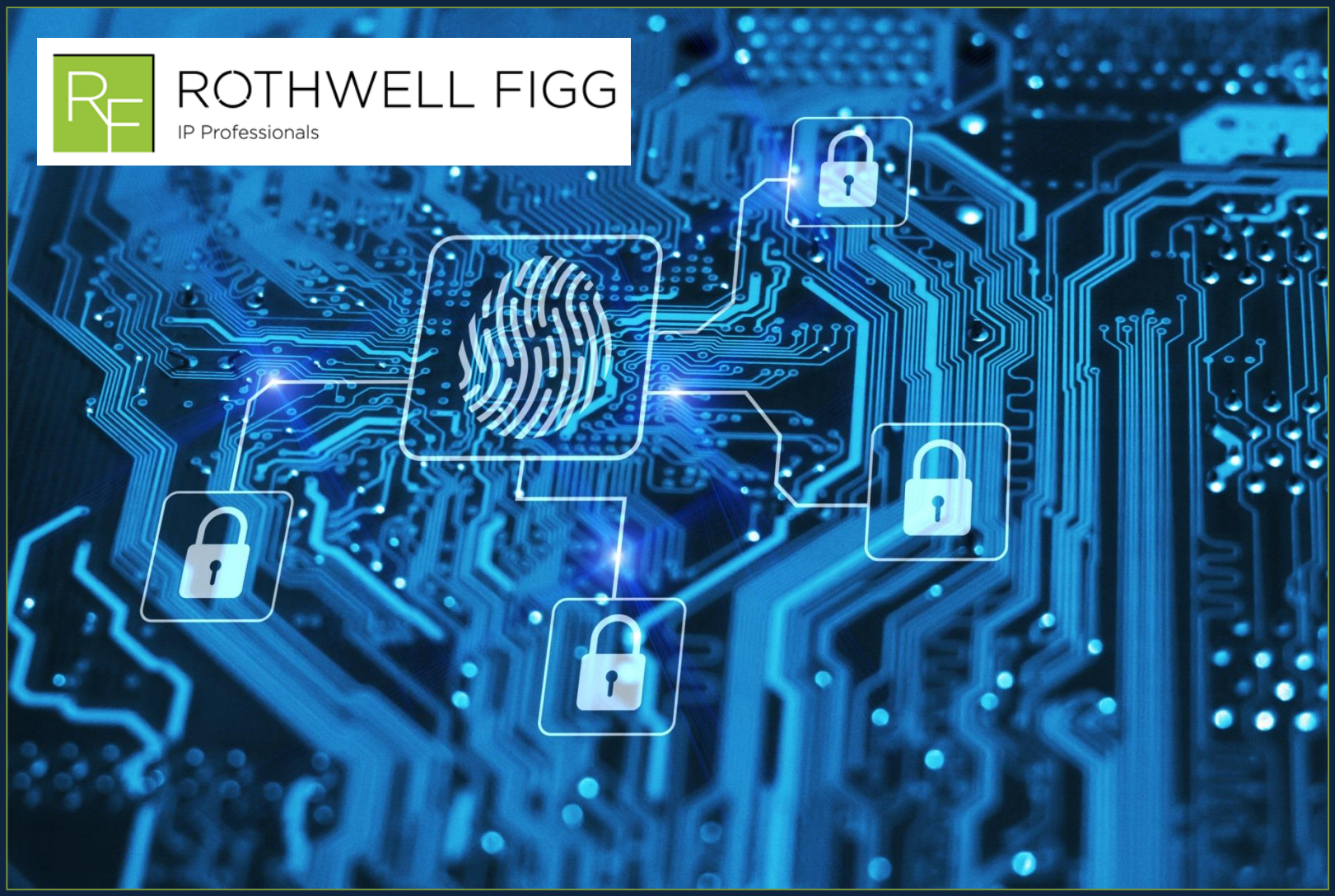
ROTHWELL FIGG
IP Professionals



California Consumer Privacy Act (CCPA) Compliance Guide

Last Revised December 2019

Privacy
Data Protection
Cybersecurity

www.rfem.com

Contents

Scope of CCPA

The California Consumer Privacy Act (CCPA) was enacted in June 2018 and goes into effect January 1, 2020. The CCPA is one of the most comprehensive privacy laws in the United States and aims to give California residents more control over how their personal information is collected, used, and sold. The California Governor signed five amendments to the CCPA on October 11, 2019, and the California Attorney General has issued proposed regulations providing guidance to businesses on how to comply.

