ONE FIRM WORLDWIDE®

California Consumer Privacy Act Guide

July 2020

JONES DAY®

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The California Consumer Privacy Act ("CCPA"), which went into effect on January 1, 2020, constitutes a major sea change in U.S. privacy law. The CCPA broadly governs the collection, use and disclosure of personal information about California "residents"—including consumers, employees, job applicants, students and other categories of individuals—as well as information about households and devices. As a result, the CCPA will impact almost all for-profit businesses that collect information about California residents. The CCPA is enforced primarily by the California Attorney General, who may seek civil penalties up to $2,500 per violation or up to $7,500 per intentional violation. The law also provides a private right of action and statutory damages for certain data breaches arising from violations of California's data security law. Affected California residents can seek up to $750 in statutory damages per individual per incident or actual damages, whichever is greater. Given the sheer quantity of data that most businesses process on a regular basis, non-compliance with the CCPA could lead to significant legal, regulatory and reputational risk to businesses subject to the statute.

This Guide provides an overview of the statute's key provisions as well as the most important changes the law makes to the existing rights, obligations, and remedies under California data privacy law. It also highlights key requirements of the proposed final regulations that companies seeking to comply with the CCPA must keep in mind when these regulations come into effect as early as July 1, 2020. While there is no substitute to reviewing the statutory terms and seeking legal advice to develop a comprehensive CCPA compliance program, we have also provided an "action item checklist" that your legal and compliance teams can use to prepare for the CCPA.

INTRODUCTION

On June 28, 2018, California Governor Edmund G. Brown Jr. signed into law the CCPA—the result of a last-minute compromise between California lawmakers and consumer privacy activists that was intended to avoid a widely criticized data privacy ballot initiative. The law went into effect on January 1, 2020, and creates certain data privacy rights for California consumers (i.e., California residents) with respect to their personal information.

This updated guide provides an overview of the CCPA's key provisions and the important changes it will make to the existing rights, obligations, and remedies under California data privacy law. In addition, each section of this guide sets out suggested actions that companies can take to prepare for and comply with the CCPA's new requirements. Please contact any of the lawyers listed on pages 36 and 37 if you would like to receive additional information.

Specifically, the CCPA grants California consumers:

1. The right to know what personal information is collected by businesses, from where it is sourced, how it is used, and whether and to whom their personal information is being disclosed or sold;
2. The right to "opt out" of the sale of personal information to third parties or, for consumers under 16 years old, the right not to have personal information sold absent "opt-in" consent;
3. The right to access personal information;
4. The right to delete personal information; and
5. The right to equal service and price, even if a consumer exercises his or her privacy rights.

Importantly, the CCPA also provides consumers with a private right of action and statutory damages in the event that certain unencrypted or unredacted personal information is subject to unauthorized access and exfiltration, theft, or disclosure as the result of a company's failure to implement and maintain reasonable security procedures and practices.

The CCPA gives the California Attorney General the power to impose substantial penalties for violations, even if those violations do not result in a data breach. When a business does not cure a violation within 30 days of notice of noncompliance, the CCPA allows for up to $2,500 in statutory damages per violation. For intentional violations, the statutory damages are elevated to up to $7,500 per violation.

INTRODUCTION

On October 11, 2019, California Governor Gavin Newsom signed into law five bills amending the CCPA, which attempt to clarify some of the statute's ambiguities and modify the scope of data covered. And on October 10, 2019, California Attorney General Xavier Becerra released proposed regulations providing guidance on how businesses must implement the CCPA. The law mandates that on or before July 1, 2020, the Office of the Attorney General adopt implementing regulations for the CCPA. Since their introduction, the proposed regulations have gone through two rounds of modifications. The Attorney General released the first set of modifications for public comment on February 10, 2020, with a second set of modifications and written comment period following on March 11, 2020. On June 1, 2020, the Office of the Attorney General submitted the final set of the proposed regulations to the California Office of Administrative Law ("OAL").

The OAL may take up to 90 working days to determine whether the record satisfies certain procedural requirements. The Office of the Attorney General has requested that the OAL perform an expedited review (within 30 working days) and that the regulations become effective upon filing with the Secretary of State. Despite the uncertainty regarding the effective date of the final regulations, the Attorney General may bring an enforcement action under the CCPA beginning July 1, 2020 and he has reiterated that his office remains committed to enforcing the CCPA beginning on that date.

In their current form, the final proposed regulations make significant changes to the initial proposed regulations published on October 10, 2019, and outline the steps that covered businesses must take to comply with the CCPA. We have added highlights from the final proposed regulations in this updated guide.

Successful compliance starts with substantial planning, preparation, and action prior to a law's effective date and then continues afterward through periodic updates and internal evaluations.

ACTION ITEMS CHECKLIST

A. Does our company fall within the scope of the CCPA?

- ✓ Determine whether your company collects personal information from California consumers.
- ✓ Assess whether your company qualifies as a business under the CCPA.
- ✓ Determine whether your company is a service provider or third party under the CCPA.
- ✓ Assess whether any exceptions may apply.

