § 7022(g)) (see Practice Note, Drafting CCPA and CPRA Notices and Privacy Policies: Opt-Out Right Notice).

Request to Know Substantive Response

The consumer's right to know consists of two related parts:

- A category-based notice about their specific personal information that the business collects, sells, or discloses (see Individualized Privacy Notice).
- A request for the specific pieces of personal information the business holds (see Data Portability Responses).

(Cal. Civ. Code §§ 1798.100, 1798.110, 1798.115, and 1798.130; Cal. Code Regs. tit. 11, §§ 7001(r), 7024, and 7031.)

Businesses must search their records to locate the consumer's personal information in response to a request. This is a broad requirement and includes unstructured records containing personal information, such as paper files.

However, to ease this burden, the CCPA Regulations provide a narrow exception for requests to know. A business is not required to search records not maintained in a searchable or reasonably accessible format for personal information if **all** the following conditions apply:

- It maintains the records containing personal information solely for legal or compliance purposes.
- It does not sell personal information contained in the records or use it for any commercial purpose.
- The request to know response sent to the consumer describes the unsearched categories of records that may contain personal information.

(Cal. Code Regs. tit. 11, § 7024(c); CCPA FSOR at 25 and 26.)

The CCPA limits the scope of the right to know response to personal information collected, sold, or disclosed in the preceding 12 months (Cal. Civ. Code §§ 1798.100(c), (d), 1798.130(a)(2), and 1798.140(y)). This 12-month reference period runs from the request's date of receipt, regardless of the time required to verify the request (Cal. Code Regs. tit. 11, § 7024(h)). For example, a business responding on March 1, 2021 to a request received on February 1, 2021 provides information for the 12-month period preceding the request, February 1, 2020 to January 31, 2021.

CPRA Revisions: Request to Know Substantive Response

The CPRA will eventually replace the CCPA's rigid 12-month look-back limitation for request to know responses with a flexible standard that obligates a

business to provide responses covering a longer time period, unless doing so proves impossible or would involve a disproportionate effort. It charges the California Privacy Protection Agency with adopting regulations that identify when providing responses covering a longer time period would qualify for the impossible or disproportionate effort exception (see CPRA Regulation Tracker). Once the regulations become effective, a business must provide responses covering longer time period unless it qualifies for the regulatory exception.

However, this expanded look-back period only applies to personal information collected on or after January 1, 2022, which consequentially serves as the outer bound for any future CPRA-based request to know responses.

(Cal. Civ. Code § 1798.185(a)(9); Cal. Civ. Code § 1798.130(a)(2)(B) (effective January 1, 2023).)

Individualized Privacy Notice

When a verified consumer requests a category-based disclosure about their personal information, the business's response must disclose, for the preceding 12 months:

- The personal information categories the business collected about them.
- The source categories from which the business collected their personal information.
- The business or commercial purpose for which the business collected or sold their personal information.
- The categories of third parties the business shared their personal information with.
- The personal information categories the business sold about them, if any, and for each identified category, the categories of third parties purchasing their personal information.
- The personal information categories the business disclosed about them for a business purpose, if any, and for each identified category, the categories of third parties receiving their personal information.

(Cal. Civ. Code §§ 1798.110, 1798.115, and 1798.130(a); Cal. Code Regs. tit. 11, § 7024(j); CCPA FSOR at 27 and 28.)

The response must use category descriptions that provide the consumer with a meaningful understanding of the categories listed (Cal. Code Regs. tit. 11, § 7024(k)). As with the privacy policy, the personal information categories must follow the personal information definition's categories that most closely describe the actual personal information involved (Cal. Civ. Code § 1798.130(c); see Box, Personal Information Categories).

To determine whether a particular personal information transfer is a sale or business purpose disclosure, see Distinguish Between Sales and Business Purpose Disclosures.

The business must provide individualized responses specific to the requesting consumer, not generalized information or privacy policy references, unless:

- The response is exactly the same for all individuals; and
- The privacy policy discloses all information required for a request to know response.

(Cal. Code Regs. tit. 11, § 7024(i).)

CPRA Revisions: Individualized Privacy Notice

The CPRA slightly tweaks the individualized disclosure requirements to:

- Change all sales-related references to sales or sharing references (Cal. Civ. Code §§ 1798.110 and 1798.115 (effective January 1, 2023)).
- Replace the term "shares" with the term "discloses" in the third-party category notice requirement, so that notice requirement continues to cover any type of personal information disclosure to a third party and not just the CPRA's new and narrow definition for sharing personal information (Cal. Civ. Code §§ 1798.110(a)(4) and 1798.140(ah) (effective January 1, 2023)).
- Require the notice to list the categories of persons to whom the business disclosed personal information for a business purpose (Cal. Civ. Code §§ 1798.115(a)(3) (effective January 1, 2023)). However, the CCPA Regulations already added this disclosure requirement (Cal. Code Regs. tit. 11, § 7024(j)(6)).
- As with the personal information category descriptions, use the sensitive personal information category descriptions listed in the term's definition (Cal. Civ. Code §§ 1798.130(c) and 1798.140(ae)(1) to (9) (effective January 1, 2023); see Box, CPRA Revisions: New Sensitive Personal Information Categories).

