Published on *The National Law Review* https://natlawreview.com

Analysis of Attorney General Regulations to CCPA – Part 2: Business Practices for Handling Consumer Requests

Article By:

Brian H. Lam

Overview

Within Article 3 (pages 10-18), the regulations detail important requirements that every business must follow when providing and fulfilling consumer rights under the CCPA. These areas include:

- Methods for Submitting Requests to Know and Delete
- Responding to Requests to Know and Delete
- Service Providers: How entities can qualify as a Service Provider, how service providers must support consumer rights, and clarifying their responsibilities
- Requests to opt-out of the sale of personal information
- Requests to opt-in after opting out
- Training and Record keeping
- Requests to Access or Delete Information at the Household Level

Interested parties will need to ensure that they not only observe the strictly factual requirements regarding these areas, but also that they pay attention to those areas of guidance that might apply based on their particular data flows and how they interact with consumers and businesses. Care should be taken understand what sorts of personal information are being collected, whether the business interacts with consumers primarily online line or perhaps at a physical location, that deletion functionality can be appropriately implemented based on the data architectures being used, that functionality is being offered to comply with opt-out requirements that comports with the regulations, and that appropriate training and record keeping is taking place.

Key Elements

§ 999.312 “Methods for Submitting Requests to Know and Requests to Delete”

Submission Methods - Businesses must provide at least two methods, at least one of which shall be a toll free number along with a method that reflects the primary way the business interacts with consumers

Businesses are required to offer at least two methods for consumers to exercise their rights to know or delete personal information. A toll free number must be offered, and businesses that interact with consumers through a website should consider offering an interactive web enabled form for submitting these requests. Additional examples of acceptable methods include submitting requests via email, in person or by mail.

Businesses are required to consider how they interact with consumers when choosing these methods. At least one method must reflect the primary way that the business interacts with the consumer even if this means that more than two methods must be offered. As a toll free number is required this means that all businesses must offer the toll free number plus at least this method. Examples provided by the regulations show that an online retailer must offer a web based option as it primarily interacts with users online, and that retailers that primarily interact with consumers at a physical location must offer an in person option.

Additionally, businesses that do not directly interact with consumers in the ordinary course of business, perhaps because these aspects are being conducted by service providers, must offer at least one method to accept request to know or delete online.

Deletion Requests – Must be Provided as a Two Step Process

Deletion Requests must be offered as a two step process where the first step allows the user to submit the request for deletion and separately confirm the personal information to be deleted.

Submitting Deletion Requests Generally

Consumers may choose to submit a request to know or delete in an alternative manner than one of the provided methods. If this occurs, business are required to either (a) accept the request, or (b) provide specific directions as to how to submit or remedy the request as applicable. Realistically, this appears to mean that businesses must direct any relevant personnel to at least forward requests to the appropriate functionality area so that it may respond as required, even if those requests are not being submitted through an offered mechanism.

Certain Types of Information Cannot Be Provided Via a CCPA Request to Know

Businesses may not disclose pieces of personal information that are likely to create a substantial, articulable, and unreasonable risk to the security of the personal information, the consumers account, or the security of the business. Additionally, businesses may never disclose a consumer’s Social Security number, driver’s license number, other government issued identification number, financial account number, health insurance or medical information number, account password, or any security question or answers.

§ 999.313 “Responding to Requests to Know and Delete”

Confirming Requests to Know and Delete

Businesses are required to respond to requests to know and delete within 10 days of receiving the request and provide information regarding how the request will be processed, the verification process, and when the consumer should expect a response, unless the request has already been granted or denied.

Businesses Must Provide Substantive Responses to Requests to Know and Delete within 45 days or provide justification for an additional 45 day period

This 45 day period beings when the request is received regardless of how long it takes to verify the request. An additional 45 days may be taken to respond if the business within the original 45 day period provides an explanation why the business will take more than 45 days to respond to the request. Businesses must provide a substantive response within 90 days unless an exception applies.

Responding to Requests Generally

Businesses must verify the identity of requestors as provided in Article 4 of the regulations before providing any personal information to the requestor, and may not provide any personal information in response to such a request if it is unable to verify the consumer. The substantive response must be individualized. If the request is denied in whole or in part, businesses must consider the request as if the requestor was seeking only categories of personal information. If a business receives on of these types of requests, but is still unable to verify the consumer, it must direct the consumer to its general business practices regarding collection, maintenance and sale of personal information as provided by its privacy policy. Further any time a verified request is denied the business must the business must provide an explanation of the denial.

When responding to verified requests to know categories of personal information, the business must provide each identified category it has collected about the consumer, including: categories of sources from which the personal information was collected, the business or commercial purpose for collection, the categories of third parties that the business has disclosed the personal information to, and the businesses purposes for the same. These categories must be identified in a meaningful manner to the consumer.

Additionally the covered by the consumer's request to know shall run from the date of receiving the request, regardless of the time taken to verify the consumer.

Businesses Cannot Disclose Certain Types of Personal Information Via a Request to Know

Businesses may not disclose pieces of personal information that are likely to create a substantial, articulable, and unreasonable risk to the security of the personal information, the consumers account, or the security of the business. Additionally, businesses may never disclose a consumer's Social Security number, driver's license number, other government issued identification number, financial account number, health insurance or medical information number, account password, or any security question or answers.

Further, providing personal information to consumers, businesses must use at least "reasonable security measures."

Responding to Requests to Delete Generally

A request to delete information that cannot be verified shall instead be treated as a request to opt out of sale. When complying with a verified request, the business must choose one of the following options:

- Permanently delete all relevant personal information except for personal information on archival or backup systems, which shall be deleted when such system is next accessed or used.
- De-identify the personal information
- Aggregate the personal information

The regulations do not provide guidance regarding how de-identifying and aggregation must take place, or how these terms differ.

