



The California Consumer Privacy Act: What You Need To Know

March 21, 2019

California has enacted the most important data privacy statute the United States has seen to date. The California Consumer Privacy Act (CCPA) brings European-style data privacy regulations to the United States. The Act:

- covers a wide range of information commonly collected by businesses
- imposes significant disclosure, record keeping, and compliance obligations
- includes stiff regulatory fines and a private right of action for consumers

The CCPA goes into effect on January 1, 2020, but it already covers personal information collected since the beginning of 2019.

The CCPA covers more businesses than you think. The CCPA applies to for-profit businesses that collect and control California resident personal information, do business within the state, and: (a) have annual gross revenues of \$25+ million; *or* (b) receive or disclose the personal information of 50,000 residents, devices, or households; *or* (c) derive more than half of their revenue from the sale of California residents' personal information.

Many more businesses. The CCPA applies to subsidiary entities that share common branding. The 50,000 threshold would be met by a daily average of 137 California visitors to a website. Although it is titled as a "consumer" act, it also covers B2B businesses. Even if a client does not meet these thresholds, one of its customers or business partners is likely to require CCPA compliance by agreement.

The definition of "personal information" is broad. It includes any 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." In addition to names, addresses, SSN, DL or account numbers, other examples include IP addresses, browsing history and purchase history. It may arguably apply to data regarding California employees.

Businesses must give notice of and protect the personal information collected. In a privacy policy or otherwise at collection, a business must disclose the consumer's rights under the CCPA, the categories of



personal information the business collects, the business purpose for each category, and the categories of personal information sold by the business in the past 12 months. It must employ "reasonable" security measures, or risk liability under the Act.

Many websites will need a new "button" that says "Do Not Sell My Personal Information." California has not decided whether the button will be of uniform design, but the law requires it to be clearly set forth on the website and any privacy policy. The CCPA's broad definition of "sale" includes any exchange that benefits the transferor of the personal information.

Businesses will have to identify or delete personal information upon request. Consumers have the right to ask a business about the personal information collected about them, and with whom the business shares it. Consumers may also demand the business delete their personal information. The business is required to respond to these requests within forty-five (45) days at no charge to the consumer.

Sanctions for violations are significant. Fines can run from \$2500 - \$7500 per incident, meaning a violation involving 10,000 residents could result in fines of \$25 million to \$75 million. California residents can bring private suits against violators for any perceived harm, with statutory penalties in the range of \$100 - \$750 per incident. Consumers can seek statutory or actual damages.