The CPRA also adds an important exception to the business's individualized privacy notice obligation. A business can meet part of its individualized notice obligation by pointing to its public privacy policy, but only if those public disclosures exactly match the individualized disclosures on personal information categories and the business or commercial purpose for collecting, selling, or sharing that personal information (Cal. Civ. Code § 1798.110(b) (effective January 1, 2023). This exception is similar, but not identical, to the privacy

notice exception that the CCPA Regulations provide (Cal. Code Regs. tit. 11, § 7024(i)).

It will also eventually expand the individualized notice to cover a longer time period than just the preceding 12 months (Cal. Civ. Code § 1798.130(a)(2)(B) (effective January 1, 2023); see CPRA Revisions: Request to Know Substantive Response).

Data Portability Responses

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

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

(Cal. Civ. Code § 1798.140(e).)

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

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

(Cal. Civ. Code § 1798.140(e).)

Businesses must also provide derived personal information like inferences generated about a consumer unless a clear exception applies. Recent guidance from the California AG confirms that internal profile inferences generated by analyzing personal information and external inferences obtained from third parties, like a person's "influencer" score, meet the CCPA's collected personal information definition and businesses should disclose them when responding to a consumer's request to know (see California AG Opinion 20-303 (March 10, 2022) and Legal Update, California AG Issues Opinion on Data Inferences and CCPA Consumer Rights). Given the CCPA's statutory requirement for liberal construction to achieve its purposes a business should consider including all the personal information it holds about the consumer when responding to requests unless the CCPA Regulations or a clear CCPA exception support withholding it (Cal. Civ. Code § 1798.194; see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Conflict of Laws and Statutory Interpretation).

If the business denies a data portability request in whole or in part, the response must fully explain the denial reasons, unless prohibited by law. Blanket trade secret or proprietary information assertions are not sufficient (see California AG Opinion 20-303 at 15). If the denial reason only applies to part of the requested information, the business must disclose the remaining information. (Cal. Code Regs. tit. 11, § 7024(e); CCPA FSOR at 27.)

CPRA Revisions: Data Portability

The CPRA confirms and strengthens this data portability right, but questions about its scope may require regulations to clarify. Under the CPRA, a business must disclose any personal information it has collected about a consumer who makes a verifiable request (Cal. Civ. Code §§ 1798.110(a)(5), (b) and 1798.130(a)(3)(A) (effective January 1, 2023)). This includes direct or indirect collections and collections made through or by a service provider or contractor (Cal. Civ. Code § 1798.130(a)(3)(A) (effective January 1, 2023)).

The CCPA's broad definition of collected did not change (Cal. Civ. Code § 1798.140(f) (effective January 1, 2023)).

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

Removing Sensitive Information

Before responding to a consumer's verified data portability request, the business must review the collected personal information and remove the following sensitive information, if present:

- Social Security number (SSN), driver's license number, or other government issued ID number.
- Financial account numbers.
- Health insurance or medical identification numbers.
- Account passwords or security questions and answers.
- Unique biometric data generated from measurements or technical analysis of human characteristics.

(Cal. Code Regs. tit. 11, § 7024(d); CCPA FSOR at 26.)

Because of security concerns, the data portability response should never directly disclose the sensitive information. It should only describe the sensitive information using sufficient detail that allows the consumer to understand exactly what the business collected. For example, if a business collected and maintained a consumer's fingerprint scan, its data portability response does not provide the actual fingerprint scan data. It simply discloses that the business collected the requestor's unique biometric data by using a fingerprint scan. (Cal. Code Regs. tit. 11, § 7024(d); CCPA FSOR at 26.)

CPRA Revisions: Removing Sensitive Information

The CPRA specifically excludes data generated to help the business ensure security and integrity, as the CPRA defines those terms, from data portability responses (Cal. Civ. Code §§ 1798.130(a)(3)(B)(iii) and 1798.140(ac) (effective January 1, 2023)). It also directs the California Privacy Protection Agency to develop regulations defining what information the business must provide when responding to data portability requests, balancing the goals of:

- Maximizing a consumer's right to access relevant personal information.
- Minimizing the delivery of information useless to that consumer, such as system log information and other technical data.

(Cal. Civ. Code § 1798.185(a)(14); see CPRA Regulation Tracker.)

Delivering the Information

The business may deliver the requestor's personal information:

- To password-protected account holders using a secure self-service portal that:
  - contains all the required information the requestor is entitled to receive;
  - uses reasonable data security controls; and
  - complies with the CCPA's verification requirements (see Verifying Using Password-Protected Accounts).
- At the consumer's option:
  - by mail; or
  - electronically.

(Cal. Civ. Code §§ 1798.100(d) and 1798.130(a)(2); Cal. Code Regs. tit. 11, § 7024(g).)

Information provided electronically should be portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit the information to another entity without hindrance (Cal. Civ. Code § 1798.130(a)(2)).

The business must use reasonable security measures when sending personal information to the consumer (Cal. Code Regs. tit. 11, § 7024(f)).