B. How does our business use personal information?

- ✓ Determine what types of consumer personal information your business collects, shares, and/or sells.
- ✓ Determine whether your business maintains the consumer personal information it collects, shares, and/or sells.
- ✓ Determine where, and for how long, your business maintains such consumer personal information.
- ✓ Develop data mapping to identify, track, and control the collection, retention, and deletion of consumer personal information.

C. How can we prepare to comply with the CCPA's automatic disclosure requirements?

- ✓ Create a description of consumer rights set forth in the CCPA.
- ✓ Draft a description of the business or commercial purpose for sharing and selling consumer personal information.
- ✓ Update your online privacy policy and/or company website to comply with CCPA disclosure obligations.

D. How can we prepare to respond to consumer CCPA requests?

- ✓ Establish a method and process for the submission of consumer requests concerning personal information.
- ✓ Draft a written description of this consumer request submission process for publication on the company website.
- ✓ Establish internal procedures for fielding, researching, and responding to consumer requests.
- ✓ Establish an internal process for dealing with, validating, and logging consumer deletion requests.
- ✓ Identify exceptions to the deletion requirement that are relevant to your business.
- ✓ Establish a communications protocol for responding to consumer deletion requests.
- ✓ Create a "Do not sell my personal information" link/website to satisfy CCPA opt-out rules.
- ✓ Update your online privacy policy and website to satisfy opt-out requirements.
- ✓ Establish a process for tracking consumer opt-outs and segregating consumer personal information sold to third parties.
- ✓ If your business is a third-party recipient of consumer personal information, establish a process for providing notice to relevant consumers of any sale of their personal information.
- ✓ Calculate the value of consumer personal information to your business.
- ✓ Consider developing financial incentive programs that comply with the CCPA.
- ✓ Establish a toll-free telephone number and website for consumer requests.
- ✓ Create an internal process for responding to requests that includes reasonable consumer authentication requirements and complies with the CCPA's time limit and format requirements.

E. How can we protect against data security incidents and related consumer lawsuits?

- ✓ Review your network security to ensure that standards are reasonable, particularly with regard to the collection and maintenance of consumer personal information.
- ✓ Tailor mechanisms to process and fulfill verifiable consumer requests such that they comply with the California Attorney General's rules and procedures, once those rules and procedures are finalized.
- ✓ Upgrade your network security as necessary.
- ✓ Identify appropriate encryption solutions and policies.
- ✓ Identify applicable cybersecurity legal requirements (e.g., HIPAA, GLBA) and standards (e.g., NIST, CIS, ISO, COBIT, PCI DSS).
- ✓ Conduct a privileged assessment of your cybersecurity program and map to applicable legal requirements and standards.
- ✓ Review and revise your incident response plan.
- ✓ Address governance issues, including how and when executive leadership manages cybersecurity and the involvement of independent directors.
- ✓ Evaluate the risk profile and appetite of your company and current levels of applicable insurance coverage, and assess the need for additional coverage.

SCOPE[1]

Overview

The CCPA gives consumers more control over the personal information that businesses collect about them. The law applies to "businesses," "service providers," and "third parties." An entity may fall into more than one category on the basis of its activities related to personal information.

Who Qualifies as a Business Under the CCPA?

A for-profit entity is a "business" under the CCPA if it does business in California, collects consumers' personal information (directly or indirectly), alone or jointly with others determines the purposes and means of processing the personal information, and satisfies at least one of the following thresholds:

- The entity has more than $25 million in annual gross revenue;
- The entity buys, receives for commercial purposes, sells, or shares for commercial purposes, alone or in combination, personal information of at least 50,000 California consumers, households, or devices; or
- The entity derives 50% or more of its annual revenues from selling consumers' personal information.

In addition, any entity that controls or is controlled by a "business," and that shares common branding with the business (i.e., a shared name, servicemark, or trademark), also qualifies as a "business." Companies do not have to be based in California or have a physical presence in the state to be subject to the CCPA.

Who Qualifies as a Service Provider Under the CCPA?

The CCPA also applies to service providers. A "service provider" is a for-profit entity that processes personal information on behalf of a business for a business purpose under a written contract containing certain restrictive terms. The contract must prohibit the entity from retaining, using, or disclosing the shared personal information for any purpose other than the contractually specified services provided to the business.

A business that discloses personal information to a service provider in accordance with the CCPA is not liable for the service provider's CCPA violations unless, at the time the business disclosed the personal information, it knew or had reason to believe that the service provider intended to violate the statute.

1 Cal. Civ. Code § 1798.115(d) (2018); § 1798.120(b); § 1798.140(c), (v), (w); § 1798.125(a)(6); § 1798.175; § 1798.145.

Who Qualifies as a Third Party Under the CCPA?

The CCPA defines "third party" in the negative. An individual, group, or entity is a "third party" when it is neither:

- A covered business that collects personal information from consumers; nor
- The recipient to whom a business has disclosed a consumer's personal information for a business purpose under a written contract containing certain specified terms restricting the retention, use, disclosure, and sale of personal information.