Further businesses must specify the manner of deletion, disclose that record of the deletion will be kept pursuant to Civil Code section 1798.105(d). The regulations specifically provide that it may delay effecting deletion on archival or backup systems until the system is used.

When denying requests, businesses must provide the consumer a notice stating the reasons for the denial, including any applicable exceptions, delete any information not subject to an exception, and not use the retained personal information for any purpose not provided for by a relevant exception.

§ 999.314 "Service Providers"

Service Providers need not provide services to a business to be deemed a service provider

If an entity is providing services to any person or organization that is not a business under CCPA, but would otherwise meet the requirements to be a service provider it will be deemed a service provider under CCPA.

Additionally, entities that are directed to collect personal information by a business and would otherwise meet the requirements to be a service provider of the business, shall also be deemed a service providers.

Scope of Service Provider Use of Personal Information

Service Providers may not may use personal information collected on behalf of a business to provide services to any other entity. However, service providers are allowed to combine personal information collected from or on behalf of businesses that it acts as service provider for as necessary to detect security incidents or prevent fraud or illegal activity.

§ 999.315 "Requests to Opt-Out"

Two or More Opt-Opt methods must be provided, including an interactive web form titled "Do Not Sell My Personal Information" or "Do Not Sell My Info" on the businesses website or mobile application and support browser or other mechanism that signal consumer's choice to Opt-Out

Similar to the requests to know or delete, the regulations require that at least two methods of submitting an opt-opt request for the sale of personal information be provided. However, for opt-out requests, a web form must be offered via a prominent link that specific title “Do Not Sell My Personal Information” or “Do Not Sell My Info.” At least one other method must be offered. Acceptable methods as before include a toll free phone number, email address, forms submitted in person or through mail. Further, businesses must accept a browser plugin or signal or other mechanism that communicate or signal the consumer’s choice to opt-out of the sale of their personal information.

Additionally, businesses must consider the methods by which it interacts with consumers, and also the methods it users to sell information to third parties and the technology used by the average consumer when choosing which opt-out methods to offer. As with requests to know and delete, at least one mechanism must reflect the primary manner in which the business interacts with the consumer.

Responding to Requests to Opt-Out Generally

If a business chooses to allow consumers to opt-out of the sale of only certain categories of personal information it must also offer global opt-out option that is more prominent.

Businesses must act on opt-opt requests in 15 days from receipt, and must notify all parties to whom it has sold relevant personal information within the 90 day period preceding the request that the consumer has exercised the opt-out right and not to further sell the personal information.

Consumers can use authorized agents to submit opt-out requests if the consumer provides authorization in writing. Businesses can refuse the request if they cannot verify that the agent is authorized. Brower controls and other similar mechanism that signal an opt-out request shall be deemed to be received directly from the consumer.

Businesses are not obligated to verify requests to opt-out to act on them, however, businesses may, upon reasonable documented suspicion that a request is fraudulent, deny the request and inform the requesting party of the same and provide an explanation.

§ 999.316 “Requests to Opt-In After Opting Out of the Sale of Personal Information”

The mechanism to opt-in after opting out must be provided in a two step process, similar to requests for deletion, where consumer clearly requests to opt-in and the subsequently confirms their request.

Businesses are allowed to inform a consumer who previously opted out when a transaction requires the sale of their personal information as a condition of completing the transaction, along with instructions as to how the consumer can opt-in. At this time it is not clear if this means that businesses are prohibited from transferring personal information of a consumer who has opted out during a transaction involving the sale or merger of the businesses or substantially all its assets, but this appears to be the intent.

§ 999.317 “Training; Record Keeping”

Businesses must provide appropriate training to all individuals responsible for assisting the business in complying with the CCPA. Further, records of all consumer requests to exercise their rights under the CCPA along with the responses of the business shall be kept for at least 24 months, and may be maintained in ticket or log format, but must include the date of the request, manner in which the

request was made, the date and nature of the business's response, and the basis for any denial. Businesses are not to use these records for any other purpose than provided by the regulations.

Additional Record Keeping Requirements for Businesses that annually buy, receives, sells or shares the personal information of more than 4,000,000 consumers

Businesses that annually buy, receive, sell, or share the personal information of more than 4,000,000 consumers must keep and compile additional metrics for the previous calendar year. These metrics include metrics regarding requests to know, delete, opt-out, and the median number of days it took to respond to these requests. Further the business must disclose this information in their privacy policy. Additionally, the business must keep records of its required training program for individuals that will assist with CCPA compliance.

§ 999.318 "Requests to Access or Delete Household Information"

If a consumer does not have a password protected account with the business, a business can choose to respond to requests to know or delete regarding household information by providing aggregate information subject to verification requirements. If all consumers jointly make such a request, and the business can verify each individually as provided by the regulations, then the business must comply with the request.

Recommendations

Businesses will need to pay close attention to how they interact with consumers, and the consumer rights that they will need to support. Ensuring that they are able to respond to requests to know and delete appropriately and that appropriate mechanisms for exercising these rights exist, along with the opt-out procedures will require understanding the organization, its data flows, and how it interacts with the consumer.

Regarding opt-outs specifically, many organizations may not be prepared to accept signals from browsers or similar technology whereby consumers exercise their right to opt-out of the sale of their information. Additionally, record keeping functionality will require a significant investment in process flows, information technology infrastructure and controls on top of that necessary to service the exercise of consumer rights.

See Yesterday's Posting in this Series: Analysis of Attorney General Regulations to the California Consumer Privacy Act

National Law Review, Volume IX, Number 290

Source URL:https://natlawreview.com/article/analysis-attorney-general-regulations-to-ccpa-part-2-business-practices-handling