CPRA Revisions: Delivering the Information

The CPRA does not substantively change these delivery requirements, but it does move the sections establishing them (Cal. Civ. Code § 1798.130(a)(2)(A), (3)(A), (B)(iii) (effective January 1, 2023)).

Deletion Request Substantive Response

Unless the CCPA specifically allows a business to retain personal information, it must comply with a consumer's verified request to delete. This requires the business to delete the consumer's personal information from its records and direct its service providers to do the same. (Cal. Civ. Code § 1798.105.)

The CCPA identifies specific business situations that may justify denying a consumer's deletion request (see Business Justifications for Denying Deletion Requests). When a deletion exception only applies to part of the request, the business must:

- Delete the consumer's personal information not covered by the exception from its records and direct its service providers to do the same.
- Restrict use of any personal information not deleted to the specific purpose justifying its retention.

(Cal. Civ. Code § 1798.105(c); Cal. Code Regs. tit. 11, § 7022(f)(2), (3).)

The business can use any of the following personal information deletion methods to comply with the consumer's request:

- Permanently erasing it.
- Deidentifying it.
- Aggregating it.

(Cal. Code Regs. tit. 11, § 7022(b); see Box, Deidentified or Aggregated Consumer Information).

As with requests to know, the business must search their records to locate and delete the consumer's personal

information. This includes back-up or archive systems. However, the business may wait to delete personal information from those systems until the next time it either accesses or restores that data to an active system or uses it for a sale, disclosure, or commercial purpose (Cal. Code Regs. tit. 11, § 7022(c)).

The business's response to the consumer must:

- Inform the requestor whether or not the business complied with the request.
- When denying all or part of a request:
  - explain the denial reason, including the CCPA exception and any conflicts with federal or state law (unless prohibited by law); and
  - provide an opt-out right notice or link whenever the business sells personal information and the requestor has not previously submitted an opt-out request.
- Disclose that it intends to maintain a record of the deletion request for at least 24 months or as otherwise needed to ensure the requestor's personal information remains deleted from the business's records.

(Cal. Code Regs. tit. 11, § 7022(d) to (g).)

For a model deletion request response, see Standard Document, Deletion Request Response Letter (CPRA).

CPRA Revisions: Deletion Request Downstream Notices

The CPRA's deletion right revisions update the business justifications for retention (see CPRA Revisions: Business Justifications for Denying Deletion Requests) and expand the business's obligation to pass the consumer's deletion request on to its service providers. The business must now notify:

- All third parties to whom it has sold or shared the consumer's personal information to delete that information, unless the notification proves impossible or involves disproportionate effort.
- Its service providers and contractors to delete the consumer's personal information from their records.

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

The CPRA obligates service providers and contractors to cooperate with the business and either delete or enable the business to delete the consumer's personal information (Cal. Civ. Code § 1798.105(c)(3) (effective January 1, 2023); see CPRA Revisions: Service Provider and Contractor Responsibility for Consumer Requests). However, service providers and contractors can retain personal information if a permitted business justification exists (Cal. Civ. Code § 1798.105(d) (effective January 1, 2023); see CPRA Revisions: Business Justifications for Denying Deletion Requests).

Business Justifications for Denying Deletion Requests

The CCPA allows a business or service provider to deny a consumer deletion request when it must maintain the consumer's personal information to:

- Either:
  - complete the transaction for which the business collected the personal information;
  - fulfill the terms of a written warranty or product recall conducted under federal law;
  - provide a good or service requested by the consumer or reasonably anticipated within the business's ongoing business relationship with the consumer; or
  - otherwise perform a contract between the business and the consumer.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity.
- Debug to identify and repair errors that impair existing intended functionality.
- Exercise a legal right, including exercising or ensuring free speech rights.
- Comply with the California Electronic Communications Privacy Act (Cal. Penal Code §§ 1546 to 1546.4).
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest if:
  - the research adheres to all other applicable ethics and privacy laws;
  - deleting the personal information is likely to make the research impossible or seriously impair it; and
  - the consumer has provided informed consent.
- Enable internal uses reasonably aligned with the consumer's expectations based on the consumer's relationship with the business.
- Comply with a legal obligation.
- Otherwise use the consumer's personal information internally in a lawful manner that is compatible with the context in which the consumer provided the information.

(Cal. Civ. Code § 1798.105(d).)

CPRA Revisions: Business Justifications for Denying Deletion Requests

The CPRA makes minor revisions to the business justifications for retention that consolidate some justifications, clarify others, and confirm that service providers and contractors can also rely on them (Cal. Civ. Code § 1798.105(d) (effective January 1, 2023)). However, these revisions do not significantly alter the reasons a business may retain a consumer's personal information after that person submits a deletion request.

