Guide to collecting personal information under the California Consumer Privacy Act of 2018

Created by: Donata Kalnenaite and Termageddon.com
Table of contents

1. Introduction;
2. The CCPA and its purposes;
3. Who the CCPA applies to;
4. Penalties for non-compliance;
5. Defining "personal information";
6. Notice requirements;
7. Privacy Policy requirements;
8. Privacy Policy disclosures;
9. Conclusion.
Introduction

What this guide is about, what it encompasses and how it will help you

The California Consumer Privacy Act goes into effect on January 1st, 2020. As more guidance is released, compliance preparations should start now. This guide is based upon and takes into account the following documentation:

(a) The California Consumer Privacy Act of 2018;
(b) AB-874;
(c) AB-1355;
(d) AB-1564;
(e) AB-1146;
(f) AB-25;
(g) AB-1202; and
(h) California Consumer Privacy Act Regulations as promulgated by the California Attorney General.

It is important to note that the Attorney General’s regulations may change. We will update this guide in the case of the amendments not being signed by the Governor or the regulations changing and will provide an updated copy to you in such cases.

We hope that this guide will enable you to:
(a) Better understand the CCPA and its amendments;
(b) Better understand the Attorney General’s regulations;
(c) Prepare your company for compliance;
(d) Prepare your law firm’s clients for compliance; and
(e) Inform you on how to properly collect personal information under the CCPA.
The California Consumer Privacy Act of 2018 ("CCPA") was passed on June 28, 2018 to provide California consumers certain rights when it comes to their data. The CCPA goes into effect on January 1, 2020 and enforcement will commence six months later. The legislature determined that the following facts warrant the provision of privacy rights:

1. The California Constitution, as amended in 1972, establishes a legal and enforceable right to privacy for every Californian;
2. The California legislature has adopted mechanisms to safeguard privacy in the past;
3. California is one of the world’s leaders in the development of new technologies and related industries. This proliferation of personal information has limited the ability of Californians to protect and safeguard their privacy;
4. As the role of technology and data in the everyday lives of consumers increases, there is an increase in the amount of personal information shared by consumers with businesses. California law has not kept pace with these developments;
5. Many businesses collect the personal information of California consumers;
6. In March, 2018, it came to light that tens of millions of people had their personal data misused by the data mining firm called Cambridge Analytics. A series of Congressional hearings highlighted that personal information may be vulnerable to misuse when shared over the internet. As a result, our desire for privacy controls and transparency in data practices is heightened;
7. People desire privacy and more control over their information. California consumers should be able to exercise control over their personal information and they want to be certain that there are safeguards against the misuse of their personal information.
It is possible for businesses to both respect consumers’ privacy and provide a high level of transparency to their data practices. When drafting the CCPA, it was the intent of the legislature to further Californians’ right to privacy by giving consumers an effective way to control their personal information by ensuring the following rights:

(1) The right to know what personal information is being collected about them;
(2) The right to know whether their personal information is sold or disclosed and to whom;
(3) The right to access their personal information;
(4) The right to say no to the sale of personal information;
(5) The right to equal service and price, even if they exercise their privacy rights.

While there are marked differences, it is easy to see the similarities between the CCPA and the General Data Protection Regulation of the European Union. Furthermore, it is interesting to note that a few other states that have proposed their own privacy bills have either cited the CCPA or have taken heavy inspiration from this law.

The CCPA applies to businesses. A business is defined as:

(a) An for-profit legal entity that collects the personal information of consumers, or on the behalf of which such personal information is collected and that alone, or jointly with others, determines the purposes and means of the processing of personal information, that does business in California and meets the following:

(b) Has annual gross revenues in excess of $25,000,000;

(c) Annually buys or receives, for business commercial purposes, rent or shares the personal information of 50,000 or more consumers, households or devices; or

(d) Derives 50% or more of its annual revenues from selling the personal information of consumers.

As the management of vendors and service providers is crucial to CCPA compliance, it is important to note that your business may be subject to the CCPA via contracts, even if it does not meet the specifications outlined above. Therefore, it is important for a lot of businesses to start preparations now.
It is possible for businesses to both respect consumers’ privacy and provide a high level of transparency to the data practices. When drafting the CCPA, it was the intent of the legislature to further Californians’ right to privacy by giving consumers an effective way to control their personal information, by ensuring the following rights:

1. The right to know what personal information is being collected about them;
2. The right to know whether their personal information is sold or disclosed and to whom;
3. The right to say no to the sale of personal information;
4. The right to access their personal information; and
5. The right to equal service and price, even if they exercise their privacy rights.

