

CCPA Compliance Is on the Horizon – What You Need to Know to Be Ready

JUNE 19, 2020

Authors: [Michael D. Stovsky](#), [Kristopher J. Chandler](#)

Enforcement Begins July 1

On July 1, businesses operating in California and collecting and processing California consumer personal data will begin to experience enforcement of California Consumer Privacy Act (“CCPA”) obligations and should be prepared to comply with applicable data security and privacy requirements. Though the CCPA went into effect on January 1, 2020, the statute and the California Attorney General permitted a delayed enforcement date of July 1, 2020. On this date those entities governed by the CCPA are potentially exposed to enforcement actions initiated by the California AG for failure to meet their compliance obligations under the CCPA. Thus, it is of key importance for businesses to understand if the CCPA applies and what their compliance obligations are in order to avoid significant liability. The California AG has specifically stated that the current health pandemic caused by COVID-19 will not impact the start of enforcement.

To understand if the CCPA applies to your business, Benesch has prepared a summary of applicability that can be [found here](#).

A key component of satisfying compliance obligations is adhering to the regulations adopted and implemented by the California AG. Though the process has been more lengthy than expected, the adoption of these rules is slated to begin very soon after a detailed rule making process.

Recent Submission of Final Regulations

On June 1, 2020, the Office of the California Attorney General (“OAG”) submitted the final proposed regulations under the CCPA. These regulations detailed specific compliance obligations with respect to the CCPA and provide further context and guidance to business in complying with obligations under the CCPA. This guidance includes further context with respect to definitions, notice requirements, responding to consumer requests, verification of consumer requests, and the special rules with respect to the collection of personal data from minors.

These final regulations have been submitted to the California Office of Administration Law (“OAL”) for final review and approval of the regulations to ensure procedural compliance with the Administrative Procedure Act. The OAL has 30 working days, plus an additional 60 calendar days (provided in response to the COVID-19 pandemic) to review the final regulations. Once approved by the OAL, the final regulation text will be filed with the Secretary of State and become enforceable by law. Because of the impending July 1 enforcement deadline, the OAG has requested an expedited review of the regulations.

These final regulations should be reviewed in tandem with the text of the CCPA as well as within the context of the six CCPA amendment bills that subsequently amended the CCPA (A.B. 25, A.B. 874, A.B. 1146, A.B. 1202, A.B. 1355, and A.B. 1564), which became law on October 11, 2019. These final regulations direct businesses, service providers, and third parties (all defined entities under the CCPA) on their rights and obligations under the CCPA. Thus, an analysis of these final regulations is important for the creation and implementation of a robust CCPA compliance program at the entity level.

Summary of CCPA Regulations

Summarized below are several noteworthy provisions of the final regulations of the CCPA. The final regulations do not diverge significantly from the proposed regulations released in March 2020. Thus, businesses that have already implemented data privacy and security policies and procedures that align with those March 2020 guidelines may not need to make significant changes ahead of the July 1 enforcement date.

- **Required Disclosures.** The final regulations clarify that every business subject to the CCPA must provide privacy policies to consumers. Privacy policies must identify the categories of sources from which personal information is collected and the categories of third parties to whom information is disclosed or sold. The regulations clarify that “categories of sources” mean groupings of persons or entities including the consumer directly, advertising networks, internet service providers, data analytics providers, operating systems and platforms, social networks, and data brokers. Similarly, the regulations expand on the definition of “categories of third parties.” Businesses are restricted to using consumer’s personal information for the purposes described in the privacy policy at the point of collection.
- **Time of Disclosure.** The final regulations require businesses to provide “timely notice” at or before the “point” of collection of the personal information from the consumer, which may be electronic or in-person. Therefore, this requirement encompasses both temporal and physical proximity to the collection of personal information.
- **Collection Formats.** The final regulations state that the collection of personal information is applicable to both online and offline formats. For example, a business will be required to include clearly a visible link to its privacy policy on its website and mobile app as well as implement separate and distinct means at a physical location or over the telephone.
- **Just-in-Time Notice Requirement.** The final regulations require businesses to provide a “just-in-time” notice to consumers containing a summary of the categories of personal information being collected and a link to the full notice at collection when collecting personal information from a consumer’s mobile device for a purpose the consumer would not reasonably expect.
- **Restriction on the Sale of Personal Information.** The final regulations provide that, unless a business has obtained a consumer’s affirmative consent for sale of his or her personal information, the business may not sell any personal information they collect during any time they had not posted a notice of the right to opt-out.
- **Verification of Consumer Requests.**

The final regulations require businesses to have a reasonable method of verifying the identity of consumers making requests to know and requests to delete. Businesses should not request additional information from the consumer for purposes of verification. In the event additional personal information is required, a business must delete this new personal information as soon as practical after processing a consumer's request.