	CCPA Provision
Who is regulated?	**Any for-profit entity that:** **(i) Does business in California,** **(ii) Collects "Personal Information" of California residents (or has such information collected on its behalf),** **(iii) Determines on its own or jointly with others the purpose and means of processing that information, and** **(iv) Meets one or more of the following criteria:** • **Has a gross revenue greater than $25 million;** • **Annually buys, receives, sells, or shares the personal information of more than 50,000 consumers, households, or devices for commercial purposes; or** • **Derives 50% or more of its annual revenues from selling consumers' personal information.** **[Hereafter a "Business"]**
Who is protected?	**"Consumers," defined as California residents, including every individual who is:** • **In California for other than a temporary or transitory purpose; or** • **Domiciled in California but is currently outside the state for a temporary or transitory purpose.**
What is protected?	**"Personal Information," which means information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with a particular Consumer or household, including (but not limited to):** • **Personal Identifiers (e.g., name, postal address, email address, online IP address, social security number);** • **Internet or other electronic network activity information; and** • **Employment, educational, and commercial information.** **Note: There is a one-year sunset clause exempting from many of the CCPA's requirements personal information obtained through business-to-business (B2B) communications and transactions. Deidentified or aggregate consumer information is also exempted.**

General Compliance Guidelines

To comply with many of the CCPA's requirements, a Business must first have ready access to certain facts about the Personal Information it collects. A best practice for gathering and sorting this data is to create a "data map" that tracks the flow of the Personal Information from the time it is collected through each point of use by the Business (collection→ use→ processing→ storage→ sale → deletion).

"[D]uty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information"
–Cal. Civ. Code § 150(a)(1)

A data map should preferably identify and trace:

- **What Personal Information it has collected about a Consumer ("category" & specific data);**
- **The sources of that Personal Information (e.g., direct collection or from a third party);**
- **How that Personal Information is collected (e.g., user input, sales transaction, cookies tracking);**
- **Where that Personal Information is stored and when it is deleted;**
- **How that Personal Information is used by the Business; and**
- **What Personal Information, if any, is "sold" to a third party and the method of sale.**

To help minimize the risk of a Consumer action, a Business should implement and maintain reasonable security practices for each point on the data map, taking into account potential vulnerabilities with individuals (e.g., employees), IT assets (hardware and software), policies and procedures, and facilities.

It is also critical for a Business to maintain documentation of its written policies and data security procedures, both for CCPA compliance and, if needed, to defend its compliance activities in a litigation or enforcement action.

[Compliance Checklist]

- ✓ **Create a data map**
- ✓ **Document processes and procedures**
- ✓ **Implement reasonable data security measures**

Notice to Consumers

The CCPA grants Consumers the right to know what Personal Information a Business collects, sells, or discloses about them, and requires the Business to make affirmative disclosures of this information "at or before the point of collection." This disclosure is typically referred to as a "Privacy Notice" (or "privacy policy" or "information notice").

"A Business that collects a Consumer's Personal Information shall, at or before the point of collection, inform Consumers as to the categories of Personal Information to be collected and the purposes for which the categories of Personal Information shall be used"
–Cal. Civ. Code § 100(b)

PRIVACY NOTICE

A Privacy Notice must disclose at least the following information with regard to a Consumer's privacy rights:

- **The categories of Personal Information collected, sold, and/or disclosed;**
- **If the Business sells personal information, the link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info";**
- **The categories of sources from which the Business collects Personal Information;**
- **The business or commercial purpose for collecting or selling Personal Information;**
- **The categories of third parties with whom the Business shares Personal Information;**
- **Descriptions of the Consumer's right to access information, right to deletion, right to opt-out of the sale of information, and right to nondiscrimination; and**
- **Two or more designated methods for submitting requests for information, including at minimum a toll-free number, or an email address if the Business operates exclusively online.**

A Business cannot collect additional Personal Information categories or use collected Personal Information for unrelated purposes without providing the required notice.

The Business must review and update its Privacy Notice at least every 12 months.

[Compliance Checklist]

- ✓ **Review existing privacy notices and verify that they meet each new requirement under the CCPA**
- ✓ **Update Privacy Notice every 12 months (and as necessary to conform with any changes to the CCPA and updates in business practices)**

Right to Access Data

The right to access data refers to the ability of a Consumer to request that a Business provide the type of Personal Information that the Business has collected, sold, or disclosed about the individual, as well as provide a copy of the specific Personal Information that the Business has on file. Access requests are often referred to as "Data Subject Access Requests" (or "DSARs" or "SARs").

"A Consumer shall have the right to request that a Business that collects a Consumer's Personal Information disclose to that Consumer the categories and specific pieces of Personal Information the Business has collected"
–Cal. Civ. Code § 100(a)

DATA SUBJECT ACCESS REQUEST

A Business must make available at least two submission methods by which Consumers can request access to their personal data, including: (1) a toll-free telephone number; and (2) a website address, if the Business has one.

