

CCPA Final Regulations Submitted, IAB Tech Lab Releases Data Deletion Request Solution

The Bottom Line

- The submission of the final regulations to the OAL now puts businesses on notice of their actual CCPA compliance obligations.
- Businesses must ensure that they are prepared for CCPA enforcement to begin on July 1, 2020, regardless of when the final regulations actually take effect.
- The newly released IAB Data Deletion Request Handling specification offers publishers in the digital advertising ecosystem a solution to help them comply with data deletion requests under the CCPA.

The final text of the California Consumer Privacy Act (CCPA) regulations were submitted by the California Attorney General to the California Office of Administrative Law (OAL) for approval on June 1, 2020. Substantively, the final text of the regulations are the same as the most recent draft regulations that were released on March 27, 2020.

While the OAL normally has 30 working days to approve the regulations, Governor Newsom's recent Executive Order N-40-20 currently extends that period by an additional 60 calendar days. Nonetheless, the Attorney General has requested that the OAL expedite and complete its review within 30 business days. Once approved by the OAL, the final regulation text will be filed with the Secretary of State and become enforceable by law. When the OAL will actually approve the final regulations remains to be seen.

Key Requirements and Takeaways From the Final CCPA Regulations

Pre-Collection Notice Requirement

Before or at the time that businesses collect personal information from consumers, they must provide a notice about the categories and purpose of personal information being collected. The regulations added a requirement for "just-in-time" notices for personal information collected through consumers' mobile devices for unexpected purposes that disclose the categories of the information collected and provide a link to the full pre-collection notice. The regulations also add a pre-collection notice exemption for businesses that do not directly collect personal information from consumers, if the business doesn't then sell that consumer's information or if the business is a registered data broker.

Opt-Out Notice

A business that "sells" personal information, as that term is defined under the CCPA, must provide:

- An opt-out notice to consumers that contains a description of the consumer's right to opt out of the sale of their personal information;

- An interactive form where consumers can submit a request to opt-out;
- Instructions for any other method through which opt-outs can be submitted; and
- A link on homepage with the words “Do Not Sell My Personal Information” or “Do Not Sell My Info.”

The regulations add that the opt-out notice is not required if the business:

1. Does not sell personal information and
2. States that it does not sell personal information in their privacy policy.

If the business does not provide such notice, it cannot sell personal information. However the regulations states that businesses still may do so if they obtain “affirmative authorization” of the consumer, which is defined as an “action that demonstrates the intentional decision by the consumer to opt in to the sale of personal information.”

Privacy Policy

Businesses need to provide information about a consumers' rights in their privacy policy, in addition to other specific disclosures. The regulations specify that the privacy policy should also include the following right to know disclosures about the collection and use of personal information:

- The categories of personal information the business collected from consumers in the prior 12 months;
- The source of that personal information;
- The purpose for collecting or selling personal information;
- The categories of personal information the business disclosed or sold to third parties in the prior 12 months and for each of those categories of personal information;
- The categories of third parties to whom the information was disclosed or sold; and
- Whether the business has actual knowledge that it sells personal information of minors under 16 years old.

Requests to Know

The regulations clarify that businesses that operate exclusively online and have a direct relationship with their consumers only need to provide an email address for requests to know. Otherwise, businesses must provide a toll-free number as well as at least one other method by which consumers can submit such requests.

In order to respond to request to know, the regulations provide an exception and state that a business does not have to search for personal information if it:

- Is not maintained in a searchable format;
- Maintains such information just for legal or compliance purposes;
- Does not sell or use such information for commercial purposes; and
- Explains to the consumer that it has not searched certain categories of records for this reason.

Request to Delete

Businesses must provide two or more methods for submitting requests. Businesses are allowed to retain personal information for archival or backup purposes and to give consumers the option to delete only portions of their personal information as long as more prominent global deletion option is also presented. Businesses must also confirm receipt of such requests within 10 business days and comply or otherwise respond to the request within 45 days.

Opt-out Requests

Businesses are required to provide at least two methods for submitting opt-out requests including an interactive webform through a “Do Not Sell My Personal Information” or “Do Not Sell My Info” link. The business must treat “user-enabled global privacy controls” such as a browser plugin, privacy setting or device setting as an opt-out of the sale of their personal information, but there remains much debate in the industry over what this means with respect to do not track features in web browsers. Businesses must comply with requests within 15 days. The regulations specify that business can deny opt-out requests if it has a good-faith, reasonable, documented belief that it is fraudulent.

Service Provider

The regulations confirm that an entity can be both a business and a service provider if it fits the corresponding requirements and obligations for both. Although the regulations expressly require a service provider to process and maintain the personal information on behalf of the business in compliance with its contract with the business, a service provider may also use the personal information:

1. To retain and employ a subcontractor;
2. For internal use to build or improve the quality of its services (as long as it does not involve profiling for other businesses or augmenting data from another source);
3. For anti-fraud and security detection; and
4. To comply with its legal obligations.

Records Requirement

A business is required to keep a record of consumer requests that it receives and its responses for at least 24 months. New reporting requirements are also imposed for a business that knows, or should reasonably know, that it buys, receives, sells or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year. Those businesses are required to disclose in their privacy policy certain metrics about the consumer request they receive and how they respond every year.

Household Information

The regulations clarify that businesses should not comply with requests to know specific pieces of information or requests to delete information for personal information connected to households, unless all of the members of the household make the request and the business verifies the identities of all of those household members.

However, if the request is made through a password-protected account, then a business’s standard verification procedures for such accounts will apply (consistent with bullet point below) and not every household member must make the request.

Request Verification

If a request is made through a password-protected account, a business can verify such requests through the usual verification processes it uses in connection with its password-protected accounts. If no such account exists, then the regulations lay out different levels of confirmation that are needed for verification in relation to different types of requests.

Requests for knowing more about the categories of personal information requires verification to a reasonable degree of certainty, which may involve matching at least two data points of identity. Requests for specific pieces of information requires verification to a reasonably high degree of certainty, which may involve matching at least three data points of identity. Request for deletion may require a reasonable or reasonably high degree of certainty depending on the sensitivity of the information requested.

Requirements for Minors

Businesses that sell the personal information of minors between at least 13 years old and under 16 years old must only do so after the minor opts in to the sale, which requires a two-step process. Minors under the age of 13 years old must have parental consent to opt-in to sales of their information. The regulations provide various examples of methods by which parents can give consent such as a signed consent form, use of a credit card or other payment system, or a video conference or phone call with trained personnel.

Authorized Agents

A consumer may use an authorized agent to submit a request to know or request to delete information. Authorized agents must be registered with the Secretary of State to conduct business in California. The business may require the consumer to verify their identity directly with the business.

Financial Incentive Notice

Businesses are required to provide notice of any “financial incentives” which is defined by the regulations as “a program, benefit, or other offering, including payments to consumers related to the collection, retention or sale of personal information.”

IAB Tech Lab Releases Deletion Request Solution

Meanwhile, the IAB Technology Laboratory (Tech Lab) has released a new Data Deletion Request Handling specification which offers a solution for handling data deletion requests under the CCPA. According to the Tech Lab, the specification is an industry first technical solution that enables the publisher’s digital property to signal a consumer request for data deletion to the publisher’s “service providers” (as defined under the CCPA). Its primary aim was to enable compliance with deletion requests made under the CCPA but can be used for deletion requests more generally.

Related People

Richard S. Eisert

Partner/Co-Chair Advertising + Marketing

212 468 4863

reisert@dglaw.com

Gary Kibel
Partner
212 468 4918
gkibel@dglaw.com