AN EPUBLICATION OF THE LOS ANGELES COUNTY BAR ASSOCIATION

LACBA

PRIVACY AND CYBERSECURITY SECTION

Section Home Page
click here ›

Third-Party & Vendor Management Considerations for CPRA Compliance

By: Kyle R. Fath, ***Associate, BakerHostetler***
Rebecca Perry, ***Director of Strategic Partnerships, Exterro***

For organizations that thought they were finished with the process of papering service providers and other data recipients with California Consumer Privacy Act ("CCPA") data processing agreements, we've got some bad news for you: you're going to have to do it all over again. The California Privacy Rights Act ("CPRA"), approved by California voters on Election Day, amends the CCPA in ways that will require businesses to revisit the categorization of their vendors and heighten the contractual restrictions and requirements for service providers and other recipients of data. The good news is that you've got a couple of years to prepare for the CPRA, which is scheduled, for the most part, to take effect at the start of 2023, giving you valuable time to begin refining your vendor management process.

There are a few big takeaways concerning the CPRA for businesses and their vendors:

Service Providers vs. Contractors:

First, the CPRA defines a new category of data recipient called a "contractor," which includes some nuanced distinctions between it and the service provider designation that will likely require businesses to draw differences among their vendors and decide which title applies.[1] The CPRA's regulations will flesh out the extent to which contractors and service providers can process personal information for their purposes and combine it with personal information from other businesses. The CPRA's newly created privacy agency—the California Privacy Protection Agency—is expected to issue the first round of regulations as soon as summer 2021. Therefore, businesses will have to monitor CPRA regulations to understand service provider-contractor distinctions as they begin to categorize vendors and enter into agreements with them accordingly.

[1] Though there is seemingly some confusion in the market on this point, the CCPA already defines a fourth category of party (outside of business, service provider and third party) in Cal. Civ. Code § 1798.140(w)(2). The CPRA's newly defined contractor largely pulls from Cal. Civ. Code § 1798.140(w)(2) of the CCPA with additional contractual obligations being required to designate a data recipient as such, discussed below.

Mandatory Agreements:

Second, the CPRA explicitly requires businesses to have contracts in place with *all* recipients of personal information, including service providers, contractors, and "third parties." Under the CCPA, this requirement was merely implied; contracts were only required, with specific language, to designate certain vendors or parties as service providers. Now, the result of not having CPRA-specific language in your agreements with vendors and other data recipients is that your organization will be explicitly violating the CPRA. Unfortunately, the specific language to designate parties as service providers and contractors remains and has been heightened, and businesses will likely not be able to rely on the agreements, amendments, and addenda they entered into for purposes of the CCPA.

Limits on Retention:

Finally, the CPRA will require businesses to disclose the length of time they intend on retaining personal information on a category-by-category basis. The extent to which this requirement will force businesses to consider the duration of their vendors' retention of data on their behalf in this disclosure is not clear. Nonetheless, businesses with either loose or non-existent data retention standards should begin to prepare for these disclosure requirements and address their vendors' retention of data as part of any developed policy. Likewise, vendors should prepare for their customers to begin imposing data retention requirements due to these new provisions in the CPRA. Customers and vendors alike that are already complying with the EU's General Data Protection Regulation ("GDPR") should be familiar with these requirements and should be able to translate some of the work they have previously done to the CPRA.