In response to a Verifiable Consumer Request (VCR), a Business must provide (within 45 days and in a readily usable format) the Consumer with:

- **The categories of Personal Information collected about the individual Consumer by the Business;**
- **The categories of sources from which the Business collected the Personal Information;**
- **The business or commercial purpose for collecting or selling the Personal Information;**
- **The categories of third parties with whom the Business shares (or sells) Personal Information; and**
- **The specific pieces of Personal Information collected.**

LIMITATIONS

The right to access is tempered by: (1) requiring Consumer identity verification (acceptable methods TBD); (2) limiting response scope to the past 12 months; and (3) a maximum of 2 requests per year.

[Compliance Checklist]

- ✓ **Make available at least 2 VCR submission options**
- ✓ **Develop ID verification process**
- ✓ **Develop standard data retrieval procedures, reporting formats, and tracking systems**

Right to Request Disclosure

In the same vein as a Consumer's right to access the Personal Information that a Business has collected about the individual, the CCPA also grants Consumers the right to know where and to whom their Personal Information is being disclosed or sold.

"A Consumer shall have the right to request that a Business that sells the Consumer's Personal Information, or that discloses it for a business person, disclose to that Consumer…" –Cal. Civ. Code § 115(a)

A Business that sells the Consumer's Personal Information, or that discloses it for a business purpose, must provide, either in response to a proper Verifiable Consumer Request or within its Privacy Notice, an itemized list of the categories of Personal Information:

- **Collected about the Consumer by the Business;**
- **Sold about the Consumer (and the categories of third parties to whom the information was sold) during the preceding 12 months or a statement that no sale was made; and**
- **Disclosed about the Consumer for a business purpose during the preceding 12 months or a statement that no disclosure was made.**

[Compliance Checklist]

- ✓ **Make available at least 2 VCR submission options**
- ✓ **Develop ID verification process**
- ✓ **Develop standard data retrieval procedures, reporting formats, and tracking systems**

Right to Deletion

Subject to a VCR under the same procedures set forth in the previous "right to access" section, a Consumer has the right to request that a Business and its Service Providers delete the Personal Information that has been collected about that individual (also referred to as the "right to be forgotten" or the "right of erasure"). Notably, the CCPA does not currently specify what actions are sufficient to constitute "deletion."

"A Consumer shall have the right to request that a Business delete any Personal Information about the Consumer which the Business has collected from the Consumer"
–Cal. Civ. Code § 105(a)

Although the right to deletion is often misinterpreted as an absolute right, in reality, it only applies in a limited number of situations.

EXCEPTIONS TO DELETION

A Business may DENY a verified deletion request when the Personal Information is necessary to:

- **Complete the transaction for which the personal information was collected, provide a good or service requested by the Consumer, or reasonably anticipated within the context of a Business' ongoing business relationship with the Consumer, or otherwise perform a contract between the Business and the Consumer;**
- **Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity;**
- **Debug to identify and repair errors that impair intended functionality;**
- **Exercise or ensure the right of another to exercise free speech, or exercise another right provided by law;**
- **Comply with the California Electronic Communications Privacy Act;**
- **Engage in certain research in the public interest;**
- **Enable solely internal uses that are reasonably aligned with the expectations of the Consumer based on the Consumer's relationship with the Business;**
- **Comply with a legal obligation; and**
- **Otherwise use the Consumer's personal information, internally, in a lawful manner that is compatible with the context in which the Consumer provided the information.**

[Compliance Checklist]

- ✓ **Establish a process to determine if one of the exceptions to the right of deletion applies**
- ✓ **Develop a means to readily access and delete specific Personal Information**
- ✓ **Develop a process to effectuate deletion by any Service Providers**

Right to Opt-In/Opt-Out of Sale

The CCPA's right to prohibit the sale of Personal Information grants Consumers over 16 years old the right to "opt-out" and grants Consumers under 16 years old the affirmative right to "opt-in." Once a Consumer opts-out or refuses to opt-in, the Business must honor the request unless that Consumer provides express authorization to resume the sale of Personal Information. Businesses must wait at least 12 months before asking the Consumer to reauthorize future sales of Personal Information.