As reformulated, a business, service provider, or contractor may deny a consumer's deletion request when maintaining that information is reasonably necessary to:

- Either:
  - complete the transaction for which it collected the personal information;
  - fulfill the terms of a written warranty or product recall conducted under federal law;
  - provide a good or service that the consumer requested or reasonably anticipated within the context of the consumer's ongoing relationship with the business; or
  - otherwise perform a contract between the business and the consumer.
- Help ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes. The CPRA defines security and integrity to mean the ability of:
  - networks or information systems to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information;
  - businesses to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions and to help prosecute those responsible for those actions; and
  - businesses to ensure the physical safety of natural persons (Cal. Civ. Code § 1798.140(ac) (effective January 1, 2021)).
- Debug to identify and repair errors that impair existing intended functionality.
- Exercise a legal right, including exercising or ensuring free speech rights.
- Comply with the California Electronic Communications Privacy Act (Cal. Penal Code §§ 1546 to 1546.4).
- Engage in public or peer-reviewed scientific, historical, or statistical research if:
  - the research confirms or adheres to all other applicable ethics and privacy laws;
  - deleting the personal information is likely to make the research impossible or seriously impair the ability to complete it; and
  - the consumer has provided informed consent.
- Enable internal uses that are:
  - reasonably aligned with the consumer's expectations based on the consumer's relationship with the business; and
  - compatible with the context in which the consumer provided the information.
- Comply with a legal obligation.

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

The CPRA also allows the business to maintain a confidential record of deletion requests to prevent the requesting consumer's personal information from being sold, for legal compliance purposes, or as the CPRA may otherwise permit (Cal. Civ. Code § 1798.105(c)(2) (effective January 1, 2023).)

The California Privacy Protection Agency may provide further guidance or regulations on when a business, service provider, or contractor may retain personal information after receiving a deletion request (Cal. Civ. Code § 1798.185(a)(7); see CPRA Regulation Tracker).

CPRA Revisions: Correction Request Substantive Response

A business must use commercially reasonable efforts to correct any inaccurate personal information that the verified consumer request identifies (Cal. Civ. Code § 1798.106(c) (effective January 1, 2023)). While this right is not absolute and must take the personal information's processing purposes and general nature into account, the CPRA doesn't directly set its boundaries (Cal. Civ. Code § 1798.106(a) (effective January 1, 2023)). Instead, it directs the California Privacy Protection Agency to develop regulations governing correction requests, including:

- How a business should respond.
- How often a consumer can make correction requests.
- What exceptions should exist, for example, when responding to a request proves impossible or involves

disproportionate effort, or the consumer improperly seeks correction of accurate information.

- How to resolve concerns about the information's accuracy.
- What steps a business may take to prevent fraud.
- Allowing a consumer to provide a written addendum of 250 words or less to any record concerning their health if a business rejects a correction request.

(Cal. Civ. Code § 1798.185(7), (8).)

Businesses should monitor the California Privacy Protection Agency's rulemaking process to understand its correction request response obligations (see CPRA Regulation Tracker).

Service providers and contractors must assist their business with responding to correction requests, including by directly correcting or enabling the business to correct inaccurate information (Cal. Civ. Code § 1798.130(a)(3)(A) (effective January 1, 2023)).

Responding to Sales Opt-Out and Opt-In Requests

Consumers age 16 or older 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. Once the business receives a consumer's opt-out request, it must respond and comply within specific timeframes (see Response Timeframes and Downstream Notices).

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

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

(Cal. Civ. Code § 1798.120(c) to (d); see Obtaining Opt-In Consent for Minors.)

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

Once a consumer submits an opt-out request or refuses to provide opt-in consent, the business must honor the request unless that consumer provides express authorization to resume personal information sales (Cal. Civ. Code §§ 1798.120(d) and 1798.135(a)(4)) (see Request to Restart Personal Information Sales). To determine whether a disclosure is a sale under the CCPA, see Distinguish Between Sales and Business Purpose Disclosures.

The CCPA contains a narrow exception to this personal information sales restriction right for vehicle or ownership information retained or shared between a new car dealer and the vehicle's manufacturer solely to enable warranty or recall related repairs (Cal Civ. Code § 1798.145(g)). Recent amendments, effective January 1, 2022, will expand this exception to include vessel information, dealers, and manufactures (AB 335 (2021-2022); see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Vehicle and Vessel Information Exception).

CPRA Revisions: Responding to Sharing Opt-Out and Opt-In Requests

The CPRA expands the CCPA's personal information sales opt-out and opt-in rights to include sharing personal information with a third party for cross-context behavioral advertising purposes (Cal. Civ. Code §§ 1798.120 and 1798.140(ah) (effective January 1, 2023)). The requirements to opt-out of sharing or obtain consent to share personal information of a consumer age 15 or younger mirror the sales opt-out and opt-in requirements (Cal. Civ. Code §§ 1798.120 and 1798.135 (effective January 1, 2023)).

The CPRA also alters the CCPA's sales definition to clearly exclude disclosures made to service providers or contractors (Cal. Civ. Code § 1798.140(ad), (ai) (effective January 1, 2023)). To determine whether a disclosure results in the sale or sharing of personal information, see Distinguish Between Sales and Business Purpose Disclosures and CPRA Revisions: Sales Definition).

Verifying Opt-Out Requests and Authorized Agents

The CCPA Regulations clarify that, unlike requests to know or requests to delete, consumers do not need to verify their identity to make a personal information sales opt-out request. However, businesses can deny opt-out requests if they have a good-faith, reasonable, and documented belief that the request is fraudulent. The business must explain its denial decision to the requestor. (Cal. Code Regs. tit. 11, § 7026(g); CCPA FSOR at 40, CCPA ISOR at 25 to 26.)