When a business sells a consumer's personal information to a third party, the third party cannot resell the personal information unless the consumer receives explicit notice and an opportunity to opt out.

Who Is a Consumer?

A "consumer" is a California resident, defined as an individual who is in California for a purpose that is not temporary or transitory or an individual who is domiciled in California but is outside the state for a temporary or transitory purpose.

Exceptions to the CCPA

Government agencies and nonprofit entities not controlling or controlled by a "business" with which they share common branding are not regulated as businesses under the CCPA. The CCPA also does not apply to the collection or sale of personal information if every aspect of that commercial conduct occurs entirely outside California.

The CCPA also does not apply to:

- Medical information governed by the California Confidentiality of Medical Information Act, protected health information collected by entities covered by the privacy rules issued by the Department of Health and Human Services pursuant to HIPAA or the HITECH Act, or providers of health care or covered entities who maintain patient information in accordance with those laws;
- Certain information collected during clinical trials; and
- Certain vehicle or ownership information necessary for implementing a product recall or fulfilling a warranty repair.

Furthermore, information collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act, the Driver's Privacy Protection Act, and the California Financial Information Privacy Act is excluded from most of the CCPA's provisions; only section 1798.150—which governs the private cause of action for data breaches affecting certain

categories of personal information—applies to this data. The same is true for Fair Credit Reporting Act ("FCRA") eligibility information that is collected, maintained, disclosed, sold, communicated, or used by a consumer reporting agency, or a furnisher or users of such information, so long as such eligibility information is used only as the FCRA authorizes.

The CCPA also exempts businesses from their CCPA obligations to the extent that the obligations conflict with businesses' ability to: (1) comply with federal, state, or local law; (2) comply with civil, criminal, or regulatory inquiries or process; (3) cooperate with law enforcement; or (4) exercise or defend legal claims.

As a result of amendments to the CCPA in October 2019, certain information is excluded from the CCPA at least temporarily. Notably, pursuant to AB 25, the CCPA excludes personal information collected by a business about a natural person in his or her capacity as a job applicant to, employee of, owner of, director of, officer of, medical staff member of, or contractor of a business to the extent the personal information is collected or used within that context. Businesses are still required to provide employees with notices about the categories of information a business collects about them and their purpose for doing so, but they would not need to offer opt-out, access, and deletion rights.

Pursuant to AB 1355, personal information collected on or about business contacts in certain business-to-business contexts is excluded from the CCPA. Specifically, the CCPA does not apply to personal information of business contacts collected between a business and an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency as part of a written or verbal communication or transaction or in the context of either due diligence or providing or receiving a product or service to or from such business or agency.

These exemptions are subject to a one-year sunset provision and will last until January 1, 2021.

Final Proposed Regulation Highlight

- **Offline Collection:** The final proposed regulations address certain requirements for businesses that interact with consumers offline. For example, the final proposed regulations contemplate the provision of notice to consumers in an offline setting by allowing a business to provide a printed notice prior to collecting personal information, to direct the consumer to a web address where the notice can be found on "prominent signage," or to provide the notice orally over the telephone or in person. The final proposed regulations also contemplate offline methods for consumers to submit requests. For example, if a business interacts with consumers in person, the business shall consider providing an in-person method for submitting a request "to know" or "to delete," such as a printed form the consumer can directly submit or send by mail, a tablet or computer portal that allows the consumer to complete and submit an online form, or a telephone by which the consumer can call the business's toll-free number.

Action Items

- ✓ Determine whether your company collects personal information from California consumers.
- ✓ Assess whether your company qualifies as a business under the CCPA.
- ✓ Determine whether your company is a service provider or third party under the CCPA.
- ✓ Assess whether any exceptions may apply.

DEFINITION OF "PERSONAL INFORMATION"[2]

Overview

The CCPA defines "personal information" as "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."

The CCPA's definition of "personal information" not only encompasses the data elements typically regarded as personal information in most data breach notification statutes (such as name and Social Security number), but also includes data such as physical characteristics, biometric information, online identifiers, and aspects of a consumer's internet activity. As a result, data such as Internet Protocol ("IP") addresses and geolocation data may be considered personal information under the CCPA, provided it 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.

Nonexhaustive List of Data Elements That Constitute "Personal Information" Under the CCPA

- Identifiers, such as a real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers;
- Characteristics of protected classifications under California or federal law (e.g., age, race, color, ancestry, national origin, citizenship, marital status, sex, or veteran or military status);
- Commercial information, including records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies;
- Biometric information;
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement;
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information;

2 Cal. Civ. Code § 1798.140(o); § 1798.145(a)(5); § 1798.140(h); § 1798.140(a).

- 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. § 1232g, 34 C.F.R. Part 99);
- Inferences drawn from certain specified information to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Limitations on the Definition of "Personal Information"

The CCPA excludes the following from the definition of "personal information":

- Consumer information that is "deidentified" or "aggregate consumer information."
- Publicly available information, meaning information that is lawfully made available from federal, state, or local government records.

