ALERTS

California Privacy Rights Act Reminder: Enforcement Begins July 1, 2023

June 20, 2023

As a reminder, on July 1, 2023, the California Attorney General and the newly created California Privacy Protection Agency will begin enforcing the California Privacy Rights Act ("CPRA"), the amended version of the California Consumer Privacy Act ("CCPA") that went into effect on Jan. 1. [1] Given the CPRA's expanded scope, more private fund managers are subject to its requirements.

In advance of the July 1 enforcement date, fund managers subject to the CPRA should ensure they are in compliance. Below, we republish our December 2022 *Alert* with key takeaways for fund managers.

Schulte December 2022 *Alert* The New California Privacy Rights Act: Key Takeaways for Private Fund Managers

On Jan. 1, 2023, the operative provisions of the California Privacy Rights Act ("CPRA") go into effect with enforcement scheduled to begin on July 1, 2023, for violations on or after July 1, 2023.[2] Because the CPRA is more expansive in application than the California Consumer Privacy Act ("CCPA") that it amends, more private fund managers and more data are in scope. Additionally, certain moratoriums that applied to the CCPA are also set to expire on Jan. 1. Thus, private fund managers that previously were not subject to the CCPA should consider whether they now must comply with the CCPA and the CPRA, and private fund managers already subject to the CCPA will have to make updates, including to privacy notices for California residents. For many private fund managers that are

Copyright © 2025 Schulte Roth & Zabel LLP

Attorney Advertising

in scope of the CPRA, the compliance burden is likely to be relatively limited.

The CPRA Applies to Any Business With Sufficient Connection to California, Including Private Fund Managers

The law applies to any business (regardless of whether it is located in California) that had at least $25 million in gross annual revenue in the preceding calendar year (even if such revenue has no nexus to California) [3] and that collects personal information from California "consumers." In the private fund context, "consumer" includes a prospective investor, service provider, employee, job applicant or independent broadly in the private fund context. Entities that share "common branding" and share personal information will be subject to the CPRA's requirements if any one of them meets the requirements.[4]

Expanded Scope of the CPRA

One key difference is that the California legislature has not extended the business-to-business ("B2B") moratorium that up until now has applied to the CCPA. The moratorium had the effect of only applying the CCPA to California residents acting in their personal capacity as opposed to those acting on behalf of an entity. As a practical matter, the lack of a B2B moratorium expands the scope of the CCPA as of January 1 and also the CPRA for private fund managers. For example, as a result of the B2B moratorium, many private fund managers were only in scope if they had prospective *natural person* investors in California. However, the CCPA and the CPRA now also will reach prospective *institutional* investors if the investors have California employees or agents from whom the private fund manager collects personal information. For example, private fund managers who have the personal phone number of a California representative of a prospect pension plan investor would be in scope. It similarly encompasses service providers that have California employees from whom the private fund manager collects personal information.

As before, California employees, independent contractors and job applicants are still in scope and, because of the expiration of an employment-related moratorium, now will get the full rights afforded to other California residents. Previously, they had more limited rights than

Copyright © 2025 Schulte Roth & Zabel LLP
Attorney Advertising

California residents in other contexts. As a practical matter, this means that California employees, independent contractors and job applicants should now get the same disclosures as other California residents.

Similar to the CCPA, the CPRA exempts any information that is "subject to" the Gramm-Leach Bliley Act ("GLBA") or Regulation S-P. This GLBA exemption effectively covers all information that fund managers collect about their existing investors, including information collected at the onboarding stage. For example, name, contact information, social security or other tax identification number and bank routing information collected in the context of a subscription agreement is covered by the GLBA and therefore CPRA-exempt. However, because Regulation S-P does not reach information collected about prospective investors prior to onboarding, such information will be subject to the CPRA. Further, the GLBA exemption does not apply to other personal information collected by private fund managers that is not covered by GLBA (e.g., employee information).[5]

Compliance With the CPRA

Although the CPRA's provisions are unlikely to impose significantly higher compliance burdens on private fund managers already subject to the CCPA, there are a few recommended steps to ensure compliance with the CPRA:

- **Inventory Data Collected from Prospective Investors, Employees, Job Applicants and Business Contacts in California:** Given the CPRA's expanded reach, firms should take stock of California residents from whom they collect personal information and the nature of the information collected – particularly now that personal information from California representatives of prospective institutional investors and service providers is in scope.[6]

- **Update Website Privacy Notices**: Firms should update the privacy notices on their websites, if they have a website, to ensure that they appropriately describe the businesses' collection, use and sharing of personal information. CPRA privacy notices should include information regarding the CPRA's new and expanded consumer privacy rights as well as any collection or use of "sensitive personal information." Firms should ensure that the language in their notices describing the collection and use of personal information is "straightforward" and "easy

Copyright © 2025 Schulte Roth & Zabel LLP
Attorney Advertising

to understand."[7] Like the CCPA, the CPRA requires that these policies be updated at least once every 12 months.

- **Disclosures at the "Point of Collection" of Personal Information:** In addition to website disclosures, private fund managers must also make disclosures at or before the "point of collection" of the personal information. "Point of collection" is still not defined in the CPRA. Many private fund managers satisfy this requirement by including a link in their email footers to the website notice given email is generally an early point of contact with California residents. Note that including California privacy notices in subscription documents or with the distribution of other annual privacy notices does *not* satisfy the CPRA's disclosure requirements.