"A Consumer shall have the right, at any time, to direct a Business that sells Personal Information about the Consumer to third parties not to sell the Consumer's Personal Information" –Cal. Civ. Code § 120(a)

OPT-OUT: Consumers Over 16

Consumers over 16 years of age may opt-out of the sale of Personal Information at any time. To help Consumers understand and exercise this right, a Business must:

- **Provide (on its general homepage or a separate homepage), a clear and conspicuous link titled "Do Not Sell My Personal Information" which enables the Consumer to opt-out;**
- **Disclose the right to opt-out in any online Privacy Notice; and**
- **Train all employees responsible for handling Consumer inquiries about the Consumer's opt-out right and how to exercise it.**

OPT-IN: Consumers Under 16

The CCPA prohibits the sale of Personal Information collected (with actual knowledge) from a Consumer who is:

- **Between 13 and 16 years old, unless the Consumer affirmatively opts-in; and**
- **Under age 13, unless a parent or guardian has affirmatively authorized the sale.**

[Compliance Checklist]

- ✓ **Clearly display an opt-out button on the Business website and develop a means to track opt-outs**
- ✓ **Develop a means for classifying Personal Information based on Consumer age**
- ✓ **Develop sale reauthorization mechanism**

Right to Nondiscrimination

The CCPA grants a right to equal service, prohibiting discrimination against Consumers who exercise their rights under the Act.

"A Business shall not discriminate against a Consumer because the Consumer exercised any of the Consumer's rights under this title"
–Cal. Civ. Code § 125(a)(1)

NONDISCRIMINATION

A Business is generally prohibited from engaging in any of the following discriminatory actions against Consumers who exercise their CCPA rights:

- **Denying goods or services to those Consumers;**
- **Charging different prices or rates, including through the use of discounts or other benefits;**
- **Providing them with a different level of quality of service; and**
- **Suggesting that they will receive a different level or quality of service.**

EXCEPTIONS

A Business may impose some price, quality, or service differences, or make financial incentive offers IF such a difference:

- **Is directly or reasonably related to the value of the Consumer's data; and**
- **Does not result in unjust, unreasonable, coercive, or usurious financial incentive practices.**

Businesses making financial incentive offers for the collection, sale, or deletion of data must also: (1) notify the Consumer of the program's material terms; and (2) obtain prior opt-in consent. The Consumer may withdraw this consent at any time.

Example: "A music streaming business offers a free service and a premium service that costs $5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale of their personal information, then the practice is discriminatory, unless the $5 per month payment is reasonably related to the value of the consumer's data to the business."

[Compliance Checklist]

- ✓ **Review business practices and policies to ensure that any incentive programs are non-discriminatory**
- ✓ **If financial incentives are offered, notify the Consumer of the material terms and obtain prior opt-in consent**

Obligations with Service Providers

The CCPA provides Businesses with additional obligations when working with Service Providers and third parties. Qualifying as a Service Provider rather than a third party provides certain advantages.

SERVICE PROVIDER QUALIFICATIONS

A Business may only provide Personal Information to a Service Provider IF:

- **The disclosure is for a business purpose pursuant to a written contract; and**
- **The Service Provider is prohibited from retaining, using, or disclosing the Personal Information for any purpose other than for the specific purpose disclosed in the contract or otherwise permitted by the CCPA.**

The CCPA treats Service Providers and third parties differently, including:

- **Limitation on Liability. The CCPA limits a Business's liability for Service Provider misconduct if certain conditions are met (e.g., compliance with the written contract provision and no actual knowledge of intent to violate the CCPA), but does not offer the same protection when a Business sells, shares, or discloses Personal Information to third parties. Similarly, Service Providers are not liable under the CCPA for the obligations of the Business for which it provides services.**

- **Limitation on Sale/Transfer of Personal Information. The CCPA limits a Business' ability to sell, share, or disclose Personal Information to third parties without prior notice and options for opt-out, but does not place the same requirements on sharing with Service Providers.**

[Compliance Checklist]

- ✓ **Track and document any disclosure of Personal Information to a third party or Service Provider**
- ✓ **Create a written contract with any third party or Service Provider limiting the use of any Personal Information to conform with the CCPA requirements**

Privacy
Data Protection
Cybersecurity

Our team at Rothwell Figg helps clients understand and navigate the rapidly evolving area of privacy, data protection, and cybersecurity law. We work with you to prepare, integrate, and implement strategies and best practices for CCPA compliance while you focus on your business needs.

We are uniquely qualified to assist you in complying with the comprehensive and complicated privacy laws contained in the CCPA. Our team includes lawyers with technical backgrounds and industry experience, including in computer science and cybersecurity. We know how to work with your IT and technical teams to understand your potential exposure, map out a legal and technical strategy, and minimize the risks of a breach or violation. We get it, and we can help you develop a CCPA readiness roadmap that suits your specific needs. If you already have a privacy plan or data protection practices in place, we can meet you where you are through a flexible and compliant plan to address the changing legal and business landscape.

MEET THE TEAM

Steven Lieberman

Martin M. Zoltick

Jenny L. Colgate

Christopher A. Ott

Jennifer B. Maisel

Caitlin M. Wilmot

202.783.6040 privacy@rfem.com www.rfem.com

Rothwell Figg, Ernst & Manbeck, P.C., 607 14th Street, Suite 800 Washington, D.C.,

ROTHWELL FIGG
IP Professionals