Action Items

- ✓ Determine what types of consumer personal information your business collects, shares, and/or sells.
- ✓ Determine whether your business maintains the consumer personal information it collects, shares, and/or sells.
- ✓ Determine where, and for how long, your business maintains such consumer personal information.
- ✓ Develop data mapping to identify, track, and control the collection, retention, and deletion of consumer personal information.

AUTOMATIC DISCLOSURES[3]

Overview

Businesses must make certain disclosures to consumers regarding their collection, use, sale, and sharing of personal information. Businesses must also provide information about consumers' rights under the CCPA and explain how consumers can exercise those rights.

Automatic Disclosures of General Practices Concerning Personal Information

Under the CCPA, businesses must disclose, at or before collection, the categories of personal information they collect and the purposes for which the personal information will be used. Also, the CCPA requires businesses to provide the following information—to be updated every 12 months—in their online privacy policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights. If the business does not maintain those policies, the information needs to be included somewhere on its website:

- A description of the consumer rights set forth in the CCPA, including the right to request information concerning the collection and sale of personal information, the right to request specific pieces of personal information the business has collected about the consumer, the right to require a business to delete consumer personal information, and the right to opt out of any sale by the business of the consumer's personal information;
- A description of the designated methods for the submission of consumer requests concerning personal information;
- A list of the categories of consumer personal information that the business has collected in the preceding 12 months, the categories of sources from which the business collects personal information, and the business or commercial purpose for collecting the personal information;
- The categories of third parties with whom the business shares personal information; and
- A list of the categories of personal information that the business has sold in the preceding 12 months—or a statement by the business that it has not sold consumer personal information in the preceding 12 months; the commercial or business purpose for selling the personal information; and a list of the categories of consumer personal

3 Cal. Civ. Code § 1798.100(b); § 1798.110(c); § 1798.130(a)(5).

information that the business has disclosed for a business purpose in the preceding 12 months—or a statement by the business that it has not disclosed for a business purpose consumer personal information in the preceding 12 months.

In addition to these automatic disclosures, businesses will have to disclose specific information in response to consumer requests to know about the collection and sale of their personal information and to access the personal information (as explained below).

Disclosure Obligations Do Not Create Certain Retention or Linkage Requirements

The CCPA provides that the obligations it imposes on businesses that collect personal information do not require such businesses: (1) to retain any consumer personal information for a single one-time transaction if, in the ordinary course of business, such information is not retained; (2) to reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information; or (3) to collect or retain personal information that the businesses would not otherwise collect or retain in the ordinary course of business.

Final Proposed Regulation Highlight

- **Consumer Notice Requirements:** The final proposed regulations elaborate on the delivery, content, and format of a business's privacy policy, notice at collection (which the regulations provide is not the same as a privacy policy), notice of the right to opt out of a sale of personal information, and notice of financial incentives. The draft regulations provide that such notices must be: (i) drafted in "plain, straightforward language" that "avoid[s] technical or legal jargon"; (ii) available in languages in which the covered entity conducts business; and (iii) reasonably accessible to consumers with disabilities. The final proposed regulations elaborate on the steps a business must take to prepare a notice that is "reasonably accessible" to consumers with disabilities. For example, for notices provided online, a business is required to follow generally recognized industry standards for website accessibility, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium. In other contexts, the business is required to provide information on how a consumer with a disability may access the notice in an alternative format.

  Notably, the final proposed regulations eliminate a business's obligation to provide notice at collection if the entity does not collect information directly from consumers (e.g., through web scraping or other third-party sources), provided the business does not sell the information. In addition, the final proposed regulations exempt businesses that are registered as data brokers with the Attorney General (i.e., businesses that sell personal information collected from consumers indirectly) from providing notice to consumers whose data they collect indirectly if their registration submission includes a link to their online privacy policy with instructions on how a consumer can submit a request to opt out.

Final Proposed Regulation Highlight

- **Privacy Policy Content and Format:** The final proposed regulations add privacy disclosures beyond those identified in the text of the CCPA. For example, a covered business must provide instructions for submitting a verifiable request, the general process the business will use to verify the consumer request, and instructions on how an authorized agent can make a request on the consumer's behalf.

  Another draft privacy policy disclosure applies to any business that knows or reasonably should know that it annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10 million or more consumers. Such entities must disclose certain metrics concerning the number of consumer requests received, complied with, and denied, as well as average response time.

  The final proposed regulations also dictate the format of a privacy policy, requiring, among other provisions, that the policy be presented in a "readable" format (e.g., visible on a smaller device such as a mobile phone or tablet), be reasonably accessible to consumers with disabilities, and be available in a format that allows consumers to print out the policy as a document.

Action Items

- ✓ Create a description of consumer rights set forth in the CCPA.
- ✓ Draft a description of the business or commercial purpose for sharing and selling consumer personal information.
- ✓ Update your online privacy policy and/or company website to comply with CCPA disclosure obligations.

KEY CONSUMER RIGHTS

In addition to providing disclosures, businesses will have to respond to verifiable consumer requests regarding the company's collection, sale, and sharing of personal information; requests to delete personal information; and requests to opt out of the sale of personal information.

