



Preparing for the California Consumer Privacy Act

We’re faced with a world in which private companies store, enrich, analyze and sell years of our location history, financial habits and even more confidential information, while criminals devise new methods to access and maliciously exploit that information.

It’s understandable that people are interested in locating, locking down and establishing ownership of their personal data. Beyond unwittingly serving as the main profit driver of many companies and the danger that it’s being held on poorly protected information technology infrastructure, personal data stored by companies is also susceptible to government subpoena.

Increasingly, efforts to define consumer rights over personal data are resulting in new laws and regulations, including the European Union’s General Data Protection Regulation (GDPR), the Delaware Data Breach Law and the California Consumer Privacy Act of 2018 (CCPA). The latter went into effect on January 1, 2020, with enforcement beginning midyear, giving law firms and other organizations little time to ensure they and their clients are compliant. California’s attorney general is actively formulating regulations to enact the CCPA. These rules will help guide businesses in applying the law to their activities.

The CCPA of 2018 broadly provides California citizens the rights to know what personal information a business has collected, sold or disclosed about them; to learn to whom their information was given; to access their information; and to opt out of its sale.

Businesses failing to comply with the law’s provisions face financial penalties that start small but quickly add up.

“The rules also require that businesses planning to sell consumer information provide a notice of such at the time they collect that information from their customers.”

DOES THE CCPA APPLY TO ME?

Many small- to medium-sized businesses will be exempt from the CCPA because they don't trade in consumer data as a main course of business and don't meet the minimum revenue threshold. Nonetheless, it's important that business owners consult with their legal professionals to discuss possible areas in which compliance with these new regulations may be necessary.

The CCPA applies to businesses engaged in collecting, processing, sharing or selling Californians' data **if**:

- They gross over \$25 million in revenue annually; **or**
- They (solely or in combination with others) deal with the personal information of 50,000 or more consumers, households or devices; **or**
- They make over 50% of their revenue from the trading of consumer data.

CCPA REQUIREMENTS

Specifically, the CCPA requires that businesses provide consumers the rights to:

- **Disclosure:** Businesses that collect personal information must disclose to requesting consumers free-of-charge within 45 days:
 - The categories of personal information it collected
 - The categories of sources from which the information was collected
 - The business or commercial purpose for the collection or sale of such data
 - The categories of third parties with whom the business shares personal information
 - The specific pieces of personal information it has collected about that consumer
- **Opt out:** They must also allow consumers to stop the further sharing of their information upon request.
- **Access:** Compliant businesses will inform consumers before or upon the collection of information and provide access to that information to consumers upon request.
- **Deletion:** Businesses must delete and direct their service providers to delete personal information upon request from consumers.
- **Nondiscrimination:** A business cannot discriminate against a consumer because they exercised any of their rights to data privacy.

The rules also require that businesses planning to sell consumer information provide a notice of such at the time they collect that information from their customers. Businesses can satisfy this requirement by posting notices on their websites and mobile apps:

1. A **"Do Not Sell My Personal Information"** or **"Do Not Sell My Info"** link leading to a webpage containing a notice of consumers' right to opt-out *and*
2. A **Privacy Policy link** leading to the business's annually updated online privacy policy that includes the following:
 - Consumers' rights under the CCPA, including their right to opt out of the sale of personal information and a separate link to the "Do Not Sell My Personal Information" page
 - The methods for submitting consumer requests
 - A list of the categories of personal information that the business has collected about consumers, sold about consumers and disclosed about consumers for a business purpose in the preceding 12 months.

GETTING COMPLIANT

Business owners should consult with legal professionals to determine their organizations' duties under the CCPA. While the regulations may seem cut-and-dry upon first glance, the ever-evolving digital and legal landscapes require deep understandings of the issues and nuances specific to each organization.

As a recent Federal Trade Commission settlement with a company for falsely claiming to comply with the GDPR shows, failure to comply can result in sanctions without there being a motivating event, such as a cyberattack or data leak.

More important for your business is that your clients expect you to store their data more safely than you'd store your own.

ABOUT THE AUTHOR

Michael Paul is the Chief Technology Officer at Innovative Computing Systems, Inc. and has over 20 years of experience in legal technology. He continually evaluates new technologies and designs systems to deliver new technology solutions to the legal community.

 mpaul@innovativecomp.com

 innovativecomp.com

 twitter.com/ICSGetsIT

 linkedin.com/company/innovative-computing-systems-inc