The California Consumer Privacy Act (CCPA) of 2018

What You Need to Know

The California Consumer Privacy Act of 2018 is a game-changer in a number of respects. The Act imports European GDPR-style rights around data ownership, transparency and control. It also contains features that are new to the American privacy landscape, including "pay-for-privacy" (i.e., financial incentives for the collection, sale and even deletion of personal information) and "anti-discrimination" (i.e., prohibition of different pricing or service levels to consumers who exercise privacy rights, unless such differentials are "reasonably related to the value provided to the consumer of the consumer's data"). ***Effective date:*** **January 1, 2020**

KEY DEFINITIONS

"***Business***" – for-profit legal entity

- Does business in California
- Collects CA consumers' "personal information" and, alone or jointly with others, "determines the purpose and means of the processing of the consumer's PI"
- Includes brick-and-mortar and online data collection, as well as IoT devices.

"Consumer" – natural person who is a CA resident however identified, including by any unique identifier.

"Sell" – includes selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating the consumer's personal information to another business or third party for monetary or other valuable consideration

CCPA applies to BUSINESSES that:

- ✓ have annual gross revenues of more than $25M; *or*
- ✓ buy, receive, sell or share (for commercial purposes) the personal information of 50,000+ CA consumers, households or devices; *or*
- ✓ derive more than 50% of their revenues from selling consumers' personal information

Importantly: The law also applies to any other entity that controls or is controlled by such a business, and that shares common branding – ***thus potentially impacting parents, subsidiaries and other related entities that otherwise have no connection to California***.

Broad definition of "PERSONAL INFORMATION"

The definition of personal information is broad and 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. This can include the following data elements:

Common identifiers: name, address, social security number, biometric data, geolocation, driver's license, passport.

Tracking data and unique identifiers: IP address, cookies, beacons, pixel tags, mobile ad identifiers and similar technology, customer numbers, unique pseudonyms, "probabilistic identifiers" that can be used to identify a particular consumer or device, and other persistent identifiers that can be used to recognize a consumer, family or device over time and across different services.

Behavioral and profiling data: browsing history, search history and information regarding a consumer's interactions with a website, application or advertisement, purchasing history, including products or services that were obtained, purchased or considered, or purchasing tendencies, and inferences drawn from the foregoing to create a profile reflecting the consumer's preferences, characteristics, psychological trends, predispositions and attitudes.

Professional and personal background data: professional or employment-related information, education information and characteristics of protected classifications under California or federal law.

Sensory data: audio, electronic, visual, thermal, olfactory or similar information.

> **Takeaway:** The CCPA will apply to most medium to large businesses in California, or doing business in California, including online and offline transactions, regardless of where in the world the business is located.

This handout does not constitute legal advice.
Contact us at CCPA@Orrick.com.

TRANSPARENCY AND INDIVIDUAL RIGHTS REQUIREMENTS

The CCPA gives consumers the right to demand transparency and exert control over their personal information. To address these consumer rights, a business must:

1. ***Disclose,*** in response a consumer request, the categories and specific pieces of personal information collected; the source of the personal information; and the categories of third parties with whom the business discloses the personal information (for business purposes and for non-business purposes) in the preceding 12 months. In other words, companies should consider how to document their data handling practices as early as January 1, 2019.
2. ***Provide access*** to personal information in a form that is portable and could be transmitted to another business.
3. ***Delete*** personal information upon request (and instruct service providers to delete such information), subject to a number of exceptions including for a business necessity, data security or to comply with a legal obligation.
4. ***Honor opt-out requests*** to prevent future data sales to third parties. The business homepage must include a link "Do Not Sell My Personal Information" to facilitate such opt-out requests.
5. ***Implement opt-in consent*** from a child younger than 16 before selling the child's personal information to a third party. The business must obtain verifiable consent from the parent if the child is younger than 13, as required by COPPA.
6. ***Revise privacy policy*** to explain the categories and pieces of personal information collected, the sources of personal information, the categories of third parties with whom the business shares the personal information and for what business or commercial purpose. The privacy policy should also explain the consumer's rights to request transparency, data access, opt-outs and deletion.

ENFORCEMENT

Implementing Regulations. The Attorney General (AG) shall promulgate regulations to address key questions of implementation, applicability and compliance by July 1, 2020 (six months after the statute effective date).

Attorney General Enforcement. The AG may bring enforcement actions for violations and is empowered to seek injunctions and assess civil penalties of $2,500 for each violation or up to $7,500 for each intentional violation. AG enforcement is delayed until six months after publication of the regulations or July 1, 2020, whichever comes first.

Consumer Private Right of Action. The CCPA includes a private right of action for consumers but only for a business's alleged failure to "implement and maintain reasonable security procedures and practices" that results in a data breach of the type that triggers California's breach notification law, Cal. Civ. Code § 1798.81.5. Consumers can recover $100-$750 per incident or actual damages, whichever is greater.

How does the CCPA differ from the GDPR?

The GDPR takes a holistic approach to data privacy and covers all aspects of data processing activities. The CCPA is more narrowly focused on transparency and choice principles. Key differences between the two may require companies to adjust GDPR activities to meet CCPA obligations. For example:

- Definitions and exceptions are not wholly aligned
- Data inventories may need to be modified
- Responses and exceptions to consumer rights requests are not consistent
- Different consent obligations for children younger than 16
- Different opt-out requirements and processes

This handout does not constitute legal advice.
Contact us at CCPA@Orrick.com.