Consumers may also use an authorized agent to make opt-out requests. A business may require proof that the consumer authorized the agent, including providing the consumer's signed, written permission. Signed permissions include both physical signatures and electronic signatures under the Uniform Electronic Transaction Act. (Cal. Code Regs. tit. 11, §§ 7001(u) and 7026(f); CCPA FSOR at 40, CCPA ISOR at 25.)

Importantly, the CCPA Regulations explicitly state that user-enabled global privacy controls, like browser-based or device setting signals, are considered direct consumer requests, not requests from an authorized agent (Cal. Code Regs. tit. 11, § 7026(f); see Opt-Out Request Submission Methods and Extra Submission Requirement for Online Personal Information Collection).

Response Timeframes and Downstream Notices

The CCPA Regulations set a maximum timeframe of 15 business days to stop selling a consumer's personal information after receiving an opt-out request. However, businesses must still act on the request as soon as feasibly possible. (Cal. Code Regs. tit. 11, § 7026(e).)

The CCPA Regulations also require:

- Businesses to notify downstream recipients receiving personal information between the opt-out request submission date and its completion date that they should not sell that consumer's personal information (Cal. Code Regs. tit. 11, § 7026(e)).
- Service providers to stop selling personal information on its business customer's behalf when a consumer submits an opt-out request to the business (Cal. Code Regs. tit. 11, § 7051(d)) (see Service Provider Responsibility for Consumer Requests).

The business must establish processes to stop personal information sales and provide these downstream notices. While the particular requirements vary for each business, key considerations may include:

- Creating automated notice systems from contract management systems.
- Establishing checklists with required actions based on the business's data map results (see Data Maps).
- Conducting strategic reviews of all personal information sales to eliminate marginal or low-value disclosures, to streamline the business's compliance burden.
- Reviewing and altering third-party arrangements so they comply with the CCPA's service provider requirements and qualify for the sales exception (see Service Provider Exception).

For more on determining when a disclosure is a sale under the CCPA, see Distinguish Between Sales and Business Purpose Disclosures.

CPRA Revisions: Response Timeframes and Downstream Notices

While the CPRA does not directly require businesses to pass on a consumer's opt-out request, it creates a strong incentive for them to do so. When a business communicates a consumer's opt-out request to a person it authorized to collect personal information, the CPRA absolves it of any liability if that person does not follow the CPRA's sales or sharing restrictions, unless the business actually knew or had reason to believe the person intended to commit the violation (Cal. Civ. Code § 1798.135(g) (effective January 1, 2023)).

The CPRA also requires the person receiving that business's downstream notice of the consumer's opt-out request to only use that consumer's personal information for the specified business purposes or as the CPRA otherwise permits, and prohibits the person from:

- Selling or sharing the consumer's personal information.
- Retaining, using, or disclosing the consumer's personal information:
  - for any purpose except the specific purpose of performing the services offered to the business;
  - outside of the direct business relationship between the person and the business; or
  - for a commercial purpose other than providing services to the business.

(Cal. Civ. Code § 1798.135(f) (effective January 1, 2023).)

Obtaining Opt-In Consent for Minors

A business with actual knowledge that it sells personal information about consumers under age 16 must establish, document, and follow reasonable processes for:

- Ensuring that these sales do not occur unless it receives the required opt-in consent for that consumer.
- Verifying that the person providing consent to personal information sales for a consumer under age 13 is that child's parent or guardian (see Verifying Parental Consent).
- Obtaining opt-in consent for personal information sales from consumers between ages 13 and 15 using

a two-step affirmative opt-in process, where the consumer must:

- clearly submit a personal information sales opt-in request; and
- separately confirm their opt-in request.

- Providing the personal information sales opt-in requestor with notice about:
  - their personal information sales opt-out right at a later date; and
  - how to exercise that right.

(Cal. Civ. Code § 1798.120(c), (d); Cal. Code Regs. tit. 11, §§ 7070 and 7071.)

While a business may use one of COPPA's verifiable parental consent methods (see Verifying Parental Consent), it must obtain a separate CCPA-related consent for personal information sales and cannot rely on a prior consent granted for COPPA compliance (Cal. Code Regs. tit. 11, § 7070(a)(1); CCPA FSOR at 49, CCPA ISOR at 34).

The business's privacy policy must include a description of its opt-in consent processes when the business targets consumers age 15 or under (Cal. Code Regs. tit. 11, § 7072(a)).

During development of the CCPA Regulations, some children-focused businesses were concerned that requiring them to post "Do Not Sell My Personal Information" links or other opt-out right notices may inadvertently cause confusion if parents mistook those statements to mean that the business intended to sell their child's personal information unless they take action (CCPA ISOR at 36). To avoid this potential confusion, the CCPA Regulations allow a business to avoid posting those links or notices if it both:

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

(Cal. Code Regs. tit. 11, § 7072(b); CCPA ISOR at 36.)

Request to Restart Personal Information Sales

The CCPA Regulations require businesses to use a two-step process to re-enroll consumers opting out of personal information sales. Once the consumer submits a clear opt-in request, the business should separately ask the consumer to confirm their opt-in choice. (Cal. Code Regs. tit. 11, § 7028(a).)

