

Alert | Data, Privacy & Cybersecurity



July 2022

Businesses Beware: Proposed Amendments to the CCPA Regulations Will Increase Cost of Doing Business in California

This GT Alert covers the following:

- A summary of the key draft amendments to the CCPA regulations proposed by the California Privacy Protection Agency.
- The timeline for submitting comments on the proposed amendments to the CCPA regulations.
- The rulemaking process for finalizing the proposed amendments.


On July 8, 2022, the California Privacy Protection Agency (CPPA) issued proposed amendments to the California Consumer Privacy Act (CCPA) regulations to harmonize them with the California Privacy Rights Act of 2020 (CPRA), which will go into effect on Jan. 1, 2023. Individuals or companies have until Aug. 23, 2022, at 5 p.m. to submit comments to the proposed amendments, and a hearing on the proposed amendments will be held on Aug. 24 and 25. Thereafter, the CPPA will have 30 business days to review the comments and publish any changes to the proposed CPRA amendments to the CCPA regulations. If the CPPA's changes are substantial and sufficiently related to the current text, another 15-day comment period will begin, and if the changes are major, another 45-day comment period will

commence. If the agency chooses to enact the rules without such changes, the rules could be finalized by the end of 2022. See [California Rulemaking Chart](#).

Even though several of the CPRA requirements are not addressed in the proposed CPRA amendments, the amendments are substantial and will likely require businesses to expend considerable time and resources to come into compliance, even those businesses that are already compliant with the CCPA. Below is an overview of the key proposed CPRA amendments to the CCPA regulations.

1. Sharing, Selling, and Opt-Out Preference Signals

Sharing & Selling Procedures. The CPRA builds on the CCPA’s consumer right to opt-out of the sale of their personal information by extending it to cover the “sharing” of personal information with third parties—which, unlike “selling,” does not require the presence of any type of bargained-for valuable consideration. In general, a consumer’s ability to exercise this right may be presented through a website header or footer link that is clearly and conspicuously labeled “Do Not Sell or Share My Personal Information” (or separate individual links to this effect). The proposed amendments confirm at § 7013(a) that the purpose of this link “is to immediately effectuate the consumer’s right to opt-out of sale/sharing, or in the alternative, direct the consumer to the notice of right of opt-out of sale/sharing,” such as a webpage where the consumer can learn about and make that choice. This inclusion may suggest that businesses will have some operational flexibility in this regard in relation to their websites.

The proposed amendments also provide for businesses to optionally use a single, clearly labeled “alternative opt-out link,” which allows consumers to easily exercise their right to opt-out of sale/sharing and limit the use of their sensitive personal information, instead of using website hyperlinks to that effect. Such a link would need to be titled “Your Privacy Choices” or “Your California Privacy Rights,” and would include the following opt-out icon:  .

Opt-Out Preference Signals. Section 1798.135(b) of the CPRA provides that a business can omit a “Do Not Sell or Share My Personal Information” link if it allows consumers to opt-out of the selling or sharing of their personal information (as well as to limit the use of their sensitive personal information) “through an opt-out-preference signal.” The proposed amendments add a new definition for “opt-out preference signal,” which means a signal sent by a “platform, technology, or mechanism, on behalf of the consumer,” that communicates the consumer’s choice to opt-out of the sale and sharing of personal information. If a business processes an opt-out preference signal “in a frictionless manner,” the link will not be required, but the business must still post a notice of the right to opt-out of sale and sharing. Section 7025(f) of the proposed amendments define “frictionless manner” to mean that when a consumer opts-out, a business shall not (1) charge a fee; (2) alter a consumer’s experience (for example, a consumer who opts-out should have the same functional product experience as one who does not opt-out); or (3) display a notification, sound, video, or other such response to the opt-out preference. An example of an opt-out preference signal that the California Office of the Attorney General has endorsed is the Global Privacy Control.

The proposed amendments describe opt-out preference signals in more detail at § 7025, including that businesses may not require a consumer to provide additional information beyond what is necessary to send the signal, but that they may optionally allow consumers to provide more information to facilitate the opt-out request, such as to provide more information “so that the request to opt-out of sale/sharing can apply to offline sale or sharing of personal information.” Further, a business “should display whether or not it has processed the consumer’s opt-out preference signal,” such as through explicit reference to the opt-out signal being honored or through a toggle or radio button.

Non-Traditional Online Environments. As an interesting aside reflecting an attempt to potentially account for non-traditional online environments—such as the “metaverse”—the proposed amendments also hold that a business that sells or shares personal information that is collected “in augmented or virtual reality, such as through gaming devices or mobile applications,” must provide notice of the right to opt-out of sale or sharing in a manner that ensures that the consumer will encounter the notice while in such environments.