RIGHT TO KNOW AND ACCESS[4]

Overview

Upon a verifiable consumer request, a business must disclose the following information to the requesting consumer:

- The categories of the consumer's personal information that the business collected;
- The categories of sources from which the business collected the consumer's personal information;
- The categories of the consumer's personal information that the business sold, and the categories of third parties to which it sold the personal information;
- The categories of the consumer's personal information that the business disclosed for a business purpose, and the categories of third parties to which it disclosed the personal information;
- The business or commercial purpose for collecting or selling the consumer's personal information;
- The categories of third parties with whom the business shared the consumer's personal information; and
- The specific pieces of personal information the business has collected about the requesting consumer.

A business is not obligated, however, to provide this information to the same consumer more than twice in a 12-month period.

Submission of Consumer Requests

Businesses must make two or more designated methods reasonably available to consumers to submit a disclosure request, one of which must include a toll-free telephone number. Any business that maintains an internet website is further required to make the website available to consumers to submit disclosure requests. However, businesses that operate exclusively online and have a direct relationship with consumers need only provide consumers an email address for disclosure requests.

4 Cal. Civ. Code § 1798.100(a); § 1798.110(a)–(b); § 1798.115(a)–(b); § 1798.130(a)(4).

Action Items

- ✓ Establish a method and process for the submission of consumer requests concerning personal information.
- ✓ Draft a written description of the consumer request submission process for publication on the company website.
- ✓ Establish internal procedures for fielding, researching, and responding to consumer requests.

RIGHT TO REQUIRE DELETION OF CONSUMER PERSONAL INFORMATION[5]

Overview

The CCPA establishes a consumer's right to request that a business delete any personal information that the business has collected from the consumer—and requires businesses to disclose this right to consumers. If a business receives such a request from a consumer, it must delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from the service provider's records.

Exceptions to the Requirement to Delete Consumer Personal Information Upon Request

The CCPA lists several exceptions to a consumer's right to require a business to delete his or her personal information. Specifically, a business may deny a verified request if the business can demonstrate that the information is necessary to:

- Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer (or one reasonably anticipated within the context of the business's ongoing business relationship with the consumer), or otherwise perform a contract with 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 existing intended functionality;
- Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law;
- Comply with the California Electronic Communications Privacy Act;
- Engage scientific, historical, or statistical public-interest research in limited circumstances;
- Enable solely internal uses that are reasonably aligned with the expectation of the consumer on the basis of the consumer's relationship with the business;
- Comply with a legal obligation; or
- 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.

5 Cal. Civ. Code § 1798.105.

If the business denies a consumer request under the CCPA, it must inform the consumer of the reasons for not taking action and any right to appeal the decision to the business.

Action Items

- ✓ Establish an internal process for dealing with, validating, and logging consumer deletion requests.
- ✓ Identify exceptions to the deletion requirement that are relevant to your business.
- ✓ Establish a communications protocol for responding to consumer deletion requests.

RIGHT TO OPT OUT OF THE SALE OF PERSONAL INFORMATION[6]

Overview

The CCPA allows consumers to prohibit a business from selling their personal information. This is referred to as the "right to opt out." In addition, businesses must affirmatively obtain permission from consumers who are at least 13 and less than 16 years of age, and parental consent from minors younger than age 13, before selling their personal information.

Opt Out

A consumer has the right, at any time, to direct a business that sells the consumer's personal information to third parties not to sell the consumer's personal information. Businesses that sell consumer personal information must provide notice to consumers that consumer personal information may be sold and that consumers have the right to opt out of the sale of such information.

The CCPA requires that businesses provide a clear link on their homepage titled "Do not sell my personal information" that will direct consumers to a webpage that enables them to opt out of the sale of their personal information. Moreover, businesses cannot require a consumer to create an account in order to effectuate this opt-out right. Businesses also must provide a description of the opt-out rights, as well as a separate link to the "Do not sell my personal information" webpage, in their online privacy policies, other business policies, or any California-specific description of consumers' privacy rights.

A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information, has not received consent to sell that personal information is prohibited from selling the consumer's personal information.

Opt Out: Requests to Sell Information After Opt-Out and Third-Party Data Sales

Once a consumer has exercised the opt-out rights, a business may not request that the consumer authorize the sale of the consumer's personal information for at least 12 months.

In addition, a third party that receives a consumer's personal information from a business may not sell the consumer's personal information unless the consumer receives explicit notice and has an opportunity to opt out.

6 Cal. Civ. Code § 1798.120(a); § 1798.135(a)(5); § 1798.120(d); § 1798.115(d); § 1798.130; § 1798.135.

Action Items

- ✓ Create a "Do not sell my personal information" link/website to satisfy CCPA opt-out rules.
- ✓ Update your online privacy policy and website to satisfy opt-out requirements.
- ✓ Establish a process for tracking consumer opt-outs and segregating consumer personal information sold to third parties.
- ✓ If your business is a third-party recipient of consumer personal information, establish a process for providing notice to relevant consumers of any sale of their personal information.
- ✓ Establish a toll-free telephone number and website for consumer requests.
- ✓ Create an internal process for responding to requests that include reasonable consumer authentication requirements and comply with the CCPA's time limit and format requirements.

