

BURR ALERT

Summary of California Data Breach Notification Law ("CCPA")

By Elizabeth B. Shirley

October 2019

I. Summary of effective dates

- Effective January 1, 2020
- Enforcement starting July 1, 2020
- Employees not covered for first 12 months*

* Except for general notice to job applicants, employees, owners, directors, officers, medical staff members, or contractors about types of PII collected and purposes for which PII is used.

II. Who Must Comply?

A business must comply with CCPA if:

- 1) it is a for-profit legal entity;
- 2) that collects consumers' personal information on its own or by others on its behalf;
- 3) that alone or jointly with others determines the purposes and means of processing;
- 4) that "does business" in California; AND
- 5) satisfies at least ONE of the following:
 - a) has annual gross revenues in excess of \$25 M;
 - b) annually buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or devices; OR
 - c) derives 50% or more of its annual revenues from selling consumers' personal information.

III. Who is a "Consumer"?

"Consumer" is defined as natural persons who are California residents, which means:

- a) In California for other than a temporary or transitory purpose, OR
- b) Domiciled in California, but are currently outside the state for a temporary or transitory purpose.

IV. What is Personal Information?

Personal information is defined broadly. It includes any information that directly or indirectly identifies, describes, or can reasonably link to a particular consumer or household.

CCPA protects data even if it does not relate to a single individual, as it covers households and data, even if the data does not contain a name.

For example:

- a real name;
- an alias;
- a postal address;
- an email address;
- a unique personal or online identifier;
- an internet protocol (IP) address;
- an account name;
- a Social Security number (SSN);
- a driver's license or passport number;
- Records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- Biometric information;
- Browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement;
- Geolocation data;
- Audio, electronic, visual, thermal, or other similar information;
- Professional or employment-related information;
- Educational information;
- Inferences drawn from any of the above to create a profile about a consumer.

V. What is NOT Personal Information?

CCPA's definition of personal information EXCLUDES:

- › "Publicly available information" – information that is lawfully made available from federal, state, or local government records;
- › "De-identified" or "aggregate" consumer information;
- › Information collected, used, sold, or disclosed pursuant to the Gramm-Leach Bliley Act, or the Driver's Privacy Protection Act of 1995, but only if CCPA is in conflict with those laws;
- › Information sold to or from a consumer reporting agency (as defined in the Fair Credit Reporting Act), when the personal information is "reported in, or used to generate" a consumer credit report.

VI. What are the CCPA's Main Requirements?

Disclosure and Transparency --

- Provide notice about collection practices.
- Disclose and keep up-to-date at least once every 12 months a description of consumers' rights, e.g., privacy policy.
- List separately the categories of PII collected, sold, and disclosed for a business purpose in the preceding 12 months.
- Provide notice about onward transfers of PII.
- Make available 2 or more designated methods for requesting PII held by business.

If selling PII:

- Provide right to opt-out via a clear and conspicuous link entitled: "Do Not Sell My Personal Information."
- Seek opt-in consent from consumers between the ages of 13-16.
- Seek opt-in consent from parents if consumer is under 13 years of age.
- Establish procedures for receiving and processing verifiable consumer requests.
- Amend contracts with third-parties to clarify that PII is not shared for value (if applicable).

Security: Implement and maintain reasonable security measures and practices.

VII. What Rights Do Consumers Have?

- Right to request disclosure of categories of PII and specific pieces of PII that the business collected on consumer in last 12 months.
- Right of access to purposes for which PII was used and with whom it is shared.
- Right of deletion.
- Right to opt-out of sale of PII.
- Right to data portability "without hindrance."
- Right to sue for data security breaches.
- Anti-discrimination for exercising rights provided by CCPA.

VIII. Enforcement

- Civil Penalties: In actions by CA Attorney General, penalties of up to \$7,500 per intentional violation. Up to \$2,500 for unintentional violation, with opportunity to cure within 30 days' notice of alleged violation.
 - › CA Attorney General may seek injunction.
- Damages: In actions by consumers for security breach violations, statutory damages between \$100-\$750 per consumer, per incident; OR actual damages, whichever is greater.
 - › May also seek injunctive or declaratory relief.

To discuss further, please contact:

Elizabeth B. Shirley in Birmingham at bshirley@burr.com or (205) 458-5186