

## California Consumer Privacy Act of 2018

**California Consumer Privacy Act of 2018 (CCPA) (Cal. Civ. Code §§ 1798.100-1798.199)** becomes operative on January 1, 2020 with enforcement to begin no later than July 1, 2020 (Cal. Civ. Code § 1798.185(c)). The CCPA is considered the strictest privacy law in the United States, requiring companies to develop and maintain data management practices. The Act expands the rights of consumers and requires companies to be more transparent about how they collect, use and disclose personal information. Under the CCPA, service providers will be held liable for civil penalties.

Currently, there are no changes by the CCPA to existing breach notification obligations under the California Civil Code and the California Health and Safety Code.

### SCOPE

The CCPA will apply to for-profit businesses, including any entities that control or are controlled by the business and shares common branding with the business, if it collects or receives personal information from California residents, either directly or indirectly, and meets one or more of the following:

1. Has annual gross revenues in excess of U.S. \$25 Million.
2. It annually receives, buys, shares or sells, directly or indirectly, the personal information of 50,000 or more California residents, households, or devices.
3. Derives 50% or more of its annual revenue from the sale of personal information about California consumers.

Under the Act, “Personal Information” means information that identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household, including, but is not limited to:

- (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.
- (B) Any categories of personal information described in subdivision (e) of Section 1798.80.
- (C) Characteristics of protected classifications under California or federal law.
- (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- (E) Biometric information.
- (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement.
- (G) Geolocation data.
- (H) Audio, electronic, visual, thermal, olfactory, or similar information.
- (I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

## PROTECTIONS

The Act offers comparable protections to the EU's GDPR, such as:

### TRANSPARENCY

The business is under an obligation to provide consumer information such as:

- (1) The categories of personal information to be collected.
- (2) The purposes for which the personal information will be used.
- (3) The categories of third parties with whom the business shares personal information.

This information must be included in the business' privacy policy and the privacy policy must be updated at least once every twelve (12) months. As a best practice, the business should document the privacy policy update processes.

### REQUIREMENTS FOR CONSUMER PROTECTION

The consumers' rights afforded under the CCPA (right to disclosure, right to deletion, right to opt-out) may not be waived or limited by contract pursuant to Cal. Civ. Code § 1798.192.

Data Access Right - Consumers have the right to obtain, within 45 days, from a business their personal information, including:

- (1) The categories of personal information it has collected about that consumer.
- (2) The specific pieces of personal information it has collected about that consumer.
- (3) The categories of third parties with whom the business shares personal information.
- (4) The categories of sources from which the personal information was obtained.
- (5) The business or commercial purpose for collecting or selling personal information.

Data Portability Right – Consumers have the right to obtain their personal information in a format that allows the consumer to transmit it to another organization.

Data Deletion Right – Consumers may request that businesses delete their personal information. The business is required to direct any service providers to delete the consumers' personal information.

Opt-out – Consumers have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell their personal information. Businesses must notify the consumer of this use and advise they have the right to opt-out.

Businesses may not discriminate against any consumer who elects to exercise any of these rights.

## CCPA ENFORCEMENT AND PENALTIES

Enforcement actions may not be brought until 6 months after the publication of the final regulations or July 1, 2020, whichever is sooner.

The Attorney General may bring a civil action against businesses, services providers or other persons, which may result in an injunction and/or civil penalties of up to \$2,500 for each violation (and up to \$7,500 for each intentional violation). Civil penalties assessed or proceeds of any settlement is to be deposited into the Consumer Privacy Fund.

Consumer's private right of action under Cal. Civ. Code § 1798.150 has legal basis for instituting a civil action by violating Cal. Civ. Code § 1798.81.5 which requires businesses to implement and maintain reasonable security procedures and practices to protect their personal information from unauthorized access, destruction, use, modification or disclosure. Where violations result in unauthorized access to a consumer's unencrypted/unredacted personal information, consumers may receive:

- (A) damages in an amount not less than \$100 and not greater than \$750 per consumer per incident or actual damages, whichever is greater;
- (B) an injunction or declaratory relief; and
- (C) any other relief as determined by a court.

It is important to note that the definition of "personal information" that applies to the private right of action is the one found in Cal. Civ. Code § 1798.81.5, which lists more traditional elements such as a consumer's name coupled with a social security number or credit card number.

Consumers must provide the business with a 30-day written notice containing any alleged violation(s), giving the business 30 days to cure the violation(s). The business must submit a written statement that the violation(s) have been cured and no further violations will occur. Consumer action may only be brought if the business does not satisfy the 30-day cure obligation, for each breach of the written statement, or for additional violations that postdate the written statement.

## CCPA Regulations and Proposed Amendments

The Attorney General's office held forums for public comment and accepted written comments. The time for the public and written comment has ended and the Attorney General's office announced that it plans to issue its Notice of Proposed Regulatory Action in the Fall of 2019.

In addition, businesses should pay close attention to several proposed amendments introduced in California relating to the CCPA, to track their progress and any impacts to the CCPA should they get passed and signed into law in 2019.