

Countdown to the CPRA



By Jennifer Mitchell, Taylor A. Bloom and Justin T. Yedor on February 15, 2022
Posted in CPRA

On Oct. 15, 2021, [BakerHostetler](#) reported on the status of the [California Privacy Protection Agency's rulemaking process](#) and the challenges the agency faces issuing regulations under the California Privacy Rights Act (CPRA) before the July 1 rulemaking deadline. As we continue to wait for the publication of regulations, what can businesses do to make progress with building a CPRA-compliant program in time for the law's Jan. 1, 2023 effective date?



We will be providing guidance on this question and exploring the path to CPRA compliance and its many nuances in this **Part 1 of BakerHostetler's Countdown to the CPRA** blog series.

First, perhaps companies can take some comfort in the fact that many of the California Consumer Privacy Act's (CCPA) requirements will remain largely the same under the CPRA. Additionally, there will be opportunities to leverage existing CCPA or General Data Protection Regulation (GDPR) processes to comply with some of the CPRA's new obligations.

Every company's approach will be different, but we recommend focusing on five key areas in the first quarter of 2022, which will be helpful when tackling the next phase of more tactical CPRA readiness.

1. Assess Threshold Applicability of the Law: Companies may overlook this critical first step, but we advise taking the time now to assess any potential changes to the CPRA's applicability to your business. The core definition of "business" – a for-profit legal entity doing business in California that collects consumers' personal information – remains the same in the CPRA as it did under the CCPA; however, the thresholds for the law's applicability have changed in ways that may be

impactful. Most significantly, the CPRA doubles the applicable threshold of consumer and household personal information, from 50,000 to 100,000. The new standard also eliminates devices as a component of this number. This shift may disqualify some smaller businesses from CPRA compliance requirements. On the other hand, the threshold is also broadened in the sense that the \$25 million revenue threshold now includes businesses that derive 50 percent or more of their annual revenue from selling **or sharing** consumers' personal information. As we know, the inclusion of the new definition of "sharing" under the CPRA in this context means that revenue derived from cross-context behavioral advertising will count toward this threshold. In light of these updates, businesses should begin by assessing whether and how the CPRA applies to them.

2. Data Mapping: Data mapping can be a burdensome and time-consuming process, particularly for bigger companies. If businesses have not begun to update their data inventories and data mapping for the CPRA, now is the time to start. Completing this exercise up front will save time and effort in the months ahead, when businesses will need to shift their attention to updating privacy disclosures, website links and consumer rights response processes. Moreover, while most CPRA provisions become operative on Jan. 1, 2023, certain "look-back" obligations were triggered as of Jan. 1, 2022. As of Jan. 1, 2023, businesses must disclose certain information about how they were processing California consumers' personal information **as of Jan. 1, 2022**. In conducting a data inventory and data map, companies should pay special attention to assessing the collection and flow of sensitive personal information under the new CPRA definition, which will include many of the data categories commonly associated with state data breach notification laws in the U.S. as well as categories, such as consumers' racial or ethnic origins or religious beliefs, considered sensitive or special under the GDPR. In addition, the CCPA's employee and business-to-business exemptions are due to sunset on Jan. 1, 2023, bringing new systems, applications and processes into the scope of the law. Application of the law to employees in particular poses serious challenges to companies, both because employment-related data may not have been inventoried before and because determining the potential applicability of exceptions to rights like the right to delete will require detailed analysis.
3. Data Retention and Governance: Now is a good time to reflect on whether a company's data governance can be improved in order to minimize redundant data and potentially mitigate a company's compliance burdens. Under the CPRA, businesses must describe the length of time for which they will retain each category of personal information, including sensitive personal information, or at least disclose the criteria used to determine the retention period. Like under existing GDPR requirements, a business cannot retain personal information for longer than is reasonably necessary for the disclosed purpose. In many cases, these new notification requirements and the substantive data retention limits require that businesses assess their internal records retention procedures to ensure that they are retaining records only for an amount of time sufficient to satisfy existing requirements under other laws, but also that they set appropriate limits on the retention of personal information.
4. Supply Chain Review: As if the new European standard contractual clauses did not present enough demands on some companies' vendor agreements, the CPRA will require businesses to

give more attention to their overall supply chain landscape. The CPRA includes additional requirements for service provider agreements, such as prohibitions on sharing personal information, retaining or using personal information for purposes outside the agreement, and combining personal information from other sources. Moreover, service providers must pass on the restrictions to subcontractors, and contracts must allow due diligence by the business to help control compliance with CPRA obligations. In addition, the CPRA expands contractual requirements to cover all parties to or with which the business sells or shares personal information. Especially because many businesses may not have contractual terms with non-service providers that govern how those parties will handle personal information, businesses should take the time now to examine transfers of personal information outside the company, establish written terms where they do not already exist or update terms that may no longer be sufficient to satisfy the requirements under the CPRA.

5. Privacy Policies and Website Updates: It is too soon to anticipate all the necessary modifications that will be required under the new CPRA disclosure requirements, and it is certainly premature to publish those updates in existing privacy policies. Nonetheless, companies should be thinking about the timing of these updates in light of other modifications to privacy policies that the business may be planning for 2022. For example, the CPRA includes new requirements to disclose the purposes for which categories of both sensitive personal information and personal information are collected or used and whether such information is sold or shared, as well as the new retention disclosure requirements discussed above. In addition, new website links and back-end processes may need to be implemented for businesses that sell or share consumers' personal information or use or disclose consumers' sensitive personal information for purposes other than those allowed by the CPRA. These businesses must provide a "clear and conspicuous link" where consumers may opt out of the selling or sharing of their personal information and opt out of the use or disclosure of their sensitive personal information. The CPRA also permits businesses to recognize an "**opt-out preference signal**" sent with the consumer's consent by a "platform, technology, or mechanism." Enabling websites to recognize such signals requires some programming updates that can be started now, particularly for existing signals like the Global Privacy Control.

BakerHostetler is closely tracking updates to the CPRA rulemaking process, and we will be sharing more updates and practical guidance in future blog posts.