Proskauer

Hedge Fund Firms – What Do You Need to Consider Under the CCPA?

December 11, 2019

The California Consumer Privacy Act of 2018 (CCPA) will take effect on January 1, 2020, and hedge fund firms may be subject to the CCPA even if they are already compliant with the Gramm-Leach-Bliley Act (GLBA), do not have a place of business in California or do not target California consumers or businesses as those terms are broadly defined in the CCPA.

The CCPA is an expansive new privacy law that gives "consumers" (broadly defined as natural persons who are California residents — potentially including current and prospective hedge fund clients and investors and personnel and job applicants of the hedge fund firm) four basic rights in relation to their personal information:[1]

1. the **right to know**, through a general privacy policy and with more specifics available upon request, what personal information a business has collected about them, from where it was sourced, for what it is being used, whether it is being disclosed or sold, and to whom it is being disclosed or sold;

2. the **right to "opt out"** of allowing a business to sell its personal information to third parties (or, for consumers who are under 16 years old, the right not to have its personal information sold absent its, or its parent's, opt-in);

3. the **right to have a business delete its personal information**, with some exceptions; and

4. the **right to receive equal service and pricing from a business**, even if it exercises its privacy rights under the CCPA.

To whom does the CCPA apply?

Only "Covered Businesses" are within the scope of the CCPA, so hedge fund business must determine whether the fund itself, the fund's manager, general partner, or other similar entities fit within that definition. Covered Businesses are those that:

1. Do business in California;

    Practice Tip: Although "doing business in California" is not defined or addressed in the CCPA, the California tax laws describe "doing business" as meeting any one of the following: (1) engaging in any transaction for the purpose of financial gain within California; (2) being organized or commercially domiciled in California; or (3) having California sales, property or payroll exceed certain threshold amounts which are subject to change each year (payroll threshold for 2018 was $58,387)).

2. Collect consumer personal information or have it collected on their behalf; and

    Practice Tip: The term "consumer" can include a current or prospective client, fund investor, employee and job applicant. This provision may be triggered if hedge funds are using a third party to collect certain client, investor, employee or job applicant personal information on their behalf.

3. Determine the purpose and means of processing that personal information.

In addition to the above requirements, to be considered a Covered Business, an entity must also satisfy at least one of the following elements:

1. Have annual gross revenue of over $25 million;

    Practice Tip: The annual $25 million gross revenue threshold includes parent companies and subsidiaries sharing the same branding even if they do not meet the applicable threshold themselves. The revenue provision needs additional clarification as drafted, and it is anticipated that this provision will be subject to litigation in the courts. Many companies are erring on the side of over-inclusion of revenue.

2. Buy, receive, sell or share the personal information of 50,000 or more consumers, households or devices for commercial purposes, or

3. Derive 50% or more of annual revenue from selling consumers' personal information.

How does GLBA compliance affect the CCPA?

The CCPA does not apply to personal information collected, processed, sold, or disclosed pursuant to the GLBA and implementing regulations. Investment advisers registered with the U.S. Securities and Exchange Commission are subject to the GLBA. However, the GLBA exception does not categorically exempt investment advisers and other financial institutions from the CCPA. Rather, the GLBA exception carves out specific categories of data. This carve-out begs the question of what information falls into this exception and what information hedge fund businesses collect that fall outside the scope of the GLBA exception.

The GLBA protects non-public personal information (NPI) of consumers, meaning information that is not publicly available that, in connection with a financial product or service, (i) the consumer provides, (ii) results from a transaction, or (iii) the entity otherwise obtains. Notably, the GLBA applies to "consumers," meaning individuals, as opposed to entities. However, the GLBA may protect individuals affiliated with entities, such as authorized signatories. NPI could include account balances, credit account data, or even web cookies if collected in association with a financial product. 12 C.F.R. §1016.3(q)(2).

The CCPA is broader than the GLBA with respect to the information to which it applies. Notably, the CCPA applies to ***all personal information relating to*** a consumer (e.g., a current or prospective investor), not just NPI. Hedge fund firms will need to carefully evaluate the nature of the information they obtain and their relationship with individuals with whom they do business, because information may be considered NPI if "otherwise obtained" in connection with providing a financial service.