The CCPA does not apply to the following:

1. Medical information governed by the Confidentiality of Medical Information Act or HIPAA;
2. A provider of healthcare governed by the Confidentiality of Medical Information Act or HIPAA;
3. Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonization or pursuant to human subject protection requirements of the United States Food and Drug Administration;
4. An activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer’s creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency or by a furnisher of information who provides information for use in a consumer report or by a user of a consumer report;
5. Personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act or the California Financial Information Privacy Act;
6. Vehicle information or ownership information retained or shared between a new motor vehicle dealer and the vehicle manufacturer if the information is shared for the purpose of effectuating a vehicle repair, warranty, service or recall.

7. Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, employee of, owner of, director of, officer of, medical staff member of, or contract of that business. This exception applies to the extent that the information is collected and used by the business solely within the context of the person’s role or former role.
8. Personal information that is collected by a business that is an emergency contact information of a person acting as a job applicant to, employee of, owner of, director of, officer of medical staff member of, or contractor of that business to the extent that the information is used solely in the context of having an emergency contact on file.
9. Personal information that is necessary for the business to retain in administration benefits for another person relating to that person acting as a job applicant to, an employee of, owner of, director of, officer of medical staff member of, or contractor of that business to the extent that the information is used solely in the context of administering those benefits.
The penalties for non-compliance are $2,500 per violation or $7,500 per intentional violation.

While the CCPA is generally enforced by the Attorney General, it also provides a private right of action. This private right of action is available to any consumer whose non-encrypted or non-redacted personal information is subject to 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 that are appropriate to the nature of the personal information.

The consumer may receive any of the following in a civil action:
(1) Damages of not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is higher;
(2) Injunctive or declaratory relief;
(3) Any other relief the court deems proper.

If a consumer files an action, the Attorney General has 30 days to determine whether he or she will prosecute the business. Implementing cybersecurity best practices should be an integral part of CCPA compliance and business should consult an IT professional to prepare.
The CCPA provides that consumers have the right to know what personal information is collected about them. This right is presented at two points in the customer journey: prior to the collection of personal information and after the collection of personal information. The CCPA requires businesses that collect personal information to have a notice and a Privacy Policy that make certain disclosures.

First, let’s define “personal information” under the CCPA. “Personal information” 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. Includes:

1. Identifiers such as name, alias, postal address, unique personal identifier, IP address, email address, account name, social security number, driver’s license number or passport number;
2. Other information such as signature, physical characteristics or description, telephone number, date of birth, number, insurance policy number, education, employment, employment history, social security number, credit card number, debit card number, any other financial information, medical information or health insurance information;
3. Any characteristics of protected classifications under California law or federal law;
4. Commercial information, including records of personal property, products or services purchased, obtained or considered or other purchasing or consuming histories or tendencies;
5. Biometric information;
6. Internet or other electronic network activity information, including browsing history, search history, and information regarding a consumer’s interaction with a website, application or advertisement;
10. Geolocation data;
11. Audio, electronic, visual, thermal, olfactory, or other similar information;
12. Professional or employment-related information;
13. Education information; and
14. Inferences drawn from any of the information above to create a profile of a consumer reflecting their preferences, characteristics, psychological traits, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.

When determining whether something is considered personal information, make sure that you are accounting for the exceptions noted above and that information kept in certain ways may be exempt.

The CCPA requires businesses that collect the personal information of consumers to provide a notice at the time of collection of personal information. This means that a business must have a notice that informs consumers of certain aspects of what data is collected, for what purposes it will be used and other disclosures.

The notice must be designed and presented to the consumer in a way that is easy to read and understandable to the average consumer. The notice must:
1. Use plain and straightforward language and avoid technical or legal jargon;
2. Use a format that draws the consumers’ attention to the notice and makes the notice readable, including on smaller screens;
3. Be available in the languages in which the business in its ordinary course, provides contracts, disclaimers, sale announcements, or other information to consumers; and
4. Be accessible consumers with disabilities.

At a minimum, the notice must provide consumers information on how they can access the notice in an alternative format. A business must include the following in its notice:
1. A list of categories of personal information it collects from consumers. Each category must give the consumer a meaningful understanding of the personal information collected.
2. For each category of personal information collected, the business or commercial purpose(s) for which it will be used.
3. If the business sells the personal information, the link titled “Do Not Sell My Personal Information” or “Do Not Sell My Info”, or, in the case of offline notices, the web address for the webpage to which it links.
4. A link to the business’ Privacy Policy or, in the case of offline notices, the web address of the business’ Privacy Policy.

In the case of personal information being collected online, this notice may be given by providing a link to the business’ Privacy Policy.

A business may not use the personal information for any purpose other than those disclosures in the notice. If you do not use it for a purpose that was not disclosed, you must directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for that new purpose. You may not collect additional information that is not listed on the notice. If you do wish to collect additional information, you must provide the consumer with a new notice at the point of collection.