The CCPA requires businesses to wait at least 12 months before asking the consumer to reauthorize future personal information sales (Cal. Civ. Code § 1798.135(a)(5)). However, when a consumer initiates a transaction or attempts to use a product or service requiring the sale of their personal information, the CCPA Regulations do allow the business to tell consumers about the sale requirement and provide instructions to opt back in (Cal. Code Regs. tit. 11, § 7028(b); CCPA FSOR at 40, CCPA ISOR at 26).

CPRA Revisions: Repeating Personal Information Sales or Sharing Requests for Minors

The CPRA requires business to wait at least 12 months or until the person turns 16 before repeating an opt-in request that would allow the business to sell or share the minor's personal information (Cal. Civ. Code § 1798.135(c)(5) (effective January 1, 2023)).

CPRA Revisions: Responding to Sensitive Personal Information Limitation Requests

When a consumer asks the business to limit the use and disclosure of their sensitive personal information, the business can only use that information to:

- Perform services or provide goods that an average consumer requesting those goods or services would reasonably expect.
- Help ensure security and integrity, as the CPRA defines those terms, 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.

(Cal. Civ. Code §§ 1798.121(a), (b) and 1798.140(e)(2), (4), (5), (8), (ac) (effective January 1, 2023).)

The California Privacy Protection Agency may adopt regulations that expand or alter the statutorily permitted activities (Cal. Civ. Code § 1798.185(a)(19)(C); Cal. Civ. Code § 1798.121(a) (effective January 1, 2023); see CPRA Regulation Tracker).

Importantly, this restriction right does not apply to sensitive personal information that the business collected or processed **without** the purpose of inferring characteristics about a consumer (Cal. Civ. Code § 1798.121(d) (effective January 1, 2023)). Regulations developed by the California Privacy Protection Agency should further define when a business collects or processes information without such as purpose (Cal. Civ. Code § 1798.185(a)(19)(C); Cal. Civ. Code § 1798.121(d) (effective January 1, 2023); see CPRA Regulation Tracker). For more on how the CPRA defines sensitive personal information, including the specific categories, see Box, CPRA Revisions: New Sensitive Personal Information Categories.

The CPRA generally aligns a business's response obligations for this new limitation right with the rights to opt-out of personal information sales and sharing (Cal. Civ. Code § 1798.135 (effective January 1, 2023); see Responding to Sales Opt-Out and Opt-In Requests). After receiving a limitation request, the business must obtain the consumer's consent to use their sensitive personal information for any purpose that falls outside of the statutorily permitted ones (Cal. Civ. Code § 1798.121(b) (effective January 1, 2023)). However, as with personal information sales and sharing opt-out requests, the business must wait at least 12 months before making those additional use requests (Cal. Civ. Code § 1798.135(c)(4) (effective January 1, 2023)).

The CPRA does not provide businesses with a grace period to stop using sensitive personal information for non-statutory purposes—the prohibition begins after receipt of the consumer's direction—and it does not require a verifiable request (Cal. Civ. Code §§ 1798.121(b) and 1798.140(ak) (effective January 1, 2023)). However, the California Privacy Protection Agency may establish rules and procedures that provide businesses with more response flexibility, such allowing them to inform consumers about the potential consequences of limiting sensitive personal information use (Cal. Civ. Code § 1798.185(a)(4), (19)(C); see CPRA Regulation Tracker).

While the CPRA does not directly require businesses to pass a consumer's limitation direction along to service providers or contractors, it does directly prohibit service providers or contractors from using personal information obtained through the relationship that it actually knows is sensitive for any other purpose once it receives the business's limitation instruction (Cal. Civ. Code § 1798.121(c) (effective January 1, 2023)).

Service Provider Responsibility for Consumer Requests

Service providers that receive a request to know or delete from a consumer must either:

- Act on the business's behalf in responding to the request.
- Inform the consumer that it cannot act on the request because it is a service provider.

(Cal. Code Regs. tit. 11, § 7051(e); CCPA FSOR at 35 and 36.)

Service providers also cannot sell a consumer's personal information for a business once that consumer submits a personal information sales opt-out request to that business (Cal. Code Regs. tit. 11, § 7051(d); CCPA FSOR at 35).

For more on qualifying personal information transfers for the service provider sales exception, see Service Provider Exception.

For more on service providers and third parties generally, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Service Providers and Third Parties. For required contract clauses, see Standard Clause, CCPA Contract Clauses for Service Providers.

CPRA Revisions: Service Provider and Contractor Responsibility for Consumer Requests

The CPRA provided much needed clarifications on a service provider's role and responsibilities, creating

direct contract obligations and imposing direct assistance obligations. It also created a new entity type, a contractor, whose responsibilities under the CPRA are nearly identical to service providers (Cal. Civ. Code § 1798.140(j) (effective January 1, 2023)).