The CCPA is also broader than the GLBA regarding whose information it applies to, though that breadth has been limited by recent amendments that are expected to be signed into law by the California governor. Further, where the GLBA is limited in protecting entity-affiliated individuals, such as employees or business-to-business contacts, Assembly Bill 25 and Assembly Bill 1355 amend the CCPA to address these issues: the former exempts certain employment-related data[2] and the latter exempts personal information collected in certain business-to-business transactions. Neither amendment provides complete exemptions, however, leaving in place some notice and opt-out obligations to consider.

Thus, the CCPA covers information outside the scope of the GLBA, which would be any personal information relating to a consumer or household that is not NPI and not covered by a separate CCPA exception. This information could include marketing data and statistics or data scraped or bought outside of the ordinary relationship with the individual.

> **Practice Tip:** Assuming that the hedge fund firm meets the CCPA thresholds and collects information that is not NPI covered by the GLBA, it should decide using a risk-based assessment whether to implement CCPA compliance across all personal information or to identify the personal information that does not fall under the GLBA and is for California residents and treat that information differently. Specific notices and means of identifying California residents would need to be operationalized and put into practice with respect to this subset of personal information that is covered by the CCPA.

How should hedge fund firms handle alternative data sources?

Whether scraping data or purchasing data from third party vendors, hedge fund firms should apply the same CCPA principles to such data. The CCPA does not apply to anonymized, aggregated, or deidentified data collected by a business, but firms may need to dedicate more resources to evaluating whether such information is truly free from personal information. Among other things, they should consider negotiating representations regarding such data in agreements with data providers. Firms may be wondering how to handle opt-out requests with regard to their alternative data sources to the extent any data contains personal information. No guidance has been issued on these matters yet, but presumably firms would not have to honor such requests where the data is fully anonymized or deidentified.

If the CCPA applies, what should I do?

If the CCPA does apply to your firm, you should:

1. *Understand how personal information flows in and out of your business*: Create an inventory, or data map, of all personal information that you collect, use, disclose, or sell pertaining to California residents, households and devices, as well as sources, storage locations, usage and third parties with whom it is shared. Determine whether you are "selling" any personal information, in which case other steps must be taken.

Practice Tip: A "sale" or "selling" of personal information under the CCPA includes "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means" the personal information of a California resident to another business or third party for "monetary or other valuable consideration." This is an extremely broad definition and even the sharing of personal information to third-party and networks through cookies may constitute a sale.

2. *Revise privacy notices and websites*: Disclose categories of personal information collected and how data is used, shared and sold. Clearly describe the rights of California residents, including: (a) the right to access personal information; (b) the right to delete personal information; and (c) the right to opt out of the sale of personal information.

3. *Prepare to receive, process and respond to California residents' request*: Create internal procedures and train applicable personnel.

4. *Do not discriminate against clients, investors, employees, job applicants and other consumers by virtue of their privacy settings:* Businesses cannot deny goods or services, charge different prices for goods or services, or provide a different quality of goods or services to those consumers who exercise their privacy rights.

5. *Add required provisions to contracts with service providers:* To avoid liability under the CCPA for the actions of your service providers, you can include the following prohibitions in your agreements with service providers, provided that you do not have actual knowledge, or reason to believe, that the service provider intended to commit the violation in question:

a. The service provider may only retain personal information "for the specific purpose of performing the services specified in the contract" or otherwise permitted under the CCPA;

b. The service provider may only use the personal information "for the specific purpose of performing the services specified in the contract" or otherwise permitted under the CCPA, or;

c. The service provider may only disclose the personal information "for the specific purpose of performing the services specified in the contract" or otherwise permitted by the CCPA.

How is it enforced?

The CCPA can be enforced through actions brought by the California attorney general and, for certain violations, through private law suits brought by consumers. Note that the California attorney general recently issued proposed rules that would expand obligations regarding initial notices at the collection of personal information, privacy policies, rights regarding sales of personal information, and notice of financial incentives for retention or sale of personal information, amongst other changes. The proposed rules will undergo a comment period in December 2019 and will be enforceable by the attorney general on July 1, 2020.

Please contact Proskauer's Privacy & Cybersecurity team and/or your regular Proskauer contact for more information and to discuss how we can assist you in complying with the CCPA.

---

[1] "Personal information" is defined, in part, as information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Note that the definition of "Personal information" does not include publicly available information or consumer information that is deidentified or aggregate consumer information. CCPA § 1798.140(o).

[2] As of this writing, the employment-related data exemption sunsets on January 1, 2021.

Related Professionals

- **Christopher M. Wells**
  Partner
- **Christina Kroll**
  Associate