RIGHT TO EQUAL SERVICE AND NONDISCRIMINATION[7]

Overview

The CCPA does not permit a business to discriminate against a consumer because the consumer exercised any of the rights in the statute. For example, businesses may not do the following after a consumer exercises CCPA rights:

- Deny goods or services to the consumer;
- Charge the consumer different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties; or
- Provide different levels or qualities of goods or services to the consumer.

Exceptions to the Differential Treatment Ban

A business may, however, charge a consumer a different price or rate, or provide a different level of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.

Businesses also are permitted to offer, on an opt-in basis, "financial incentives" to compensate consumers for the use of their data, but not if the financial incentives are "unjust, unreasonable, coercive, or usurious in nature." For example, a business can offer payments as compensation to consumers who are willing to have their data shared or sold to third parties.

7 Cal. Civ. Code § 1798.125.

Final Proposed Regulation Highlight

- **Responses to Access, Deletion, and Opt-Out Requests:** The final proposed regulations give timing requirements for consumer requests. Within 10 business days of receiving a request for information or deletion, a business must confirm receipt and explain in general to the consumer the procedures for identity verification and request processing, as well as when the consumer can expect to receive a substantive response. The business must give the substantive response within 45 calendar days, or the business can take up to an additional 45 calendar days if it gives the consumer notice and an explanation for the delay.

  Upon receiving a request to opt out of the sale of personal information, a business must comply with the request as soon as possible, but no later than 15 business days from the date of receipt.

  The final proposed regulations also clarify that a business can respond to a deletion request by either permanently erasing personal information from existing systems, deidentifying the personal information, or aggregating the personal information.

  Additionally, the final proposed regulations require that if a business denies a consumer's request to delete, it must ask the consumer if he or she would like to opt out of the sale of his or her personal information, if the business sells personal information and the consumer has not made an opt-out request.

  Finally, under the final proposed regulations, covered businesses cannot disclose sensitive data, such as Social Security numbers, driver's license or other government ID numbers, financial account numbers, health insurance or medical identification numbers, account passwords, security questions and answers, or certain biometric data, in their response to a consumer request for specific pieces of personal information. But the covered business must still inform the consumer with sufficient particularity that it has collected the type of information.

- **Verification of Consumer Requests:** The final proposed regulations require a business to establish, document, and comply with a "reasonable method" of verifying the identity of a consumer who makes a request for information or deletion. The method by which a business chooses to verify must be scaled to the sensitivity of the data request. To that end, the final proposed regulations provide factors a business should consider when implementing a verification method, including:

  - Where feasible, matching the identifying information provided by the consumer to the personal information already maintained by the business;
  - Avoiding collection of certain sensitive personal information, such as a Social Security number or driver's license number; and
  - Considering the type, sensitivity, and value of personal information maintained by the consumer; the risk of harm to the consumer from unauthorized access or deletion; or the likelihood that the request is fraudulent or malicious.

Action Items

- ✓ Calculate the value of consumer personal information to your business.
- ✓ Consider developing financial incentive programs that comply with the CCPA.

ENFORCEMENT, REMEDIES, AND DATA BREACHES[8]

Overview

The California Attorney General may recover statutory damages for violations of the CCPA that are not cured within 30 days of notice to the business (up to $7,500 per intentional violation and up to $2,500 per unintentional violation). The statute also provides for a limited private right of action for a consumer when certain of his or her personal information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of its duty to implement and maintain reasonable security procedures and practices. The California Attorney General may also adopt additional regulations setting forth rules and procedures to follow when fulfilling verifiable consumer requests or any regulation necessary to further the CCPA's purpose. The Attorney General's expanded regulation-making power exposes businesses to additional compliance obligations.

The Private Right of Action

In an effort to remedy violations of the duty to implement and maintain "reasonable security procedures and practices" commensurate with the nature of personal information collected and maintained by companies, the CCPA creates a limited private right of action for a consumer "whose nonencrypted and nonredacted personal information … is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of" this duty. An injured consumer can recover between $100 and $750 per violation, or actual damages (whichever is greater), but first must give the defendant notice of the violation(s), and 30 days to cure the violation(s), before filing a lawsuit. If the business is able to cure the problem within the 30-day window, statutory damages become unavailable to the consumer.

Importantly, the CCPA incorporates by reference the narrower definition of "personal information" set forth in section 1798.81.5(d)(1)(A) for use in determining the viability of a private right of action. This section defines "personal information" as: (i) an individual's first name (or initial) and last name, in combination with certain government-issued identification, certain financial information that would permit access to an individual's financial account, medical or health insurance information, or certain biometric data; or (ii) a username or email address in combination with a password or security question and answer that would permit access to an online account.

