

Five Things to Do Now to Prepare for the CCPA Enforcement Deadline on July 1, 2020

Article By:

Matthew J. Marino

Kathryn Garcin

As you likely know, the California Consumer Privacy Act of 2018 (CCPA) went into effect on January 1, 2020. The CCPA is revolutionary legislation relating to California consumers' rights in their Personal Information (as defined in the CCPA), and is estimated to impact 75 percent of California businesses. Online video conference companies Zoom and Houseparty have already been sued under the CCPA's private right of action for alleged breaches of Personal Information of California residents. Beginning on July 1, 2020, (despite a request for delay from affected California businesses due to the COVID-19 pandemic), the California Attorney General's office may bring enforcement actions with penalties for any violation of the CCPA. This is a broader right than the one granted to consumers to bring private rights of action. The AG may enforce CCPA violations after a 30-day notice and cure period seeking penalties of up to \$2,500 per violation, or up to \$7,500 per intentional violation. While the definition of a "violation" under the CCPA is unclear, it is possible that each consumer and each request under the CCPA will be individually treated as a "violation." For example, if a business fails to provide adequate notice when it collects Personal Information, and it collects the Personal Information of 1,000 consumers before revising its notice procedure, the statutory penalty could be up to \$2.5 million.

Therefore, it is important for companies to make any final and necessary preparations now to prepare for the possibility of CCPA enforcement beginning on July 1, 2020. Below are five suggested actions to consider as the enforcement date approaches.

1. ENSURE YOUR PRIVACY NOTICE AND WEBSITE ARE UPDATED

Businesses must provide sufficient notice to a consumer identifying the categories of Personal Information the business collects and the purpose of collection. Businesses must also disclose their practices regarding the collection, use, and sharing or sale of Personal Information. Other requirements include: a description of the consumers' rights, the methods for consumers to exercise them, the methods by which the business will verify the consumers' identity, and the ability for consumers to opt out of the sale of their information. The disclosure must cover the past 12 months and it must be updated at least every 12 months to account for any new practices. If your company sells Personal Information or receives compensation or other benefits from sharing Personal

Information, you may be required to post a prominent "Do Not Sell My Personal Information" website or link to allow consumers to opt out of the sale of their data.

This is possibly the most critical component of the CCPA: to provide consumers – and any employees located in California – with notice of their rights with respect to their data. The most critical thing a company can do to prepare is to ensure its privacy policies and website are updated to comply with the CCPA.

2. CONDUCT A DATA INVENTORY

The CCPA grants all California consumers the right to know what Personal Information related to the consumer is maintained by a business, and the categories of third parties to whom the business has disclosed or sold Personal Information. Therefore, it is critical that companies be able to promptly assess and respond to these requests. This may require a data inventory, updated regularly, in order to ensure that companies can fully and accurately respond. While companies generally have 45 days to respond, it may be too late to begin this process when a request is received.

3. DOCUMENT A PROCESS AND TRAIN EMPLOYEES TO RESPOND TO CONSUMER REQUESTS

Any employee who is responsible for responding to consumer requests under CCPA must be trained to do so in a manner that is consistent with CCPA and the company's internal policies. Implementing appropriate internal protocols makes this process more efficient and consistent. This will ensure that no deadlines are missed and all responses are as complete and accurate as possible. A clear, well-documented process, with associated employee training, will reduce the risk of penalties.

4. ENSURE YOUR COMPANY HAS APPROPRIATE SECURITY PROCEDURES AND PRACTICES

Under CCPA, California consumers now have a private right of action for breaches of their Personal Information that are due to a company's failure to maintain and implement "reasonable security procedures and practices." Proof of actual damage is not required for recovery; consumers may recover the greater of their actual damages or up to \$750 per consumer per incident in statutory damages. To mitigate the risk of liability, businesses should ensure that they have appropriate practices for the storage and destruction of Personal Information.

5. REVIEW CONTRACTS WITH SERVICE PROVIDERS FOR CCPA ISSUES

If your company discloses Personal Information to service providers, the contract governing the relationship should include CCPA-specific provisions. The service provider should agree by contract to not retain, use or disclose Personal Information other than for the specific purposes specified in the contract. Other recommended provisions include an agreement to assist with consumer rights requests, safeguard all information received, and report data breaches. Consider reviewing your key vendor contracts and amending them to ensure CCPA compliance.

CONCLUSION

With the July 1, 2020, deadline upcoming, now is the time to make any last-minute CCPA assessments or updates.

National Law Review, Volume X, Number 143

Source URL: <https://natlawreview.com/article/five-things-to-do-now-to-prepare-ccpa-enforcement-deadline-july-1-2020>