2. No Dark Patterns

The proposed amendments specifically address the use of dark patterns. The amendments establish that “a user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decision-making, or choice, *regardless of the business’s intent*” (emphasis added). The amendments clarify that any agreement obtained through the use of dark patterns may not constitute a consumer consent, such that, for example, “a business that uses dark patterns to obtain consent from a consumer to sell their personal information shall be in the position of never having obtained the consumer’s consent to do so.”

Businesses, therefore, should be mindful of how they design and implement methods for submitting consumer requests or obtaining consent, making them easy to understand, providing symmetry in choice, avoiding confusing interactive elements, and avoiding manipulative language or choice architecture, as further detailed in § 7004. This emphasis is in line with [recent guidelines issued by the European Data Protection Board](#) and a workshop and [policy statement issued by the Federal Trade Commission](#) warning companies against deploying illegal dark patterns that trick or trap consumers into subscription services.

3. Consumer Rights Requests

Right to Correct Inaccurate Personal Information. The proposed amendments add a new section introducing obligations for the CPRA’s right to correct inaccurate personal information, including considerations for determining the accuracy of the contested personal information, methods for correction, documentation requirements, grounds, disclosure requirements for denial, and alternative solutions (*see, e.g.*, § 7023). Although these may be familiar measures for businesses subject to the GDPR, they may be new for companies solely used to complying with the CCPA or federal sectoral legislation.

Before complying with a correction request, businesses must first determine the accuracy of the contested personal information (§ 7023(b)). The determination should be based on the totality of the circumstances, including:

- the nature of the personal information;
- how the business obtained the contested information; and
- documentation relating to the accuracy of the information (§ 7023(b)(1)).

If the business is not the source of the personal information and lacks any documentation supporting the contested information’s accuracy, the business, after verifying and authenticating the consumer’s identity, should correct the information based on the consumer’s assertion (§ 7023(b)(2)). The proposed amendments require that businesses, when they are not the source of the inaccurate information, provide consumers with the name of its inaccurate data source (such as a data broker) (§ 7023(i)). This requirement may be burdensome and difficult to comply with for businesses without a data inventory or data mapping program, especially those that regularly receive data in bulk from data brokers or other third parties.

A business must also instruct its service providers and contractors to make the necessary corrections in their respective systems (§ 7023(c)). In responding to the correction request the business must inform the consumer whether it has complied with the request (§ 7023(f)).

Rather than correct the personal information, a business may choose to delete the contested information if the deletion does not negatively impact consumers (i.e., impacting the consumer's opportunity to obtain a job, housing, credit, or education), or the consumer consents to the deletion (§ 7023(e)). The proposed amendments also account for exceptions to complying with a correction request and the information that must be provided to a consumer if the business does so.

Right to Delete. Section 1798.105(c)(1) of the CPRA expands the obligation to pass deletion requests on to service providers, contractors, and, unless impossible or it involves disproportionate effort, to all third parties to whom the business sold or shared the personal information. The proposed amendment regulations further clarify that the impossibility and disproportionate effort must be supported by detailed factual explanations (§ 7022(b)(3)).

To reflect this expansion, the proposed amendments include new sections to address and operationalize these additional obligations, requiring businesses to notify relevant service providers, contractors, and third parties as part of complying with a deletion request (§ 7022(b)).

The proposed amendments at § 7022 further specifies what is required of service providers and contractors who have received deletion requests from businesses. For example, a service provider or contractor can comply with a deletion request by either permanently erasing the personal information on its existing systems, de-identifying the personal information, or aggregating it. Similarly, service providers and contractors can delay compliance with the deletion request for information stored on archived or backup systems. To effectuate a consumer's deletion request, the proposed amendments make clear that service providers and contractors are obligated to pass along that deletion request to their own service providers, contractors, and any third parties that may have accessed the personal information.

Verification of Requests. The proposed amendments at § 7060 require businesses to implement a method for verifying consumer requests to correct, as was required in relation to CCPA requests to know and delete. In relation to the newly offered right to correct, the proposed amendments establish a general rule requiring businesses to complete the verification based on the information that is not the subject of the correction request.

