

Data Privacy & Cybersecurity Flash



Andrew J. Schlidt III
414.287.9624
aschlidt@gklaw.com



Justin P. Webb
414.287.9527
jwebb@gklaw.com



Sarah A. Sargent
414.287.9450
ssargent@gklaw.com

The information in this article is based on a summary of legal principles. It is not to be construed as legal advice. Individuals should consult with legal counsel before taking any action based on these principles to ensure their applicability in a given situation.

CCPA alert: California Attorney General releases draft regulations

On Oct. 10, 2019, the California Attorney General released the highly anticipated [draft regulations](#) for the California Consumer Privacy Act (CCPA). The regulations focus heavily on three main areas: 1) notices to consumers, 2) consumer requests and 3) verification requirements. While the regulations focus heavily on these three topics, they also discuss special rules for minors, non-discrimination standards and other aspects of the CCPA. Despite high hopes, the regulations do not provide the clarity many companies desired. Instead, the regulations layer on new requirements while sprinkling in further ambiguities.

The most surprising new requirements proposed in the regulations include:

- New disclosure requirements for businesses that collect personal information from more than 4,000,000 consumers
- Businesses must acknowledge the receipt of consumer requests within 10 days
- Businesses must honor “Do Not Sell” requests within 15 days and inform any third parties who received the personal information of the request within 90 days
- Businesses must obtain consumer consent to use personal information for a use not disclosed at the time of collection

The following are additional highlights from each of the three main areas:

1. Notices to consumers

The regulations discuss four types of notices to consumers: notice at the time of collection, notice of the right to opt-out of the sale of personal information, notice of financial incentives and a privacy policy. All required notices must be:

- Easy to read in plain, straightforward language
- In a format that draws the consumer’s attention to the notice
- Accessible to those with disabilities
- Available in all languages in which the company regularly conducts business

The regulations specifically provide that for offline collection, businesses could provide a paper version of the notice or post prominent signage. Similar to General Data Protection Regulation (GDPR), a company may only use personal information for the purposes identified at the time of collection. Otherwise, the business must obtain explicit consent to use the personal information for a new purpose.

In addition to the privacy policy requirements in the statute itself, the regulations require more privacy policy disclosures. For example, the business must include instructions on how to verify a consumer request and how to exercise consumer rights through an agent. Further, the privacy policy must identify the following information for each category of personal information collected: the sources of the information, how the information is used and the categories of third parties to whom the information is disclosed. For businesses that collect personal information of 4,000,000 or more consumers, the regulations require additional disclosures related to the number of consumer requests and the average response times. Given the additional nuances of the disclosure requirements, we recommend working with counsel to develop your privacy policy.

If a business provides financial incentives to a consumer for allowing the sale of their personal information, then the business must provide a notice of the financial incentive. The notice must include a description of the incentive, its material terms, instructions on how to opt-in to the incentive, how to withdraw from the incentive and an explanation of why the incentive is permitted by CCPA.

Finally, the regulations state that service providers that collect personal information on behalf of a business may not use that personal information for their own purposes. Instead, they are limited to performing only their obligations under the contract between the business and service provider. The contract between the parties must also include the provisions described in CCPA to ensure that the relationship is a service provider/business relationship, and not a sale of personal information between a business and third party.

2. Consumer requests

Businesses must provide at least two methods for consumers to submit requests (most commonly an online form and a toll-free number), and one of the methods must reflect the manner in which the business primarily interacts with the consumer. In addition, businesses that substantially interact with consumers offline must provide an offline method for consumers to exercise their right to opt-out, such as providing a paper form. The regulations specifically call out that in-person retailers may therefore need three methods: a paper form, an online form and a toll-free number.

The regulations do limit some consumer request rights by prohibiting the disclosure of Social Security numbers, driver's license numbers, financial account numbers, medical-related identification numbers, passwords, and security questions and answers. Presumably, this is for two reasons: the individual should already know this information and most of these types of information are subject to exemptions from CCPA.

One of the most notable clarifications related to requests is that the 45-day timeline to respond to a consumer request includes any time required to verify the request. Additionally, the regulations introduce a new timeline requirement for consumer requests. Specifically, businesses must confirm receipt of a request within 10 days. Another new requirement is that businesses must respond to opt-out requests within 15 days and must inform all third parties to stop selling the consumer's information within 90 days. Further, the regulations require that businesses maintain request records logs for 24 months.

3. Verification requirements

The most helpful guidance in the regulations relates to verification requests. The regulations provide that a more rigorous verification process should apply to more sensitive information. That is, businesses should not release sensitive information without being highly certain about the identity of the individual requesting the information. Businesses should, where possible, avoid collecting new personal information during the verification process and should instead rely on confirming information already in the business' possession. Verification can be through a password-protected account provided that consumers re-authenticate themselves. For websites that provision accounts to users, requests must be made through that account. Matching two data points provided by the consumer with data points maintained by the business constitutes verification to a reasonable degree of certainty, and the matching of three data points constitutes a high degree of certainty.

The regulations also provide prescriptive steps of what to do in cases where an identity cannot be verified. For example, if a business cannot verify the identity of a person making a request for access, then the business may proceed as if the consumer requested disclosure of only the categories of personal information, as opposed to the content of such personal information. If a business cannot verify a request for deletion, then the business should treat the request as one to opt-out of the sale of personal information.

Next steps

These draft regulations add new wrinkles, and some clarity, to what is required for CCPA compliance. As we move closer to Jan. 1, 2020, companies should continue to focus on preparing compliant disclosures and notices, finalizing their privacy policies and establishing procedures to handle consumer requests. Despite the need to press forward on compliance, the regulations are open to initial public comment until Dec. 6, 2019, with a promise to finalize the regulations in the spring of 2020. We expect further clarity as these draft regulations go through the comment process and privacy professionals, attorneys, businesses and other stakeholders weigh in on their clarity and reasonableness.

Join Godfrey & Kahn's Data Privacy & Cybersecurity Team for our CCPA webinar at 12:00 p.m. CT on Oct. 29, 2019, to learn more. If you have questions or want to discuss how these regulations could impact your company, contact our Data Privacy & Cybersecurity Team.

Practice Group Members

PRINCIPAL CONTACT

Andrew J. Schlidt III
aschlidt@gklaw.com

MADISON OFFICE

Kendall W. Harrison
kharrison@gklaw.com

Todd G. Smith
tsmith@gklaw.com

MILWAUKEE OFFICE

Sean O'D. Bosack
sbosack@gklaw.com

Richard S. Marcus
rmarcus@gklaw.com

Sarah A. Sargent
ssargent@gklaw.com

Justin P. Webb
jwebb@gklaw.com