8 Cal. Civ. Code § 1798.155; § 1798.150; § 1798.185.

Current California Data Breach Law Remains Largely Intact

The CCPA leaves intact the current California data breach notification statute, § 1798.82. For example, data breach notification requirements will continue to be triggered only in the case of breaches involving the narrower categories of personal information set forth in section 1798.82(h), rather than the more expansive definition of "personal information" found in the CCPA for purposes of businesses' notice obligations and consumer rights.[9]

Action Items

- ✓ Review your network security to ensure that standards are reasonable—particularly with regard to the collection and maintenance of consumer personal information.
- ✓ Tailor mechanisms to process and fulfill verifiable consumer requests such that they comply with the California Attorney General's rules and procedures, once those rules and procedures are finalized.
- ✓ Upgrade your network security as necessary.
- ✓ Identify appropriate encryption solutions and policies.
- ✓ Identify applicable cybersecurity legal requirements (e.g., HIPAA, GLBA) and standards (e.g., NIST, CIS, ISO, COBIT, PCI DSS).
- ✓ Conduct a privileged assessment of your cybersecurity program and map to applicable legal requirements and standards.
- ✓ Review and revise your incident response plan.
- ✓ Address governance issues, including how and when executive leadership manages cybersecurity and the involvement of independent directors.
- ✓ Evaluate the risk profile and appetite of your company and current levels of applicable insurance coverage, and assess the need for additional coverage.

9 The section 1798.82(h) definition of "personal information" is nearly identical to the definition of "personal information" in section 1798.81.5(d)(1)(A), which is incorporated for purposes of the CCPA's private right of action. The only difference between sections 1798.81.5(d)(1)(A) and 1798.82(h) is that section 1798.81.5(d)(1)(A) does not include "[i]nformation or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5" in the definition of "personal information." For additional information about the definitions, please see the glossary at the end of this guide.

SIGNIFICANT MISCELLANEOUS PROVISIONS[10]

Overview

There are a number of other notable provisions in the CCPA. Below are three examples:

- **Ability to Seek an Attorney General Opinion:** The CCPA allows businesses and third parties to seek an opinion of the Attorney General for guidance concerning how to comply with the provisions of the law.
- **Ability to Cure:** The statute also gives businesses 30 days from the date they are notified of noncompliance by the Attorney General to cure any related violations.
- **Creation of a Consumer Privacy Fund:** The CCPA creates a Consumer Privacy Fund ("CPF") within the General Fund of the State Treasury. The purpose of the CPF is to offset any costs incurred by the Attorney General's office in carrying out its duties under the CCPA, as well as any costs incurred by the state courts in connection with actions brought to enforce the statute. Any civil penalties and the proceeds of any settlements resulting from the Attorney General's enforcement actions will be directed into the CPF.

10 Cal. Civ. Code § 1798.155; § 1798.60.

GDPR COMPARISON

Overview

The CCPA is often compared to the European Union's General Data Protection Regulation ("GDPR"). While both laws provide rights to individuals, the CCPA and the GDPR differ in many respects. The GDPR is a far-reaching regulation that encompasses a broad array of compliance topics, including, *inter alia*, personal data processing principles, the legal basis for personal data processing, various rights for data subjects, accountability measures, governance mechanisms for data processing, data security requirements, data breach notification obligations, and conditions for the international transfer of personal data outside the European Union. In contrast, the CCPA focuses on providing consumers more information about businesses' collection, use, disclosure, and sale of consumers' personal information and giving them more control over their personal information.

Comparison Highlights

TOPIC	GDPR	CCPA
Whose data is protected?	Data subjects (i.e., natural persons).	Consumers (i.e., California residents).
Scope	Omnibus law on wide range of topics, including notice, legal basis, cross-border data transfers, data breach notification, etc.	Focuses primarily on consumer rights and disclosures required to consumers.
Who is regulated?	Data controllers and data processors.	Businesses, service providers, and third parties. Businesses have the most CCPA obligations.
Personal information	Any information relating to an identified or identifiable data subject.	Any information that identifies; relates to; describes; is capable of being associated with, or may reasonably be linked, directly or indirectly, with a particular consumer or household.
Individual rights	Access, deletion, rectification, objection, data portability, not to be subject to automated decision making, etc.	Access, opt out of sale, deletion, equal services.

TOPIC	GDPR	CCPA
Legal basis required to process personal information?	Yes.	No.
Notice requirements	Identity of controller, the personal data processed, purpose of processing, legal basis, recipients, data transfer (and mechanism), retention period, data subject rights, etc.	Personal information collected, disclosed for a business purpose, or sold in the last 12 months; the source of the personal information and purpose of the collection; categories of third parties with whom personal information is shared; the purpose for selling personal information; a description of consumer rights and how to exercise the rights.
Service providers	Must execute a written data processing agreement that describes the processing and imposes numerous limitations and obligations on the processor.	Must execute a written agreement that prohibits retaining, using, or disclosing the personal information for any purpose other than performing the services specified in the agreement.

