Privacy Alert
June 2020

While Final CCPA Regulations Await OAL Approval, Companies Should Move Forward with Compliance Efforts

Key Takeaways

- The final versions of the CCPA regulations are substantively identical to the draft modifications released in March.
- The AG has requested an expedited review, which means the regulations could be enforced as early as July 1.
- Now is the time to address any gaps between your compliance efforts and the text of the regulations.

The California Attorney General submitted final California Consumer Privacy Act (CCPA) regulations to the California Office of Administrative Law (OAL) on June 1, along with a request that the OAL expedite its review to complete it within 30 business days. The regulations—which are substantively identical to the second set of modified proposed regulations that the AG released in March—will become enforceable once approved by the OAL and filed with the Secretary of State. The OAL can take up to 60 days for its review and currently has a significant backlog of requests. While it's not yet clear whether the OAL will prioritize its review of the CCPA regulations, the AG has requested that the regulations take effect upon approval, so even if the regulations are not effective on July 1, they could be in effect shortly thereafter.

What should businesses do while they wait for the final regulations to be approved?

It's time to move forward with compliance. The regulations introduce a number of substantial additional requirements not found in the CCPA. While waiting for final regulations, there are a few steps you may need to take now:

- Review Your Privacy Notices. The regulations provide guidance on where to post notices in mobile apps, and impose new obligations for just-in-time notifications and notices of financial incentives that you may not have implemented if you published a new privacy notice in January.
- Review Your Processes for Verifying Consumer Requests. The regulations include updated requirements for verification and steps to take for consumers who can't be verified. The regulations also provide guidance on responding to requests made via an authorized agent.
- Track Your Requests and Response Times. The regulations introduce new obligations to retain and publish records regarding the number of consumer requests received and the time to respond. Companies should implement a process for tracking and retaining this information for 24 months.
- Review Your Security Standards and Service Provider Agreements. The regulations don't introduce new security requirements, but a review of security standards may have been de-prioritized while you

Attorney Advertising

were preparing your consumer-facing compliance efforts. The only private right of action under the CCPA arises from a company's failure to reasonably protect data that leads to a security breach, which makes updated security measures a key component of CCPA readiness. The regulations also clarify the restrictions a business must place on a Service Provider's use of personal information.

With three versions of draft regulations published over the past eight months, it may be difficult to recall what new requirements (and key clarifications) made it into the final regulations, so we've provided the highlights for you below.

Review Your Privacy Notices

Notice of Information Collection

The CCPA requires companies to provide notice "at or before the point of collection." The final regulations:

- Require just-in-time notices for unexpected data collection. If an app collects information that the consumer would not reasonably expect to be collected, the business must provide a just-in-time notice of that collection (e.g., through a pop-up window) that briefly explains the collection and includes a link to the full privacy policy.
- Clarify that businesses that don't collect personal information directly from consumers do not have to give the notice at collection to consumers as long as they do not sell consumers' personal information.
- State that any company that doesn't collect personal information directly from consumers but **does** sell personal information should register as a data broker and provide its notice via a privacy policy link included with its registration submission.

Notice of the Right to Opt Out of a Sale of Personal Information

The CCPA requires companies to provide a clear and conspicuous link on the business's internet homepage, titled "Do Not Sell My Personal Information" that goes to a webpage that enables a consumer to opt out of the sale of their personal information.

The final regulations:

- Clarify that companies that do not sell personal information do not have to provide the do-not-sell link but must state in their privacy policy that they do not sell information. A business that does not display a notice and opt-out for sales may not sell personal information collected without affirmative consent.

Notice of Financial Incentives

The CCPA requires businesses that offer financial incentives to notify consumers of such incentives.

The final regulations:

- Require businesses that offer a financial incentive to provide consumers with a notice that includes a summary of services offered; the material terms, including the categories of personal information implicated and the **value of the consumer's data**; a mechanism to opt out of the incentive; and a statement of the consumer's right to withdraw. **Companies should evaluate the metrics they will use to calculate the value of consumer data**. Disclosures should be carefully crafted to minimize litigation risk.
- Require businesses to **disclose a good-faith estimate** of the value of the consumer's data to the business and a description of the methods used to calculate that value.
- Underscore that if a business is unable to calculate a good-faith estimate of the value of the consumer's information or show that the financial incentive or price or service difference is reasonably related to the value of the consumer's information, the business cannot offer the financial incentive or price or service difference.

Review Your Processes for Verifying Consumer Requests

The CCPA makes it clear that businesses are not obligated to provide information to consumers if the business cannot verify the consumer.

The final regulations:

- Require businesses to have a reasonable method to verify that the person making a request matches the consumer whose information was collected, taking into consideration the sensitivity and value of the information and the risk of fraud.
  - Where a consumer has a **password-protected account** with the business, the business may use the authentication process for the account to verify the consumer's identity.

- If a consumer **does not have a password-protected account** with the business, the regulations provide this guidance:
  - Where categories of personal information are requested, the consumer's identity must be verified to a reasonable degree of certainty. This may include matching **at least two data points** from the consumer with data points in the information maintained by the business.
  - Where specific pieces of information are requested, the consumer's identity must be verified to a **reasonably high degree of certainty**. This may include matching **at least three data points** and having a signed declaration from the consumer stating that the requester is the consumer. These declarations must be kept by the business.
  - Verify the identity of the consumer to a reasonable or a reasonably high degree of certainty for a request to delete information. The more sensitive the information and the greater the risk to the consumer that deleting the information creates, the higher the degree of certainty needed.
- If the business cannot verify the consumer within the 45-day time period, the business may deny the request.
- A business can deny the request if it has a good-faith, reasonable and documented belief that the request is fraudulent.