Consumers cannot require service providers and contractors to directly respond to a verifiable request to exercise their CPRA rights (Cal. Civ. Code §§ 1798.105(c)(3) and 1798.130(a)(3)(A) (effective January 1, 2023)). However, the CPRA now directly obligates service providers and contractors to help the business respond to consumer rights requests by, for example:

- Providing personal information in its possession obtained through the business relationship that a response to know or data portability request should include (Cal. Civ. Code § 1798.130(a)(3)(A) (effective January 1, 2023)).
- Deleting or allowing the business to delete personal information and notifying the service provider's or contractor's downstream entities about the consumer's deletion request (Cal. Civ. Code §§ 1798.105(c)(3) (effective January 1, 2023)).
- Correcting or enabling the business to correct a consumer's inaccurate information (Cal. Civ. Code § 1798.130(a)(3)(A) (effective January 1, 2023)).
- Limiting sensitive personal information use upon the business's instruction (Cal. Civ. Code § 1798.121(c) (effective January 1, 2023)).

For more on service providers and contractors, 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.

Distinguish Between Sales and Business Purpose Disclosures

Providing the individualized privacy notice and honoring the consumer's opt-out and opt-in rights requires the business to determine whether personal information transfers to another entity are:

- Sales, which consumers can stop (see Personal Information Sales).
- Disclosures for a business purpose (see Business Purposes).

When sharing personal information qualifies as a business purpose disclosure instead of a sale, the business:

- Can classify it as a disclosure for a business purpose when responding to requests to know (see Individualized Privacy Notice).
- Does not need to stop sharing the personal information or provide downstream notices when it receives an opt-out right request (see Response Timeframes and Downstream Notices).
- Does not need opt-in consent to share personal information from a consumer under age 16 (see Obtaining Opt-In Consent for Minors).

If the business can properly classify all of its transfers as business purpose disclosures, it may be able to avoid the CCPA's requirements for businesses that sell personal information entirely, including "Do Not Sell My Personal Information" notices and links.

Personal Information Sales

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

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

The term "sale" includes actions, such as:

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

(Cal. Civ. Code § 1798.140(t)(1).)

A recent California AG enforcement action found that a business sells consumers' personal information when

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

The CCPA's sale definition contains four exceptions:

- Service providers (see Service Provider Exception).
- Consumer requests (see Consumer-Directed Transfer Exception).
- Honoring sale opt-out requests (see Honoring Opt-Out Requests Exception).
- Mergers and acquisitions (see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Mergers and Acquisitions Exception).

(Cal. Civ. Code § 1798.140(t)(2).)

CPRA Revisions: Sales Definition

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

- The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the business.
- A service provider to the business.
- A contractor.

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

Service Provider Exception

The CCPA treats sharing personal information with qualified service providers as a business purpose disclosure instead of a sale. However, to qualify for the exception, a business must meet all of the following conditions:

- Sharing or using personal information with the service provider is necessary to perform a business purpose, as defined by the CCPA (see Business Purposes).
- The business disclosed that it uses or shares personal information with a service provider in required CCPA notices.
- The service provider does not further collect, sell, or use the consumers' personal information, except as necessary to perform the business purpose.
- The business entered into a written contract with the service provider containing required clauses (see Standard Clause, CCPA Contract Clauses for Service Providers).

(Cal. Civ. Code § 1798.140(t)(2)(C), (v); Cal. Code Regs. tit. 11, § 7051.)

Qualifying an entity that the business shares personal information with as a service provider can significantly streamline its CCPA compliance obligations, particularly around the personal information sales opt-out and opt-in rights (Responding to Sales Opt-Out and Opt-In Requests).

For more on the CCPA's service provider requirements and obligations, see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Service Providers and Third Parties.

CPRA Revisions: Service Provider and Contractor Exception

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

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

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

So while the CPRA removes the CCPA's current service provider exclusion from the sales definition (Cal. Civ. Code §1798.140(t)(2)(C)), it retains the exception through a different statutory formulation. These definition changes should also simplify the business's process for responding to consumer rights requests since providing personal information to service providers and contractors under a CPRA-compliant contract should always qualify as a disclosure for a business purpose.

Consumer-Directed Transfer Exception

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

- The consumer intentionally requests the action by deliberate interaction. Interactions like hovering over, muting, pausing, or closing a piece of content do not indicate a consumer's intent.

- The third party does not further sell the personal information using a disclosure inconsistent with the CCPA.

(Cal. Civ. Code § 1798.140(t)(2)(A).)

CPRA Revisions: Consumer-Directed Transfer Exception

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

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

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

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

Honoring Opt-Out Requests Exception

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

CPRA Revisions: Honoring Opt-Out Requests Exception

The CPRA kept this exception in place and expanded it to cover informing others about consumer requests to exercise the CPRA's new right to limit use of their sensitive personal information (Cal. Civ. Code § 1798.140(ad)(2)(B) (effective January 1, 2023)).

Business Purposes

A business uses personal information for a business purpose if the use is both:

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

(Cal. Civ. Code § 1798.140(d).)

The CCPA identifies seven types of approved business purposes (Cal. Civ. Code § 1798.140(d)(1) to (7); see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): Business Purposes). 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. The CCPA Regulations do not directly address this ambiguity.

CPRA Revisions: Business Purposes

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

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

- The business's operational purposes.
- The business's other notified purposes.
- The service provider's or contractor's operational purposes, as defined by regulations that the California Privacy Protection Agency will adopt (Cal. Civ. Code § 1798.185(a)(11); see CPRA Regulation Tracker).