- **Revisit Third-Party, Service Provider and Contractor Agreements:** The CPRA will require that businesses have written agreements in place with any services providers to which they disclose personal information or any third parties to which they sell personal information.[8] Private fund managers should review and amend applicable agreements to ensure compliance with the CPRA's outlined obligations. For the time being, private fund managers should also consider reserving the right to make further amendments to these agreements based on the CPRA's implementing regulations, which have not yet been finalized.

CPRA Considerations for Alternative Data Diligence

Private fund managers that use alternative data for investment research will want to confirm during due diligence of alternative data providers that the collection of any personal information from California residents by the vendor or any downstream supplier complies with the CPRA. Further, even though "de-identified information"[9] and "aggregate consumer information"[10] are excluded from the definition of "personal information" under the CPRA,[11] private fund managers will want to ensure that the data sets they receive meet the CPRA's requirement that the de-identification/aggregation cannot be readily reverse-engineered.

The CPRA's more robust exception for "publicly available" information should be welcome news for web scrapers. Under the CCPA, "publicly available" was limited to information made available from federal, state or

Copyright © 2025 Schulte Roth & Zabel LLP
Attorney Advertising

local government records. Thus, for example, when scraping the public portions of social media sites, personal information of California residents was in scope of the CCPA even where the California resident had chosen to make such information public.[12] The CPRA, however, addresses some of the anomalous results this caused by expanding the exclusion for "publicly available" information to include information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.[13]

Authored by *Alexander M. Kim, Kelly Koscuiszka, Philip J. Bezanson, Steven M. Appel and Marissa Volpe.*

If you have any questions concerning this Alert, please contact your attorney
at Schulte Roth & Zabel or one of the authors.

---

[1] While the CA AG and California Privacy Protection Agency can only bring enforcement actions for violations of the CPRA that occur on or after July 1, 2023, violations of the CCPA that it amended that occurred prior to July 1, 2023, can still be the basis for an enforcement action.

[2] The CPRA will be enforced by a new agency – the California Privacy Protection Agency.

[3] The $25 million threshold is not limited to revenue earned in California or from California residents. The CPRA also applies to any business that (a) alone or in combination, annually buys, sells or shares the personal information of 100,000 or more California consumers or households or (b) derives 50 percent or more of its annual revenues from the sale or sharing of personal information. Cal. Civ. Code § 1798.140(d)(1)(A)-(C).

[4] Cal. Civ. Code § 1798.140(d)(2) ("'Common branding' means a shared name, servicemark, or trademark that the average consumer would understand two or more entities are commonly owned.").

[5] *See* Cal. Civ. Code § 1798.145(c)(1)(e).

[6] The CPRA includes limitations on the collection, use, retention and sharing of a consumer's personal information to what is "reasonably

Copyright © 2025 Schulte Roth & Zabel LLP
Attorney Advertising

necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes." Cal. Civ. Code § 1798.100(c).

[7] *See* Cal. Code Regs. Tit. 11 § 7012.

[8] These written agreements must: (1) specify that the personal information is sold or disclosed only for limited and specified purposes; (2) require the third party, service provider or contractor to comply with the obligations of CPRA and "to provide the same level of privacy protection" as required by CPRA; (3) permit the business "rights to take reasonable and appropriate steps" to ensure any personal information transferred is used in a manner consistent with CPRA; (4) require the third party, service provider or contractor to "notify the business if it makes a determination that it can no longer meet its obligations under" CPRA; and (5) grant the business the right, upon notice, "to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information." Cal. Civ. Code § 1798.104(d). Relationships with service providers and contractors have additional requirements as laid out in their respective definitions under the CPRA. *See* Cal. Civ. Code § 1798.140(ag); *see also* Cal. Civ. Code § 1798.140(j).

[9] De-identified is defined as "information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information: (1) [t]akes reasonable measures to ensure that the information cannot be associated with a consumer or household[;] (2) [p]ublicly commits to maintain and use the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision[;] (3) [c]ontractually obligates any recipients of the information to comply with all provisions of this subdivisions." Cal. Civ. Code § 1798.140(m).

[10] "Aggregate consumer information" is defined as "information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. . . . [It] does not mean one or more individual consumer records that have been deidentified." Cal. Civ. Code § 1798.140(b).

Copyright © 2025 Schulte Roth & Zabel LLP
Attorney Advertising

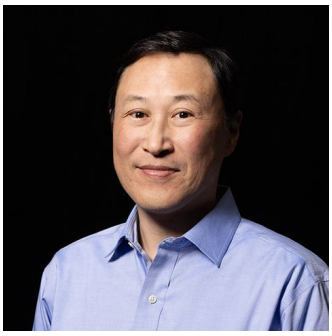
[11] *See* Cal. Civ. Code § 1798.140(v)(3).

[12] Cal. Civ. Code § 1798.140(o)(2) (to be replaced by Cal. Civ. Code § 1798.140(v)(3)).

[13] Cal. Civ. Code § 1798.140(v)(2).

This communication is issued by Schulte Roth & Zabel LLP for informational purposes only and does not constitute legal advice or establish an attorney-client relationship. In some jurisdictions, this publication may be considered attorney advertising. © 2023 Schulte Roth & Zabel LLP. All rights reserved. SCHULTE ROTH & ZABEL is the registered trademark of Schulte Roth & Zabel LLP.

Related People



Alexander Kim

Partner

New York

Kelly Koscuiszka

Partner

New York

Philip Bezanson

Special Counsel

Washington, DC

Steven Appel

Associate

New York

Copyright © 2025 Schulte Roth & Zabel LLP

Attorney Advertising

Marissa Volpe

Associate

New York

Practices

INVESTMENT MANAGEMENT

Attachments

Download Alert

Copyright © 2025 Schulte Roth & Zabel LLP

Attorney Advertising