LONG LAW

CCPA Cheat Sheet

Table of contents:

Applicability

Effective Date: January 1, 2020

Applies to:

Any for-profit organization doing business in California, that collects consumers' personal information or determines the purposes and means of processing consumers' personal information and meets any one of the following criteria:

- Has annual gross revenue in excess of $25 million;
- In possession of personal information of 50,000 or more consumers, households, or devices; or
- Earns 50% or more of its annual revenue from selling consumers' personal information.

Exceptions:

Does not apply to:

- Covered entities subject to HIPAA;
- Medical information from a HIPAA-covered entity;
- Data collected as part of a clinical trial;
- Personal information collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act;
- Personal information provided to law enforcement agencies or disclosed in the course of exercising/defending legal claims; and
- Several other exceptions.

Definitions

"Personal Information":

Information that "identifies, relates to, describes, or is associated with a particular consumer or household," within 11 enumerated categories:

1. Name, address, personal identifier, IP address, email address, account name, social security number, driver's license number, and passport number.

2. Personal information under California's records destruction law (Cal. Civ. Code § 1798.80(e)):

- E.g., signature, physical characteristics or description, telephone number, insurance policy number, education, employment, employment history, or financial account information.

3. Characteristics of protected classifications:

- Federal: Race, Color, Sex. Age, Religion, National origin, Disability, Citizenship status, Genetic information
- California: Marital status, sexual orientation and identity, medical condition, AIDS/HIV, military or veteran status, political affiliations or activities, and status as a victim of domestic violence, assault, or stalking.

4. Commercial information: records of personal property, products, or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

5. Biometricinformation.

6. Internet or other electronic network activity, such as browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement.

7. Geolocation data.

8. Audio, electronic, visual, thermal, olfactory, or similar information.

9. Professional or employment-related information.

10. Educational information.

11. Inferences drawn from any of the information listed above to create a profile reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

"Business Purpose":

Entails "the use of personal information for the business's or service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which it was collected."

Includes:

- auditing;
- detecting security incidents;
- performing services (as defined); and
- undertaking internal research for technological development and demonstration.

"Breach": Defined in California Civ. Code s. 1798.82(a) as an incident where either (1) unencrypted personal information is reasonably believed to have been acquired by an unauthorized person, or, (2) encrypted personal information is reasonably believed to have been acquired by an unauthorized person and the encryption key or security credential is reasonably believed to have been acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable.

CCPA Rights

Right to Opt-Out: Consumers must be notified if their personal information may be sold, and informed they have the right to opt out of such sale. A CCPA covered business must post a "clear and conspicuous link" on its website titled "Do Not Sell My Personal Information," and must include a link to the "Do Not Sell My Personal Information" page in its privacy policy.

Right to Opt-In: The CCPA prohibits businesses from selling the personal information of consumers between the ages of 13 and 16 without first obtaining affirmative opt-in consent (1) from the consumer or (2) from a parent or guardian where the consumer is under the age of 13.

Right to Be Forgotten: Subject to several exceptions, businesses must inform consumers of their right to be forgotten. The CCPA does not state how consumers should be informed of this right. Adding this disclosure to the privacy policy or having a link on the home page may be sufficient.

Right to Know Businesses must disclose, at or before the time of collection:

- The categories of personal information to be collected about the consumer and the purposes for which the information will be used, and
- The categories of consumers' personal information that were actually collected in the preceding 12 months and sold or disclosed for business purposes in the preceding 12 months.

Right to Receive Personal Disclosures:

With some exceptions, the CCPA requires two or more designated methods for the consumer to request information pertaining to the collection, sale, or disclosure of the customer's personal information, including, at a minimum, a tollfree telephone number and website address.

In response to such requests, the business must disclose:

- The categories of personal information collected about the consumer;
- The categories of sources from which personal information is collected;
- The business or commercial purpose for collecting or selling personal information;
- The categories of third parties with whom the personal information was shared;
- The specific pieces of personal information collected about the consumer;
- The categories of the consumer's personal information that were sold or disclosed for business purposes in the preceding 12 months.

Right To Equal Service:

Prohibits businesses from discriminating against consumers who exercise their rights under the CCPA. Specifically, the business may not, based on the exercise of the consumer's CCPA rights:

- Deny goods or services;
- Charge a different price or rate for goods or services including by discounts or other benefits;
- Impose penalties;
- Provide a different level of quality or service; or
- Suggest that a consumer will receive a different price or rate or different level of quality of goods or services.

Cybersecurity Compliance

Vendor Management:

Businesses may share personal information with third parties or service providers for business purposes if there is a written contract prohibiting the third party or service provider from selling the personal information or "retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract."

Without a CCPA-compliant service provider agreement, disclosure of personal information to a vendor may constitute a "sale of personal information" that triggers the consumer's right to opt-out.

Reasonable Security Measures:

A business's "duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information" is guided by the California Attorney General's recommendations.

In its most recent California Data Breach Report, the Attorney General offered this guidance:

"The 20 controls in the Center for Internet Security's Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."

In addition to the CIS Top 20 framework, CCPA-compliant businesses should also look into:

- Established, comprehensive data security frameworks like the NIST Cybersecurity Framework or ISO 27001.
- FTC guidance in "Start with Security," "Stick with Security" and recent FTC enforcement actions.
- Look to industry standards but note the California Attorney General's guidance that industry standards may not be adequate or fully updated.

Breach Response

Breach Notification Law:

Separate from the CCPA, and thus applicable to any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information," California Civ. Code s. 1798.82(a) requires such persons or businesses to "disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California."

The disclosure shall be made in the most expedient time possible and without unreasonable delay.

The form of notice is provided for by statute.

Attorney General Notification:

A person or business that is required to issue a security breach notification to more than 500 California residents because of a single breach of the security system shall electronically submit a single sample copy of that security breach

notification, excluding any personally identifiable information, to the California Attorney General.

Private Right of Action:

In addition to state enforcement actions, the CCPA provides consumers with a limited private right of action when "nonencrypted and nonredacted personal information…is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information."

Violations are subject to penalties of $100 to $750 per incident, actual damages, and injunctive relief. Typically, each record that is breached is considered a separate incident. Thus, violations can be quite costly.

Before bringing an action for a security breach, the CCPA requires consumers to provide covered businesses with 30 days written notice, identifying the specific provisions the business allegedly violated. The business then has 30 days to address and resolve the violations without penalty.

Additional Resources

1. CCPA Full Text
2. California Civ. Code s. 1798.80
3. California Civ. Code s. 1798.82
4. California Data Breach Report
5. CDC HIPAA Guidance
6. CIS Top 20 Cybersecurity Framework
7. FTC Guidance "Start with Security"
8. FTC Guidance "Stick with Security"
9. FTC Guidance on Gramm-Leach-Bliley Act
10. HHS HIPAA Guidance
11. ISO 27001 Information Security Framework
12. NIST Cybersecurity Framework