Steptoe

California's New Privacy Law: Compliance Guidelines, Comparing the GDPR

Overview

The California Consumer Privacy Act (CCPA) was enacted on June 29, 2018 and is scheduled to go into effect on January 1, 2020. The attorney general has until July 1, 2020 to promulgate the implementing regulations, and enforcement of the statute is delayed until that date.

The law was passed to head off a ballot initiative proposed by privacy rights advocates that would have imposed even more stringent requirements on businesses. Because the law is not yet in effect, several companies have announced plans to lobby for further changes, and others have noted inconsistencies in the law likely resulting from the speed with which it was drafted (for instance, the law variously requires companies to respond to consumer requests for information within 45, 90, and 135 days). Accordingly, we suspect the law will be revised between now and 2020. However, we believe the core set of privacy rights and protections will remain intact.

In particular, complying with the CCPA will likely require companies to do the following:

- Track all information retained regarding California consumers if the transactions have any connection to California
- Keep records regarding how consumer information is used, and in particular with whom it is shared
- Create a system for responding to consumer requests that is capable of (a) identifying a requesting consumer's information and how it is used or shared; (b) stopping the sharing of that information upon the consumer's request; and (c) deleting that consumer's information upon request
- Create a system for responding to claims of data breaches that is capable of curing the breaches within 30 days

The CCPA authorizes suits by private individuals, provided they give 30 days' notice of the claimed breach and also inform the Attorney General. The Attorney General is also authorized to bring suit on the public's behalf. Private suits may have damages ranging from $100 to $750 per violation per consumer, while Attorney General suits may have damages ranging up to $7,500 per violation per consumer. Given that there are nearly 40 million potential California consumers, liability under the CCPA could easily be substantial.

CCPA (as written) Compliance Steps

1. Identify all California Consumer information maintained by the company

This includes all personal information such as names, addresses, SSNs, and driver's license numbers. But beyond the usual identifiers, the CCPA also specifically calls out demographic information, biometric information, Internet

history, geolocation data, audiovisual information, educational information, or any inferences drawn from such information that is used to create a consumer profile.

Private information under the CCPA does not include anything that is publicly available, information relating to people who are not California residents, or information collected from transactions that occur entirely outside the state of California.

If California Consumer information is maintained in any form, it must be preserved for at least 12 months.

2. Create and post notices at the sites where information is collected

The CCPA requires companies to affirmatively disclose, at the point of information collection, what information is collected and generally how that information will be used (including if that information will be shared with third parties and the general types of third parties it will be shared with and how they will use it).

3. Create a system for responding to consumer requests regarding their information

The CCPA has detailed requirements regarding how consumers should be permitted to submit requests regarding their information. Companies must offer both a phone line and a website. The website must be linked to in a conspicuous manner on the company's homepage, and the link must be titled "Do Not Sell My Personal Information."

The CCPA further requires companies to disclose on their websites what their privacy policy is and to identify Californians' privacy rights. Companies can create a California-specific website if this is easier, although that site must be capable of capturing all transactions with Californians.

Types of requests – Consumers can make three types of requests: what information is maintained about them, stop sharing their information, or delete their information. When asked what information is maintained about a consumer, the company must provide the categories of information collected, the categories of sources from which that information comes, the purposes for which that information is collected, and the categories of third parties with whom that information is shared. The company must also specifically identify the information collected on the requesting consumer.

A request for information, to stop sharing information, or to delete information must be responded to in 45 days. The statute allows, in different provisions, for companies to extend this period by an additional 45 or 90 days; both provisions require notice to the consumer within the original 45-day period.

Answers to requests need only provide information dating back 12 months. And requests to stop sharing information need only be honored for a period of 12 months.

4. Create a system for identifying information collected regarding minors

Information about consumers under 16 years old can only be collected with affirmative consent or "opting in." Consumers aged 13 to 16 may opt in themselves, but information cannot otherwise be collected about them. Consumers under age 13 may not opt in themselves, and companies can only collect information about them if their parents consent.

5. Create a system for identifying and remediating any breach

Once a company has notice of a breach, it has 30 days to cure the problem. If it does not cure the problem, a lawsuit can be brought.

