COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2023
A New Decade in Data Privacy: Complying with the CCPA

By Lisa J. Sotto and Danielle Dobrusin[1]

Following daily headlines of data breaches and companies using or maintaining individuals' data in less than desirable ways, governments around the globe have increasingly taken notice and started passing laws governing the rights of individuals with respect to their data, and the way others can permissibly use it.

Leading the pack was the European Union, whose General Data Protection Regulation[2] (GDPR), came online in 2018. While companies doing business in the European Union worked to become compliant with the GDPR, various states in the US recognized that the federal government lacks much, if any, of the framework around this issue. As a result, several states have contemplated passing their own data privacy laws and regulations.

The most significant of these laws, the California Consumer Privacy Act[3] (CCPA), was passed in June 2018. As California wrestled with the specifics of how compliance and enforcement would work, the state delayed the compliance deadline until January 1, 2020.[4] Enforcement of the law began on July 1, 2020.

In November 2020, California voters approved the California Privacy Rights Act of 2020 (CPRA), which significantly amends and expands the CCPA. Most of the CPRA's substantive provisions become operative on January 1, 2023, with enforcement beginning on July 1, 2023.

The goals of this article are to (1) inform businesses whether they fall within the CCPA's reach, (2) provide an understanding of the basics of the law, (3) provide an update on the key changes made by the CPRA, and (4) offer practical tips on how to comply.

The CCPA in a Nutshell

Dubbed California's version of the GDPR, the CCPA shares a basic framework with its European predecessor, creating new rights for Californians with respect to their personal information and imposing obligations on certain businesses that handle it. Nonetheless, there are key differences in the components and workings of these laws, such that a company already in compliance with the GDPR cannot assume compliance with the CCPA, or vice versa.

To state the obvious, the scope of coverage is different, focusing on California residents rather than Europeans. Specifically, the CCPA covers *for-profit* entities that do business in California, collect California residents' personal information, and determine the means of processing that personal information, in addition to meeting any one of the following criteria:

- Have an annual gross revenue exceeding $25 million;
- Alone or in combination, annually buy, receive, sell, or share, for commercial purposes, personal information of 50,000 or more consumers, devices, and households;[5] or
- Derive 50% or more of annual revenue from selling consumers' personal information.[6]

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

When reviewing these criteria, it is important to note that subsidiaries or entities that control or are controlled by a business and share common branding with a business are also covered.

Broadly, the CCPA grants rights to California consumers (i.e., residents) and imposes obligations on covered entities regarding how they process a California consumer's personal information. In terms of what constitutes personal information, the CCPA's definition is extremely broad—in some respects broader than the GDPR's.[7]

Specifically, the CCPA defines personal information as information that reasonably "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Examples of personal information subject to the CCPA include, but are not limited to, names, mailing addresses, Social Security numbers, unique personal identifiers (including a device identifier; an Internet Protocol address; and cookies, beacons, pixel tags, mobile ad identifiers, or similar technology), online identifiers, passport numbers, financial information, email addresses, driver's license numbers, and biometric information.

The bottom line is that the CCPA covers all personal information that can be linked to a household or individual in California. The linkage to a household is an area where the CCPA appears to go beyond the GDPR, which generally focuses only on individuals. There are a few key exclusions, however, of which businesses should be aware. For example, the CCPA currently does not apply to personal information collected in the human resources or business-to-business contexts, though these exemptions are set to expire on January 1, 2023.

In determining the most efficient use of a business's limited resources, understanding the CCPA's enforcement mechanisms and penalties, as well as California's enforcement priorities, can become almost as important as understanding what is required to comply. Violations of the CCPA's substantive provisions are enforceable by California's Office of the Attorney General.[8] A limited private right of action also exists.

The CCPA fixes statutory damages of $2,500 for each violation, or $7,500 for each intentional violation, with the California attorney general issuing these fines.[9] However, before the attorney general can bring an action for violation of the CCPA, a business must be given 30 days' notice to cure the violation, with fines potentially being assessed if the issues are not resolved. While the notice provision provides some level of comfort for businesses, implementing a "cure" within 30 days, especially if it fundamentally alters a company's data governance practices, could be an onerous task. Moreover, as discussed in further detail below, this 30-day cure period will not be guaranteed under the CPRA.

In addition to attorney general enforcement, the CCPA includes a limited private right of action for Californians in certain data breach scenarios. If a data breach occurs and the business failed to implement and maintain reasonable security procedures and practices, a private right of action could cost as much as $100–$750 per consumer per incident or actual damages, whichever is greater.[10] Class action lawsuits are also contemplated—a class of consumers can sue a business stemming from a data breach when the business egregiously does not establish reasonable safety measures to prevent the data breach.

Nonetheless, there are a few key exclusions with respect to the scope of the CCPA. For example, the law does not restrict a business's ability to collect or sell a consumer's personal information if every aspect of that commercial conduct takes place outside of California. Additionally, the CCPA does not apply to information that is subject to other federal regulations, including the Health Insurance Portability and Accountability Act of 1996, the Gramm–Leach–Bliley Act, the Fair Credit Reporting Act, or the Driver's Privacy Protection Act.[11]

Since the law became enforceable on July 1, 2020, there has been little news from the attorney general about enforcement. This likely is due to the existing 30-day cure period discussed above.

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

This document is only available to subscribers. Please log in or purchase access.

Purchase Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.