VORYS

Publications

# *Privacy Alert*: California Attorney General May Commence Enforcement Actions for CCPA Violations on July 1, 2020

### Related Attorneys

Eric W. Richardson

Jacob D. Mahle

J.B. Lind

Brent D. Craft

### Related Services

Data Strategy, Privacy and Security

**CLIENT ALERT** | 6.29.2020

As most businesses are aware, the California Consumer Privacy Act of 2018 (CCPA) went into effect on January 1, 2020. The key components of the CCPA include a number of new rights regarding consumer data as well as new compliance obligations for covered businesses.

Consumers are provided the right to obtain their personal information collected by businesses in the prior twelve months, and are entitled to know the categories of personal information collected, sold, and disclosed by the business, the categories of third-party recipients who received the personal information, and the uses of the consumer's personal information. Consumers are further afforded the right to obtain deletion of personal information and to opt-out of the sale of personal information. On the compliance side, businesses are required to assess and document data practices related to the collection, disclosure, and use of personal information and to publish specific contact information to allow consumers to exercise their rights.

The act broadly applies to "businesses," which is defined to include any for-profit legal entity (e.g., corporation, partnership, LLC) that does business in the State of California, that collects consumers' personal information, and that meets **one** of the following thresholds:

- Has gross revenue in excess of $25,000,000;
- Buys, receives, or sells for commercial purposes the personal information of 50,000 or more consumers, households, or devices; **or**
- Derives 50 percent or more of its revenue from selling consumers' personal information

**Starting July 1, 2020, the California Attorney General's office may bring administrative enforcement actions for violations of the CCPA and its requirements.** Applicable provisions of the CCPA allow the California Attorney General to seek, after a 30-day notice and cure period, penalties of up to $2,500 per violation, and $7,500 per intentional violation.

In light of the looming administrative enforcement commencement date, it is very important for businesses to closely evaluate their processes, procedures, and vendor relationships for CCPA compliance. While many of the actions listed below are highly recommended as cybersecurity/data privacy best practices regardless of the jurisdictions in which your company does business, they take on heightened importance on July 1, 2020 for those entities that do business in California and meet any of the CCPA application thresholds listed above.

1. **Know what consumer data you hold and purge any consumer data that is not necessary.** As explained above, the CCPA gives consumers substantial rights regarding their personal information and imposes a number of obligations on companies that hold such data. In order to comply with CCPA requirements, it is essential that companies know what consumer data they hold and where/how to access it so that consumer requests and demands pursuant to the CCPA can be quickly addressed. Additionally, companies should ensure that they are not holding any consumer data that is not essential for their business to avoid unnecessary obligations under the CCPA and to limit the amount of personal information that could be subject to a breach.

2. **Update your company's privacy policy and be prepared to periodically review it.** The CCPA requires businesses to provide notice to consumers regarding the personal information that it collects, the purposes for which the information is collected, and how the company collects, uses, and shares the information. The notice must also inform consumers of their rights (pursuant to the CCPA) associated with their personal information and how they can exercise them. This notice/disclosure must account for the company's practices over the last year, and must be updated on an annual basis. Because this requirement directly impacts the consumer rights enshrined in the CCPA, a careful compliance review of company privacy policies and relevant website sections is essential.

3. **Evaluate the soundness of and appropriately update your company's data security processes and procedures.** The CCPA creates a private right of action for any consumer whose "nonencrypted or nonredacted" personal information is subject to unauthorized access and exfiltration "as a result of a business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate…to protect the information." In such an action, affected consumers can recover the greater of actual damages or statutory damages of up to $750 per consumer per incident. Thus, it is very important that companies have in place appropriate and up-to-date data security processes and procedures that are reasonably designed to safeguard consumer data.

4. **Review vendor agreements and revise them as necessary to account for CCPA compliance issues.** To the extent that your company shares consumer information with vendors and service providers, any applicable agreements should be reviewed and appropriately updated to account for CCPA requirements. As a general matter, the vendor should only be given access to consumer data that it needs, and the vendors should agree that it will only use, retain, and/or disclose data for purposes stated in its contract. Vendor agreements should also include provisions requiring the vendor to maintain security procedures reasonably designed to protect the consumer data in its possession, to

cooperate with any consumer requests regarding personal information (a necessity for CCPA compliance), to promptly report data breaches, and to indemnify the company for data security failures by the vendor.

5. **Train your staff so that it can adequately respond to consumer demands and requests.** The CCPA gives consumers significant rights regarding the use of their data and allows them to demand deletion and/or opt out of the sale of their data. Accordingly, company employees must know how to quickly collect customer information in order to respond to consumer requests, and be versed in deletion protocols so that consumer demands can be swiftly executed. Ensuring that all relevant employees are trained in the processes that will allow them to address questions and instructions regarding consumer data held by the company is critical to CCPA compliance.

If you have concerns about CCPA compliance and/or administrative enforcement issues, or any questions regarding general cybersecurity/data privacy best practices please contact a member of the Vorys cybersecurity team: Eric W. Richardson, Jacob D. Mahle, JB Lind or Brent D. Craft.