In contrast, businesses should not require a consumer to verify their identity when making a request to opt-out of sale or sharing, or requests to limit the use and disclosure of sensitive personal information. However, this does not mean that the business may not ask for additional information from the requesting consumers when handling requests to opt out of sale or sharing, and requests to limit the use and disclosure of sensitive personal information. Businesses must limit the additional information collection to the extent that it is necessary to complete the request and not overly burdensome on the consumer. According to the example given by the proposed amendments, asking for IDs, such as a driver's license, would be considered a burdensome request.

Authorized Agent. The proposed amendments clarify at § 7063 that businesses, when designing and implementing methods for consumers to use authorized agents to submit their rights requests, may not de facto correlate the usage of authorized agents with the power of attorney requirement. If consumers would like to engage authorized agents to act on their behalf, businesses cannot require the agent to provide evidence of power of attorney but may separately contact the requesting consumers to confirm their

engagement of authorized agents or require the authorized agents to provide signed permission from consumers through the requesting channel.

4. Sensitive Personal Information Rights

Notice of Right to Limit. The CPRA requires that businesses must provide consumers with notice of their right to limit the use and disclosure of their sensitive personal information and notice about how to opt-out of having their sensitive personal information used for other purposes. “Notice of right to limit” is now defined under § 7001(o) of the proposed amendments. The right to limit or opt-out only applies to the extent a consumer’s sensitive personal information is used for a purpose other than to perform the services or provide the goods. The proposed amendments also outline several exceptions to this right, noting that the right to limit does not apply when the sensitive personal information is: (a) necessary to detect security incidents to resist malicious or illegal attacks on the business; (b) necessary to ensure the physical safety of natural persons; (c) used for short-term, transient use; (d) used to perform services on behalf of the business; or (e) used to verify or maintain the quality or safety of the business (§ 7027).

To the extent a business must offer the right to limit, it must provide at least two designated methods for submitting such requests, and one of the opt-out methods must reflect how the business interacts with the consumer. For example, a business that primarily interacts with a consumer online must allow consumers to submit opt-out requests through an online form either accessible by a “Limit the Use of My Sensitive Personal Information” link, the privacy policy, or an alternative link such as an opt-out preference signal described above (§ 7015). The link should be conspicuous, located either at the header or footer of the business’s internet homepages, or on mobile apps in settings menu and within its privacy policy. According to the proposed amendments, a business then has 15 days to comply with the opt-out request, including notifying service providers, contractors and third parties, and must provide consumers with a means by which they can confirm their request to limit has been processed (§ 7027(g)).

5. Contracting - Data Processing and Sharing Agreements

Service Providers/Contractors. The proposed CPRA amendments include several new and modified requirements for data processing contracts with service providers (§ 7051). Specifically, such contracts must include provisions prohibiting service providers or contractors from:

- using, retaining or disclosing the personal information or any purposes than to perform the specific services (business purposes);
- selling or sharing the personal information;
- retaining, using or disclosing personal information outside of the direct business relationship between the service provider and the business; and
- combining personal information from different sources.

In the data processing contract, service providers and contractors must also agree:

- to notify the business of sub-processors;
- to bind sub-processors to the same obligations in a written contract; and
- to notify the business no later than five business days after it make a determination that it can no longer meet its obligations under the CCPA and the regulations;

- to assist the business in responding to verifiable consumer requests;
- to assist the business through appropriate technical and organizational measures in complying with the requirement to implement reasonable security procedures and practices; and
- to permit the business to audit/monitor compliance.

In addition to these provisions, contractors are required to certify their understanding of and compliance with the contractual requirements.

Third Parties. The proposed CPRA amendments require that a business that sells or shares personal information with a third party enter into an agreement with that third party that includes some of the same requirements as those proposed for a service provider contract. The proposed amendments do not define the term “third party” but seem to refer to any person or entity that receives personal information from a business and is not a service provider or contractor. Third parties are not permitted to process or store personal information without a contract and are required to comply with the CPRA and its regulations. Pursuant to § 7053 of the proposed amendments, a third-party contract must include the following provisions:

- include a specific description of the limited purpose(s) for which the personal information is sold or disclosed and require the third party to only use it for those limited and specified purposes.
- specify the business is disclosing the personal information to the third party only for the specified purposes in the contract;
- require the third party to comply with all applicable sections of the CCPA and the regulations, including providing the same level of privacy protection as required by businesses;
- grant the business the right to take reasonable and appropriate steps to ensure that the third party uses the personal information that it received from, or on behalf of the business, in a manner consistent with the business’s obligations under the CCPA and these regulations;
- grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information;
- require the third party to notify the business no later than five business days after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

6. Privacy Policy Requirements

In addition to the prior requirements under the CCPA that a business notify consumers of the categories, purposes, and sources of personal information, § 7011 of the proposed amendments outline several new requirements. According to the proposed amendments, a business’s privacy policy must now also include:

- the date it was last updated;
- the length of time the business intends to retain each category of personal information, or if that is not possible, the criteria used to determine the period of time it will be retained;
- if a business allows third parties to control of the collection of personal information, the names of the third parties, or information about the third parties’ business practices;

- a description of a consumer’s new rights described above (the right to correct inaccurate personal information, the right to opt-out of sale or sharing of personal information, and the right to limit the disclosure of sensitive information);
- clear instructions on how consumers can exercise these rights; and
- a description of how an opt-out request will be processed.