Accordingly, the company should have in place an investigation policy that includes at least the following features:

- Identify what information was accessed
- Determine whether the accessed information contains personal information, and if so, what kind (*e.g.*, names, DNA, customer profiles, *etc.*)
- Evaluate whether the information was accessed because of a failure to comply with the CCPA
- Determine, to the extent possible, how the information was used or disclosed
- Identify and begin implementing remedial measures
- Create a record of the results of the investigation and the remedial measures taken

6. Appoint a privacy officer

The CCPA authorizes the California Attorney General to promulgate additional privacy regulations. And, in light of the GDPR and CCPA, we expect many other jurisdictions will soon be enacting similar privacy laws. Companies should accordingly begin developing privacy compliance departments to ensure all of these laws and regulations are complied with.

GDPR v. CCPA

California's enactment of CCPA is not entirely surprising given the introduction of its European counterpart, the General Data Protection Regulation, which came into effect in May 2018.

While there are a number of differences, both statutes create broadly similar rights in consumers to control how their private data is used, who it is shared with, and whether it can be kept at all or must be deleted. The statutes also authorize suits by private individuals against companies that violate their provisions. The following chart generally summarizes and compares the two laws:

	GDPR	CCPA
What is personal data?	Broadly defined as "any information relating to an identified or identifiable natural person."	Includes standard identifiers, but also less conventional categories such as biometric data, Internet activity, geolocation data, and individual consumer profiles built with other data.

	GDPR	CCPA
What is data processing	Any operations performed on personal data, automated or otherwise.	Same
Whose information is protected?	Natural persons or "data subjects" who can be identified, directly or indirectly, by reference to an identifier.	Consumers who are natural persons residing in California.
Who must comply?	"Controllers" (who determine the "purposes and means of processing the data") and "processors" (who process personal data for the controller) that process personal data of data subjects in the European Union (regardless of where the processing occurs).	Businesses that collect consumers' personal information or authorize another to collect it on their behalf, and have either (1) annual gross revenues of $25 million or more; (2) annually buy, receive, sell, or share, for commercial purposes, information from at least 50,000 consumer, households, or devices; or (3) derive at least 50% of their annual revenues from selling consumers' personal information.
When can data be processed?	When there is a specific lawful basis, including: consent, performance of a contract, to protect a person's vital interests, for the public interest, or legitimate interest of the controller or a third party.	The law does not enumerate specific bases for processing, although sale of consumer information is prohibited if the consumer has opted out.
What rights do consumers have?	(1) Right to be informed of data processing practices (2) Right to access personal data and other information about processing (3) Right to rectification (4) Right to be forgotten (5) Right to restrict processing (6) Right to data portability (7) Right to object to processing (8) Right not to be subject to a decision based solely on automatic processing	(1) Right to know what personal information is being collected (2) Right to know whether personal information is being sold or disclosed and to whom (3) Right to say no to the sale of personal information (4) Right to access personal information (5) Right to equal service in price, even if other privacy rights are exercised

	GDPR	CCPA
How do the laws apply to children's data?	Processing children's data is lawful if the child is at least 16, otherwise parental consent is required. However, EU member states may lower the age to require parental consent to 13.	Businesses cannot knowingly sell data of consumers younger than 16 unless the consumer has opted in to the sale if the consumer is between 13 and 16, or if the parent has consented, if the consumer is under 13.
What are the exemptions?	Processing by legal authorities in relation to investigating, detecting, or prosecuting criminal offenses or penalties; processing for journalistic, academic, or literary expression purposes; limited exemptions for processing for scientific, historical research, or archiving purposes in the public interest; processing for purely personal or household activities.	Processing for compliance with federal or state local laws, including, but not limited to, GLBA and HIPAA, or legal investigations; collection or sale of de-identified or aggregate consumer information; collection or sale of personal information that takes place wholly outside of California; sale of information to consumer reporting agencies for a consumer report; where compliance would violate evidentiary privilege.
Do consumers have a private cause of action?	Yes	Yes, but only with respect to data breaches.
What fines can be levied?	Depending on the violation, administrative fines of up to €20,000,000 or up to 4% of the total worldwide annual turnover of the previous year.	For private causes of action for data breaches, between $100 and $750 per consumer per incident, or actual damages, whichever is greater. For actions brought by the Attorney General, civil penalties of $2,500 per violation per consumer or up to $7,500 per intentional violation per consumer.