- Clarify that a toll-free number is not required for online-only businesses, giving effect to an amendment to the statute and specifying that a business that operates exclusively online and has a direct relationship with the consumer is required to provide only an email address for submitting access requests.
- Require businesses to inform consumers when they are unable to reasonably verify the consumer's identity to the degree of certainty required and explain why it has no reasonable method by which it can verify the identity of the requester. A business must also explain in its privacy policy why it has no way to reasonably verify the requester's identity and evaluate yearly whether it can establish a method for verification.
- Opt-outs do not require verification.

Access Requests

The CCPA requires businesses to provide consumers with access to their personal information upon request. However, the regulations provide some helpful carve-outs to this obligation.

The draft regulations:

- Make it clear that, in responding to an access request, a business is not required to search its records for personal information if each of the following criteria are met: (1) the business doesn't keep the information in a reasonably accessible format, (2) the business keeps the information only for legal or compliance purposes, (3) the business does not sell the information or use it for any commercial purpose, and (4) the business tells the consumer the categories of records that may contain personal information but that weren't searched because the information met each of the above criteria.
- Clarify that sensitive information, such as financial account numbers, government identification numbers, Social Security numbers, driver's license numbers, medical and insurance information, passwords, security questions, and unique biometric data, cannot be disclosed in connection with requests for specific pieces of information. The business shall, however, inform the consumer with sufficient particularity that it has collected that type of information.
- Provide that a business may avoid providing specific pieces of information due to a conflict with applicable law, or based on an exception to the CCPA, provided that the business informs the consumer and explains the basis for the denial.

Deletion Requests

The CCPA requires businesses to delete certain consumer personal information upon request.

The draft regulations:

- Make it clear that if a business that denies a consumer's request to delete sells personal information and the consumer has not already made a request to opt-out, the business must ask the consumer if they would like to opt out of the sale of their personal information and shall include either the contents of, or a link to, the notice of the right to opt out in its response to the consumer.

- Clarify that a business may deny a deletion request for any information that is necessary to maintain a consumer's enrollment in a loyalty program, if the consumer has informed the business that he or she would like to remain in the program but otherwise have their personal information deleted.

Do Not Sell

The CCPA requires businesses to honor consumer requests to opt out of the sale of their personal information.

The final regulations:

- Require businesses to honor user-enabled global privacy controls such as browser-based signals. The AG's statement of reasons notes that this is a forward-looking statement (no "opt-out of sale" signals or plug-ins exist today). However, companies should monitor the activities of browsers and other developers that may look to create these mechanisms in the next few weeks or months. Businesses can notify a consumer when their privacy controls conflict with the consumer's business-specific privacy settings and give the consumer the option to limit the opt-out.
- With a request to opt out or delete, a business may give the consumer a choice to opt out or delete only portions of personal information, but only if a global option is given and is more prominently displayed.

Authorized Agents

The CCPA allows consumers to exercise their individual rights through an authorized agent.

The final regulations:

- Provide that businesses may require a consumer who seeks to use an authorized agent for access and deletion requests to 1) provide the authorized agent written and signed permission to submit on the consumer's behalf, 2) verify their own identity directly with the business, and 3) directly confirm with the business that they provided the authorized agent permission to submit the request.
- Provide that authorized agents may submit opt-out requests on behalf of consumers only if the consumer provides the agent written permission signed by the consumer.

Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf must be included in the privacy policy. A business may deny a request from an authorized agent that does not submit proof that they have been authorized by the consumer to act on their behalf.

Household Requests

The CCPA allows for consumers to submit requests for personal information relating to a household.

The final regulations:

- Define "Household" – a term that was previously undefined in the statute – as a person or group of people who (1) reside at the same address, (2) share a common device or the same service provided by a business, **AND** (3) are identified by the business as sharing the same group account or unique identifier.
- Provide that a business may decline an access or deletion request unless 1) the family has a password-protected account with the business or 2) the business can verify that each member of the household making the request is currently a member of the household.
- Prohibit a business from complying with a household's deletion or access request if the requesting household does not have a password-protected account with the business, unless 1) all consumers of the household jointly request access or deletion of household personal information, 2) the business can verify each member of the household, and 3) the business can verify that each member of the household making the request is currently a member of the household.

Track Your Requests and Response Times

The final regulations impose new record-keeping requirements on businesses that are not detailed in the statute, including the following:

- Businesses must generate and retain metrics on how they value consumer data (when financial incentives are offered).
- Businesses must also maintain (for 24 months) records of consumer requests made pursuant to the CCPA and details on how the business responded to these requests.
- Businesses that touch the personal information of more than 10 million consumers must compile metrics of the consumer requests they have received, including

the median time it took the business to respond. This information must be included in the privacy policy.
- Businesses that receive, share or sell the personal information of 10 million consumers in a calendar year must establish, document and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA or for the business's compliance with the CCPA are informed of all CCPA requirements.

Review Your Security Standards and Service Provider Agreements

Security Standards

The CCPA requires businesses to implement and maintain reasonable security procedures and practices.

The final regulations:

- Address the need to protect personal information (including personal information contained in the records, which need to be kept for 24 months).

Service Provider Agreements

The CCPA prohibits service providers from retaining, using or disclosing personal information obtained in the course of providing services, except in limited circumstances (e.g., to detect security incidents or protect against fraud or illegal activity).

The final regulations:

- Expand a service provider's ability to use personal information for non-service provider purposes by allowing service providers to use the information for its own internal purposes, including to build or improve the quality of its services, so long as that use doesn't include building or modifying household or consumer profiles or cleaning or augmenting data obtained from another source.

If you have any questions about the regulations, please reach out to a member of Loeb's Privacy team.

Related Professionals

Jessica Lee . . . . . jblee@loeb.com
Chanda Marlowe . . . . . cmarlowe@loeb.com

6361 REV2 06-11-2020