Businesses that handle the personal information of more than 10,000,000 consumers in a calendar year must also include a link to certain reporting requirements.

7. Notice of Collection

Specific Notification. If a business collects personal information online, the proposed amendments require that consumers have meaningful control of their personal information, which § 7012 defines as the consumer having all the information necessary “to choose whether or not to engage with the business, or to direct the business not to sell or share their personal information and to limit the use and disclosure of their sensitive personal information.” The proposed amendments require that businesses that collect personal information online must provide the consumer with a link to the *specific* section of the privacy policy that describes: (a) the personal information collected and purposes for such collection, (b) whether the personal information is sold or shared, (c) the retention period for each category of personal information collected, (d) a link to the opt-out of sale/sharing (if the business sells/shares), and (e) if the business allows third parties to control the collection of personal information, the names of third parties or their business practices (§ 7012 (f)). This represents potentially significant new burdens that in-scope businesses must think through and accurately disclose.

Notification of Third-Party Involvement. Section 7012(g) of the proposed amendments require that where a third party is involved and controls the collection of personal information (such as a cookie analytics provider), a business must notify the consumer of the third-party collection and identify the third party. The proposed amendments note that this requirement also applies to physical businesses that allow a third party to collect personal information.

8. Investigations and Enforcement

In addition to addressing California Privacy Protection Agency-initiated investigations and complaint referrals, the proposed amendments set forth a method for individuals to submit sworn complaints to the CPPA via an electronic complaint system available on its website or by mail. Such complaints must identify the business, service provider, contractor, or person who allegedly violated the CCPA; establish the underlying facts of the allegation; authorize the alleged violator and the CPPA to communicate regarding the complaint (which will be disclosed to the alleged violator); and provide contact information and be signed and submitted under penalty of perjury. The CPPA’s Enforcement Division will notify the complainant of any action it has taken or plans to take, along with reasons for that action or nonaction. The proposed amendments also set forth procedures for probable cause proceedings (§ 7302) and stipulated orders (§ 7303).

The proposed amendments confirm that the CPPA may audit a business, service provider, contractor or person “to ensure compliance with any provision of the CCPA.” Not only may the CPPA do so to investigate possible violations of the law, but it also may “conduct an audit if the subject’s collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law.” Audits may be

announced or unannounced at the CPPA's discretion, and a subject's failure to cooperate may result in the issuance of a subpoena, a warrant, or the exercise of other enforcement powers.

Conclusion

The proposed amendments to the CCPA regulations present, in some cases, potentially challenging regulatory hurdles that businesses will be forced to carefully consider and implement across their digital properties, supporting them through appropriate people, process and technology investments. Of note, the proposed amendments are not yet final and so there is the possibility that they will change with public input.

Subscribe to [Greenberg Traurig's Data, Privacy & Cybersecurity blog](#) for updates.

Authors

This GT Alert was prepared by:

- [Darren Abernethy](#) | +1 415.655.1261 | abernethyd@gtlaw.com
- [Gretchen A. Ramos](#) | +1 415.655.1319 | ramosg@gtlaw.com
- [Sherry Xiaoxuan Ding](#) | +1 415.655.1300 | dings@gtlaw.com
- [Roya L. Butler](#) ‡ | +1 415.655.1269 | Roya.Butler@gtlaw.com

‡ Admitted in the District of Columbia. Not admitted in California.

Albany. Amsterdam. Atlanta. Austin. Boston. Charlotte. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany. † Houston. Las Vegas. London.* Long Island. Los Angeles. Mexico City.+ Miami. Milan.» Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Sacramento. Salt Lake City. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.* Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. †Greenberg Traurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Santa Maria, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ‡Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimbengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by GREENBERG TRAUIG Nowakowska-Zimoch Wysokiński sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in GREENBERG TRAUIG Nowakowska-Zimoch Wysokiński sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2022 Greenberg Traurig, LLP. All rights reserved.*