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

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

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

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

The statute goes on to list eight specific business purposes ((Cal. Civ. Code § 1798.140(e)(1) to (8) (effective January 1, 2023); see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): CPRA Revisions: Business Purposes). While it remains unclear whether this statutory list merely provides examples of business purposes or restricts the term to just those activities, the definition's reference to a business's "other notified purposes" indicates that the

term should cover any purpose the business disclosed in its collection notices. Future CPRA regulations may address this issue. However, the revised definition does clarify that service providers and contractors only use personal information for a business purpose when the use is for their operational purposes, which future CCPA regulations should define. The CPRA does not contain a definition for the term operational purposes.

Training and Recordkeeping Obligations

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

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

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

When maintaining CRR Records, the business must:

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

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

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

For a list compiling the general recordkeeping or documentation obligations found in other CCPA Regulation sections, see Practice Note, Understanding the California Consumer Privacy Act (CCPA): CCPA Regulations Required Documentation List.

CPRA Revisions: Training Obligations

The CPRA extends the CCPA's training obligation to include the new CPRA consumer rights. A business must ensure that all individuals responsible for handling consumer inquiries about its privacy practices or CPRA compliance understand the CPRA's consumer rights and know how to direct consumers to exercise them (Cal. Civ. Code §§ 1798.130(a)(6) and 1798.135(c)(3) (effective January 1, 2023)).

Metrics for Large Businesses

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

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

- For each request type (requests to know, requests to delete, and opt-out requests), 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.)

Optionally, the large businesses may:

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

business can provide consumer-only CRR Metrics to the California AG.

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

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

Business that meet the large business thresholds should establish programs to track and tabulate these metrics.

Key Definitions

Personal Information

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

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

(Cal. Civ. Code § 1798.140(o)(1).)

The CCPA lists specific examples of potential personal information, such as internet protocol (IP) addresses, but the statute also emphasizes that each data example must actually identify, relate, describe, or reasonably associate or link, directly or indirectly, to a particular individual or household before it qualifies as personal information. The examples list also breaks the definition down into 11 different personal information categories (see Box, Personal Information Categories).

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

- Residing at the same address.
- Sharing a common device or the business's service.
- Using the same group account or unique identifier.

(Cal. Code Regs. tit. 11, § 7001(k).)

Personal information does not include:

- Information lawfully made available from government records.
- Deidentified or aggregate consumer information (see Box, Deidentified or Aggregated Consumer Information).

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

CPRA Revisions: Personal Information

The CPRA does not change the CCPA's current personal information definition, but it does add a new category for sensitive personal information (Cal. Civ. Code § 1798.140(v)(1) (effective January 1, 2023; see Box, CPRA Revisions: New Sensitive Personal Information Categories)). It also broadens the exclusion for publicly available information (Cal. Civ. Code § 1798.140(v)(2) (effective January 1, 2023); see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA): CPRA Revisions: Publicly Available Information).

Personal Information Categories

The CCPA's statutory personal information definition provides a list of 11 personal information categories with examples, highlighting that they only apply if 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 SSN;
  - a driver's license or passport number; or
  - another form of persistent or probabilistic identifier that can identify a particular consumer, family, or device.
- Personal information categories described in the California Customer Records statute, which, in addition to the identifiers described above, also lists a person's:
  - signature;
  - state identification card number;

  - physical characteristics or description;
  - insurance policy number;
  - education;
  - employment or employment history;
  - bank account number, credit card number, debit card number, or any other financial information; or
  - medical information or health insurance information.

  (Cal. Civ. Code § 1798.80(e).)
- Characteristics of protected classifications under California or federal law, like race, national origin, religion, gender, or sexual orientation (see State Q&A, Anti-Discrimination Laws: California).
- Commercial information, including records of personal property and purchasing habits.
- Biometric information, including genetic, physiological, behavioral, and biological characteristics, or activity patterns from which organizations can extract a template or other identifier or identifying information, such as:
  - fingerprints, faceprints, and voiceprints;
  - iris or retina scans;
  - keystroke, gait, or other physical patterns; and
  - sleep, health, or exercise data.
- Internet or other similar network activity, including:
  - browsing history;
  - search history; or
  - information regarding a consumer's interaction with an internet website, application, or advertisement.
- Geolocation data.
- Audio, electric, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.
- Non-publicly available educational information as defined under the Family Educational Rights and Privacy Act (FERPA) and related regulations (20 U.S.C. § 1232g; 34 C.F.R. §§ 99.1 to 99.67).
- Inferences drawn from other personal information to create consumer profiles reflecting:
  - preferences;
  - characteristics;
  - psychological trends;
  - predispositions;
  - behavior;
  - attitudes;
  - intelligence;
  - abilities; or
  - aptitudes.

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

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

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

(Cal. Civ. Code § 1798.175.)

CPRA Revisions: New Sensitive Personal Information 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).

Deidentified or Aggregated Consumer Information

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

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

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

  (Cal. Civ. Code § 1798.140(a).)

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

The CCPA establishes separate requirements for deidentifying 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 or Aggregated Consumer Information

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

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

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

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