- **10-day Response Requirement to Requests to Know and to Delete.** The final regulations require businesses to acknowledge a consumer's request to know or to delete within 10 business days, and to provide information as to how they will process the request.
- **15-day Opt-out Requirement for Sale of Personal Information.** The final regulations require a business to comply with a request to opt-out as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. Further, should a business sell a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request, it shall notify those third parties that the consumer has exercised his or her right to opt-out and shall direct those third parties not to sell that consumer's information.
- **Handling Consumer Rights Requests.** The final regulations also clarify that the two-step process for online requests to delete personal information is optional and not mandatory. Under the two-step process, a business may require a consumer to first request deletion and then confirm the request in a separate communication. The final draft of the regulations also states that a business may deny a consumer's request if it cannot verify the consumer's identity within a 45-day time period. In responding to a consumer's "request to know," businesses are not required to search for personal information if all of the following requirements are met: 1) the business does not maintain the personal information in a searchable or reasonably accessible format; 2) the business maintains the information for legal or compliance purposes; 3) the business does not sell the personal information or use it for commercial purposes; and 4) the business describes to the consumer the categories of records that may contain personal information that it did not search pursuant to this provision of the regulations.
- **Service Providers.** The final regulations explain that a business that provides services to an entity that is not a "business" under the CCPA may still qualify as a service provider. This helps clarify the scope of the regulations' applicability to entities that provide services to nonprofits that are not "businesses."
- **Business to Business Collection.** The final regulations deem any business that collects personal information on behalf of another business to be a "service provider" of the that business.
- The final regulations largely exempt employee and prospective employee data until the year 2021. However, companies are still required to issue a notice at the point of collection to employees and prospective employees identifying the categories of personal information they collect about employees or prospective employees and the business or commercial purpose for which the categories will be used. All businesses must ensure that they have a protocol in place to issue this notice to employees and prospective employees.
- **Record-Keeping.** Finally, the regulations now require businesses to implement and maintain reasonable security procedures and practices to protect the records that the CCPA requires them

to maintain about personal information. This modification ensures that businesses understand their obligation to securely maintain these required records, which is especially important in light of the CCPA's requirement that the records be maintained for at least 24 months. The regulations also authorize businesses to use those records "as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and its regulations."

- **IP Addresses.** The final regulations clarify that an IP address alone that does not or could not reasonably link it to a particular consumer does not qualify as personal information.

Because of the breadth of the regulations and the quickly approaching enforcement deadline, we expect that the final rules submitted to the OAL will be those rules submitted to the Secretary of State for adoption. We do not expect OAL to make many (if any) substantive changes.

To assist with the development and implementation of a CCPA compliance program, Benesch is happy to provide clients with a more detailed analysis of the regulations as well as the comments individuals and entities provided to the OAG during the rule making process.

CCPA Compliance is Fluid and Will Continue to Change

The hallmark of an expansive data security and privacy law is the fact that it is subject to continuous change as technology change and further impact of the law becomes clear once it has been in force. Though having already been amended six times, the CCPA will be potentially amended further in response to a ballot initiative started by Californians for Consumer Privacy, the privacy rights advocacy group who sponsored the CCPA. Californians for Consumer Privacy is pursuing even more restrictive consumer privacy rights with the ballot initiative, the California Privacy Rights Act ("CPRA").

Recently, the group secured the 900,000 signatures required for the petition to assume a spot on California's November 2020 ballot. If it actually appears on the ballot and subsequently passes, businesses will once again be required to heighten their current privacy policies and procedures to comply with this more stringent law.

The CPRA would amend the CCPA, which is one of the most comprehensive privacy regulatory schemes in the United States. Essentially, the amendment would expand the privacy rights of California residents and make compliance obligations more robust for businesses.

The CPRA proposes, among other things, the following:

- Adding a new category of information known as "sensitive personal information", which would include health, financial, and geolocation information collected, and allow California consumers to block businesses from using this information. Much of this information is covered by federal privacy laws, like the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA).
- Enhancing children's privacy rights and tripling fines for collecting and selling information of minors under 16 years of age. The current penalties under the CCPA provide for \$2,500 for each violation or \$7,500 for each intentional violation. Businesses should keep in mind that penalties

are imposed based upon each piece of personal information, such as name, mailing address, email address, or account name.

- Establishing a new enforcement authority to protect data privacy rights.
- Giving Californians the right to ask businesses to correct inaccurate personal information.
- Updating data breach liability, specifically for breaches of a consumer's email with a password or a security question. In such cases, hackers would be able to access the consumer's account, and the CPRA could result in liability for the company experiencing the breach.

While the privacy rights of consumers is the fundamental concern of the CPRA, the legislation does include some provisions beneficial to businesses. One such provision is that business will be provided with an additional two-year extension to exemptions for employee and business-to-business data. The current exemption is set to expire at the end of 2020. It is important to note that under the current exemption, while employees are temporarily excluded from most of the CCPA's protections, two areas of compliance remain: (i) providing a notice at collection, and (ii) maintaining reasonable safeguards for personal information driven by a private right of action now permissible for individuals affected by a data breach caused by a business's failure to do so.

The final step for this petition to appear on the November ballot is certification of the signatures collected. The California Secretary of State and local election officials must certify those signatures by June 25, 2020. Specifically, 675,000 of the 900,000 signatures must be certified as valid for the CPRA to be included on the ballot.

As CCPA compliance comes into effect and CCPA obligations continue to be amended and further interpreted, the Benesch Data Security and Privacy team is committed to staying at the forefront of knowledge and experience to assist our client in complying with legal obligations. We are available to assist you with any compliance efforts. You may reach Michael Stovsky at 216-363-4626 or at mstovsky@beneschlaw.com, or Kris Chandler at 614-223-9377 or at kchandler@beneschlaw.com.