GLOSSARY

Aggregate consumer information	Information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified. (§ 1798.140(a))
Business	**(1)** A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds: **(A)** Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185. **(B)** Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices. **(C)** Derives 50 percent or more of its annual revenues from selling consumers' personal information. **(2)** Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark. (§ 1798.140(c))
Consumer	A natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier. (§ 1798.140(g))

Deidentified	Information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information: **(1)** Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain. **(2)** Has implemented business processes that specifically prohibit reidentification of the information. **(3)** Has implemented business processes to prevent inadvertent release of deidentified information. **(4)** Makes no attempt to reidentify the information. (§ 1798.140(h))
Probabilistic identifier	The identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of "personal information." (§ 1798.140(p))
Processing	Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. (§ 1798.140(q))
Pseudonymize or Pseudonymization	The processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer. (§ 1798.140(r))

Personal information under the CCPA	**(1)** 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. Personal information includes, but is not limited to, the following if it 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: **(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 website, 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, as defined in the Family Educational Rights and Privacy Act (20 U.S.C. § 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. **(2)** "Personal information" does not include publicly available information. For purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government records. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. **(3)** "Personal information" does not include consumer information that is deidentified or aggregate consumer information. (§ 1798.140(o))

Personal information under the California Consumer Records Act's security procedures and practices provision (incorporated by reference in the CCPA's private cause-of-action provision)	**(1)** "Personal information" means either of the following: **(A)** An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: **(i)** Social Security number. **(ii)** Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual. **(iii)** Account number or credit or debit card number, in combination with any required security code, access code, or password, that would permit access to an individual's financial account. **(iv)** Medical information. **(v)** Health insurance information. **(vi)** Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes. **(B)** A username or email address in combination with a password or security question and answer that would permit access to an online account. … **(4)** "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. (§ 1798.81.5(d))

Personal information under the California Consumer Records Act's data breach notification provision (not referenced in the CCPA)	**(h)** "[P]ersonal information" means either of the following: **(1)** An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: **(A)** Social Security number. **(B)** Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual. **(C)** Account number or credit or debit card number, in combination with any required security code, access code, or password, that would permit access to an individual's financial account. **(D)** Medical information. **(E)** Health insurance information. **(F)** Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes. **(G)** Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5. **(2)** A username or email address, in combination with a password or security question and answer, that would permit access to an online account. **(i)(1)** For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. (§ 1798.82)

Service provider	A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business. (§ 1798.140(v))
Third party	A person who is not any of the following: **(1)** The business that collects personal information from consumers under this title. **(2)(A)** A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract: **(i)** Prohibits the person receiving the personal information from: **(I)** Selling the personal information. **(II)** Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract. **(III)** Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business. **(ii)** Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them. **(2)(B)** A person covered by this paragraph who violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation. (§ 1798.140(w))

CONTACT INFORMATION

Americas

Daniel J. McLoon

Los Angeles
+1.213.243.2580
djmcloon@jonesday.com

Lisa M. Ropple

Boston
+1.617.449.6955
lropple@jonesday.com

Edward S. Chang

Irvine
+1.949.553.7561
echang@jonesday.com

Ryan M. DiSantis

Boston
+1.617.449.6911
rdisantis@jonesday.com

Jennifer C. Everett

Washington
+1.202.879.5494
jeverett@jonesday.com

Samir C. Jain

Washington
+1.202.879.3848
sjain@jonesday.com

Richard J. Johnson

Dallas
+1.214.969.3788
jjohnson@jonesday.com

J. Todd Kennard

Columbus
+1.614.281.3989
jtkennard@jonesday.com

James T. Kitchen

Pittsburgh
+1.412.394.7272
jkitchen@jonesday.com

Guillermo E. Larrea

Mexico City
+52.55.3000.4064
glarrea@jonesday.com

Richard M. Martinez

Minneapolis
+1.612.217.8853
rmartinez@jonesday.com

Mauricio F. Paez

New York
+1.212.326.7889
mfpaez@jonesday.com

Jeff Rabkin

San Francisco/Silicon Valley
+1.415.875.5850/+1.650.739.3954
jrabkin@jonesday.com

John A. Vogt

Irvine
+1.949.553.7516
javogt@jonesday.com

Amy Harman Burkart

Boston
+1.617.449.6836
aburkart@jonesday.com

Europe, the Middle East, and Africa

Olivier Haas

Paris
+33.1.56.59.38.84
ohaas@jonesday.com

Dr. Undine von Diemar

Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Dr. Jörg Hladjk

Brussels
+32.2.645.15.30
jhladjk@jonesday.com

Jonathon Little

London
+44.20.7039.5224
jrlittle@jonesday.com

Asia-Pacific

Chiang Ling Li

Hong Kong
+852.3189.7338
chianglingli@jonesday.com

Michiru Takahashi

Tokyo
+81.3.6800.1821
mtakahashi@jonesday.com

Adam Salter

Perth
+61.8.6214.5720
asalter@jonesday.com

Special thanks to the following associates who assisted in the preparation of this Guide: Frances P. Forte, Daniel Lopez, Christina L. O'Tousa, Clinton P. Oxford, Bailey E. Loverin, Jacqueline M. Triggs, and Sharnell S. Simon.


JONES
DAY