ALERTS

The California Consumer Privacy Act: Key Points for Private Fund Managers

December 6, 2019

Jan. 1, 2020 is the effective date of the California Consumer Privacy Act ("CCPA"), the country's first comprehensive privacy law. For many private fund managers, the compliance burden presented by the CCPA is likely to be relatively limited. Still, there are several key aspects that are important for fund managers to keep in mind.

Who Must Comply?

Despite its name, the CCPA goes well beyond California "consumers," as that term is typically used — the Act defines a "consumer" as any "natural person who is a California resident."[1] The law applies to any business with at least $25 million in gross annual revenue[2] that collects personal information from "consumers," which in the private fund context could be an investor, prospective investor, employee, job applicant, independent contractor or potentially even a business contact who resides in California.[3] A business that does not meet the threshold may still be subject to the CCPA if it controls, or is controlled by, a business that meets the criteria and shares common branding.[4] This expansive covered business concept means that, in the private fund context, managers will need to assess the potential coverage of the CCPA at both the adviser or sponsor level as well as for the funds themselves.

Like "consumers," the definition of "personal information" receives broad treatment, being defined as information that "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."[5] This is much broader than other privacy laws and expressly includes items such as email addresses, internet protocol addresses and biometric information.[6]

What Does the Law Require?

At a high level, the CCPA requires covered businesses that collect personal information about California residents to:

- Make certain disclosures concerning the collection and use of personal information, including the purposes for which the personal information is used and the categories of third parties with whom the personal information is shared;
- Inform individuals of their rights to request detailed information about how their personal information is used or to request deletion of their personal information, and implement policies to comply with such requests;
- Provide "conspicuous" notice and a means for individuals to opt out of the sale[7] of their personal information; and
- Be accountable for data breaches that result from a failure to maintain reasonable security practices.

What Is the Timing?

The CCPA goes into effect on Jan. 1, 2020.

The California Attorney General, who is primarily tasked with enforcement, is still in the process of finalizing regulations. Because final regulations are unlikely to be published before Jan. 1, 2020, the CCPA precludes the commencement of any enforcement actions prior to July 1, 2020;[8] actions brought after July 1, however, may relate to conduct between Jan. 1 and July 1, 2020. The attorney general may assess civil penalties of up to $2,500 per unintentional violation and $7,500 per intentional violation. A business is not liable if it cures any noncompliance "within 30 days after being notified of alleged noncompliance,"[9] although the Attorney General has stated some violations may not be capable of being cured after the fact.

The private right of action provided for in the CCPA is limited solely to consumers whose personal information (defined more narrowly for these purposes)[10] has been subject to unauthorized access or disclosure as a result of the covered business' failure to maintain reasonable security procedures.[11] Further, a consumer must give the business 30 days' written notice and an opportunity to cure (if a cure is possible) prior to bringing any action.[12] A consumer may seek statutory damages in an amount of not less than $100 and not greater than $750 per consumer per incident, or actual damages, whichever is greater, as well as an injunction or any relief a court deems proper.[13]

What Investor Information Is Covered?

Personal information that private fund managers collect from existing investors who are individuals (i.e., natural persons) typically will be exempt from the CCPA, but other categories of information are covered:

- *Existing Individual Investors*. Undoubtedly the most pertinent CCPA provision for private fund managers is the exemption for any information collected "pursuant to" the Gramm-Leach-Bliley Act ("GLBA").[14] The GLBA regulates information privacy practices of financial institutions and covers personal information that is collected in the specific context of providing an individual with a financial product or service. This exemption for information collected under the GLBA effectively covers all information that funds collect about their existing investors. 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 CCPA exempt.

- *Prospective Individual Investors*. Because the GLBA does not reach prospective investors, personal information collected from prospective individual (natural person) investors in California will be subject to the CCPA, requiring CCPA disclosures at the point of collection. The method of making these disclosures will depend on the context in which the personal information is collected. For example, a fund manager that makes substantive information available to prospective investors via its website might add CCPA disclosures to an existing online privacy policy. A manager may also add a CCPA disclosure along with other disclosures in pitch books or other marketing materials, or as a notice at the bottom of investor relation emails.

- *B2B Contacts*. Unlike most privacy laws, the CCPA's expansive definition of "personal information" encompasses information that identifies an individual person exchanged in a purely business-to-business context, such as the email address of a California resident acting on behalf of an institutional investor or service provider. Due to the difficulties raised by businesses over complying with the CCPA for this category of information, the California legislature has placed a one-year moratorium on the statute's coverage for personal information obtained by a business from a California resident acting for another entity occurring "solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from" the other entity.[15] As such, the moratorium delays enforcement for things like the professional email address of a California resident working on behalf of an institutional investor or service provider but does not appear to apply to information obtained from a third party, such as a list provider.

What HR-Related Information Is Covered?

The CCPA requires disclosures to be made to employees, job applicants and independent contractors in California about the categories of personal information collected and the purposes for which the personal information will be used. This can be accomplished by adding notices in job applications, employee handbooks and independent contractor agreements. For persons already engaged by a fund manager, disclosure can be made through circulating an email with a link to the disclosures. In this context, there is a one-year moratorium during which the disclosure requirements are limited to a description of the categories of information being collected and the purpose for which the categories of information will be used. Absent an extension to the moratorium or amendment, the CCPA's more extensive disclosure requirements will apply commencing Jan. 1, 2021.[16]

Is Alternative Data Covered by the CCPA?

Alternative data in which personal information has been "deidentified" or "aggregated" is excluded from the CCPA.[17] Fund managers should undertake vendor diligence to confirm the data has been "de-identified" consistent with the specific requirements of the CCPA (e.g., the service provider must implement business processes that specifically prohibit re-

identification of the information)[18] and confirm service provider agreements contain language required for CCPA compliance.

