the EdgeRoom®

September 17, 2019

Data Privacy Déjà Vu? CCPA on the Heels of GDPR

By Megan Miller

The European Union General Data Protection Regulation, better known as GDPR, came into effect in May 2018. Just a month later, the state of California passed into law the California Consumer Privacy Act, nicknamed California's GDPR. The CCPA, scheduled to take effect in January 2020, creates sweeping new rights for Californians and onerous transparency and other obligations for businesses handling their information.

While it's natural to make the comparison, calling the CCPA California's GDPR may be a bit of a misnomer. The two laws share some key components, yet differ in several aspects. If your company created a compliance program for GDPR, you may be a step ahead, but you'll still want to take a thorough look at the new CCPA, adapt internal processes where needed and train employees to understand and appropriately handle information requests from California contacts.

CCPA in Short

The CCPA was created in response to high-profile data breaches, as well as the increasing trend of mishandling personal data by brokers and marketers. Designed to protect consumers from the mishandling of their private data by giving the consumer control over what data is shared or sold, the law will take effect January 1, 2020. By that date, qualifying businesses need to make their data protection and user privacy policies compliant with the new regulations or risk stiff penalties.

Under the CCPA, consumers have the right to:

1. Know what personal information is being collected on them.
2. Know if their information is being sold and to whom.
3. Opt out of that information being sold.
4. Obtain a copy of their personal information.
5. Receive equal service and price regardless of whether they exert the above rights. A common example of this would be loyalty programs, which often require customer registration to earn benefits.

Will CCPA Impact Your Business?

The CCPA applies to any business operated for the profit or financial benefit of its owners, which:

- Has annual gross revenues in excess of $25 million.
- Derives 50% or more of its annual revenues from selling consumers' personal information.
- Buys, receives, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households or devices.

If one of the above is true, and the organization collects the personal information of anyone in California and controls the purposes and means of processing that information, then that business is subject to the CCPA.

The owners of a small or regional business outside the state of California might initially conclude that they are likely not subject to these rules. However, the definition of "personal information" under this law is fairly broad. Any business with a website will likely have information on visitors' IP addresses, browsing information and/or geolocation data. These data elements are considered personal information under the CCPA, so having an active website accessible to Californians can make your company subject to the law.

Comparison to GDPR – A Few Key Differences

If your organization is already compliant with GDPR, it may be easiest to think of the CCPA in terms of the elements that are different from that regulation. An important caveat here is that the CCPA is still evolving, and amendments currently under consideration may change the ultimate form of the regulation.

- **CCPA is not in its final form.** GDPR is fairly well-established, detailed and in active use. The CCPA is not complete, and some legal experts say it's overly complex. Debates on several amendments are ongoing. On September 6, the California legislature passed amendments to the state's data breach notification statutes and information security statute. Amendments in process will require an up or down vote of both the Senate and Assembly before they can move to the governor for signing. So it's important to keep an eye on the evolution of the law and pending amendments, some of which may impact decisions on data governance that companies need to make soon.
- **Processing vs. Sale of Data:** For data collection and processing to be compliant under GDPR, one of six legal bases for processing data must apply: consent, contract, legal obligation, vital interests, public task or legitimate interest. Consent and contract are "opt-in" bases. The CCPA does not have a concept equivalent to "basis for processing." It provides consumers with the right to opt out to prevent businesses from selling their personal information. "Sale" is defined as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information to another business or a third party for monetary or other valuable consideration."

- **Nonprofit Organizations:** GDPR applies to any organization that collects the data of EU residents, irrespective of whether payment is required. The CCPA is different in that it applies specifically to businesses. The CCPA defines a business as any legal entity (e.g., corporations, associations, partnerships, etc.) that is "organized or operated for the profit or financial benefit of its shareholders or other owners." U.S. nonprofits are exempt from many data privacy and security regulations, including the CCPA, experts advise.
- **Consumers and Households:** While GDPR is specifically focused on all data related to the individual EU consumer or citizen, the CCPA considers both the consumer and household entities. The CCPA doesn't clearly define the word "household." Until that term is clarified, providers should consider it broadly in compliance efforts. For example, a business may assume that two unrelated individuals sharing an apartment are considered to be in the same household for the purposes of the law (though in many cases that information won't be known to the business). The challenges of compliance are evident here, and amendments to it – or removal of the term – have been suggested.
- **Fines:** Under GDPR, an offending business may be fined up to 20 million euros, or up to 4% of its total global revenue of the preceding fiscal year, whichever is higher. Depending on the offense, civil penalties under the CCPA may be up to $2,500 per violation or $7,500 per violation for intentional violations. The law states that damages will be calculated on a per-capita basis. Each user whose profile is illegally processed, sold, etc., will represent an independent violation. So, for example, the sale or disclosure of a database with information on 10,000 California residents could incur a fine of up to $75 million. However, enterprises have 30 days after receiving notice of noncompliance from the California attorney general's office to cure it, and only thereafter are they subject to an enforcement action for violating the law.

Actions to Take Now

The CCPA may change shape a bit before January 1, but it's a good idea to get on top of it now and identify any data management processes, or even application changes, that may need attention to be compliant by January 1. First steps include:

- Determine whether your business is subject to the CCPA.
- If the CCPA applies to your company, get executive-level support and begin an internal education program to help employees understand the new laws.
- Consult with in-house legal, compliance or outside counsel for advice on meeting requirements.
- Take an inventory of existing data: know what personal data your company is collecting and why, where it is stored and which people (partners, third parties, vendors etc.) it is shared with.
- Identify existing methods for customers to make data requests. The CCPA requires two means of access for consumers: a toll-free number and a web form request. Create or update these to be compliant.

Keep up to date on amendments and changes to the CCPA. Some good resources include the following:

- The International Association of Privacy Professionals (IAPP) offers many resources, including an Amendment Tracker on CCPA amendments.
- The state of California attorney general's office website offers background on the law, timelines and public information on data privacy.
- Am Law 100 law firm Norton Rose Fulbright offers Data Protection Report – a series of posts on evolving law and compliance topics in data privacy.

At Edge we help technology and service providers build brands and grow client relationships. While we are not legal consultants on GDPR or the CCPA, we help clients meet their own compliance efforts by supporting marketing communications, public relations, marketing automation and website design.

About the Author

Megan Miller, a senior consultant with Edge, assists clients in development and execution of strategic marketing plans in the legal and accounting tech industries. A certified eDiscovery expert, Miller has written on trends and topics in electronic discovery, cybersecurity, blockchain, consumer electronics and the Internet of Things. Her work has appeared in Attorney at Law, Legaltech News, US Tech, TechnoLawyer, ACEDS and other industry publications.

Originally published September 17, 2019 by www.theedgeroom.com