What About Sharing Personal Information with Service Providers?

The CCPA imposes various obligations with respect to sharing consumer information. As a threshold matter, a business must disclose to consumers the purposes for which it shares personal information.[19] This can be accomplished by adding language in an online privacy policy or similar disclosure. The CCPA contains certain more burdensome obligations with respect to the "sale" or use for a "commercial purpose"[20] of consumer information, such as providing the ability to "opt out," providing consumers the right to request deletion of their information or responding to other individual information requests.[21] However, transferring a consumer's personal information to a service provider for a "business purpose" is generally an exception to what constitutes a "sale" under the CCPA.[22] Most of the purposes for which fund managers share information with service providers will fall into one of the CCPA's seven categories of "business purposes," which are, in short:

(1) Auditing interactions with consumers;

(2) Detecting security incidents and protecting against illegal activity;

(3) Debugging to repair errors;

(4) Short-term "transient" uses;

(5) Performing services on behalf of the business that collected the information;

(6) Internal research for technological development; and

(7) Maintaining and verifying quality and safety.[23]

Thus, these additional requirements are likely inapplicable to how many private fund managers share information with service providers.

The CCPA requires businesses to contractually prohibit its service providers from retaining, using or disclosing the consumer's personal information for any purpose other than performing the services specified in the contract.[24] Therefore, fund managers will want to review, and

possibly amend, existing agreements with service providers that have access to personal information of consumers and update vendor due diligence questionnaires to account for CCPA-related requirements.

How Does CCPA Compliance Relate to GDPR Compliance?

Despite frequent analogies between the GDPR and the CCPA, GDPR compliance does not ensure CCPA compliance because there are significant differences in requirements, definitions and scope.[25] That said, the data inventorying and mapping that many firms have already undertaken for purposes of GDPR compliance can be leveraged to assess the categories of information collected and how such information is used for purposes of CCPA compliance.

Conclusion

This is a rapidly changing and dynamic regulatory environment, in which the CCPA is one of the many pieces. The requirements of the CCPA are themselves evolving as the Attorney General has yet to issue final regulations. There is also the likelihood that further amendments will be proposed in 2020. As other states are considering comprehensive privacy regulation similar to the CCPA, many businesses are advocating for a federal law that would create uniform requirements.

Authored by Brian T. Daly, Marc E. Elovitz, Edward H. Sadtler and Kelly Koscuiszka.

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

---

[1] California Consumer Privacy Act, CAL. CIV. CODE § 1798.140(g).

[2] *Id.* § 1798.140(c)(1)(A). The statute does not specify whether the $25-million gross annual revenue threshold is based on gross revenue in California, the United States or worldwide. For the time being, fund managers are advised to assume it is worldwide revenue.

[3] *Id.* § 1798.145(a)(6). For a company without a physical presence or affiliate in California, the statute provides a narrow exemption if the "commercial conduct takes place wholly outside of" and it is not otherwise

"doing business" in California. This requires not having a single investor, prospective investor, employee or independent contractor in California.

[4] *Id.* § 1798.140(c)(2). Two other criteria less likely to apply to private funds are businesses that (i) annually buy, sell, receive or share, for commercial purposes, personal information of 50,000 or more consumers, households or devices; or (ii) derive 50% or more of annual revenue from selling consumer's personal information. *Id.* § 1798.140(c)(1)(B)-(C).

[5] *Id.* § 1798.140(o)(1).

[6] *Id.* § 1798.140(o)(1)(A).

[7] "Sale" is defined broadly to include any disclosure or dissemination of personal information "for monetary or other valuable consideration." *Id.* § 1798.140(t).

[8] *Id.* § 1798.185(c).

[9] *Id.* § 1798.155(b).

[10] For purposes of the private right of action, the definition of "personal information" is defined as an individual's unencrypted and non-redacted first name or initial and/or last name *combined with* certain other types of personal information, such as social security number, account number or credit card number. *Id.* § 1798.150(a)(1).

[11] *Id.* § 1798.150(a)(1).

[12] *Id.* § 1798.150(b).

[13] *Id.* § 1798.150(a)(1).

[14] *Id.* § 1798.145(e). The CCPA contains exemptions in relation to certain other statutes, including the California Information Privacy Act, but the GLBA exemption is the most relevant to fund managers.

[15] *Id.* § 1798.140(o) (as amended by AB-1355). The moratorium does not apply to the private right of action or the right to opt out of selling for these type of business contacts.

[16] *Id.* § 1798.145(h).

[17] *See,* e.g., *Id.* §§ 1798.140(o)(2); 1798.145(a)(5).

[18] *Id.* § 1798.140(h).

[19] *Id.* § 1798.100(b), 1798.140(t)(2)(C)(i).

[20] "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. *Id.* § 1798.140(f).

[21] *Id.* § 1798.140(t)(2)(C); 1798.140(v).

[22] *Id.* § 1798.140(t)(2).

[23] *Id.* § 1798.140(d).

[24] *Id.* § 1798.140(v).

[25] The California Attorney General has in fact specifically rejected a safe harbor exemption for GDPR-compliant businesses. *See* OFFICE OF THE ATTORNEY GEN., STATE OF CAL. DEP'T OF JUSTICE, INITIAL STATEMENT OF REASONS (ISOR) (2019), available here.

Related People

Marc Elovitz

Partner

New York

Kelly Koscuiszka

Partner

New York

Practices

CYBERSECURITY AND DATA PRIVACY

INVESTMENT MANAGEMENT

REGULATORY AND COMPLIANCE

Attachments

Download Alert