Note that while it may be tempting for businesses to provide a GDPR-like notice and consent solution, the CCPA does not require opt-in consent for the collection of personal information in most cases, meaning that GDPR-like notices may not be required under the CCPA.

The CCPA also requires businesses that collect the personal information of consumers to provide a Privacy Policy.

The Privacy Policy must meet all of the same requirements as the notice in terms of readability, format, availability and accessibility. However, the Privacy Policy must also include an alternative format that allows the consumer to print it out as a separate document.
The requirements of the CCPA should not be construed to require the business to retain any personal information collected for a single, one-time transaction, if the personal information is not sold or retained by the business or to re-identify or otherwise link personal information that is not maintained in a manner that would be considered personal information.

A Privacy Policy must be posted online through a conspicuous link using the word “privacy” on the business’s website homepage or on the download or landing page of a mobile application. If the business has a California-specific description of consumer’s privacy rights on its website, then the Privacy Policy must be included in that description. A business that does not operate a website must make the Privacy Policy conspicuously available to consumers.

How can a Privacy Policy be conspicuous? While this is done expressly defined by the CCPA, the California Online Privacy Protection Act of 2003 (“CalOPPA”) defines “conspicuously post” as posting the Privacy Policy with a text that hyperlinks to a web page on which the Privacy Policy is posted and if the text link does any of the following to include the word “privacy”:

1. Is written in capital letters equal to or greater in size than the surrounding text or
2. Is written in larger type than the surrounding text, or in contrasting type, font (or color) to the surrounding text of the same size or set off from the surrounding text of the same size by symbols or other marks that call attention to the language.

The requirements of the CCPA should not be construed to require the business to retain any personal information collected for a single, one-time transaction, if the personal information is not sold or retained by the business or to re-identify or otherwise link personal information that is not maintained in a manner that would be considered personal information.

A Privacy Policy must disclose:

1. A description of the consumer’s rights and one or more methods for designating requests;
2. A list of categories of personal information the business has collected about consumers in the last 12 months, by reference to categories in §3;
3. Two separate lists:
   i. A list of categories of personal information the business has sold in the last 12 months. If no personal information is sold, then you must disclose that;
   ii. A list of personal information categories the business has disclosed in the last 12 months. If no personal information has been disclosed, then you must disclose that;
4. How a consumer can designate an authorized agent;
5. A contact that the consumer can reach for any questions or concerns;
6. The date the Privacy Policy was last updated; and
7. If the business annually sells the personal information of 4,000,000 or more consumers, include the required disclosures.
When it comes to the right to know about the personal information collected, disclosed, or sold, the Privacy Policy must disclose the following:

1. Explain that the consumer has the right to request that the business disclose what personal information it collects, discloses, and sells.
2. Provide instructions for submitting a verifiable consumer request to know and provide links to an online request form or portal for making the request, if offered by the business.
3. Describe the process the business will use to verify the consumer request, including any information that the consumer must provide.
4. List the categories of personal information the business has collected about consumers in the preceding 12 months.
5. For each category of personal information collected, provide the categories of sources from which the personal information was collected, the business or commercial purposes for which the personal information is collected, and the categories of third parties with whom the business shares the personal information.

Privacy Policy disclosures

The CCPA requires you to provide disclosures for the right to know.
When it comes to the right of a consumer to request the deletion of their personal information, your Privacy Policy must disclose:

1. Explain that the consumer has the right to request the deletion of their personal information collected or maintained by the business;
2. Provide instructions for submitting a verifiable consumer request to delete and provide links to an online request form, or points for mailing the request, if offered by the business;
3. Describe the process by which the business will verify the consumer request, including any information that the consumer must provide.

The CCPA requires you to provide disclosures for the right to request deletion.
When it comes to the right of a consumer to opt-out of the sale of their personal information, your Privacy Policy must disclose the following:

1. Explain that the consumer has the right to opt-out of the sale of their personal information by the business; and
2. Include the contents of the notice of right to opt-out in accordance with the CCPA.

Please note that we will be creating a separate guide to selling personal information under the CCPA for businesses that participate in such sales.

The CCPA requires you to provide disclosures of the right to opt-out of the sale of their personal information.

It is important to remember that the CCPA defines “selling” as selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business or another business or a third party, for monetary or other valuable consideration.

Note that due to this broad definition, you need to ensure that your contracts with vendors specify that you are not selling the personal information of your customers.
When it comes to the right of a consumer to not be discriminated against, your Privacy Policy must explain that the consumer has the right not to receive discriminatory treatment by the business for the exercise of their privacy rights granted by the CCPA.

The CCPA prohibits discrimination by:
1. Denying goods or services to the consumer;
2. Charging different prices or rates for goods or services, including through the use of discounts or other benefits imposing penalties;
3. Providing a different level or quality of goods or services to the consumer or suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

The CCPA requires you to provide disclosures of the right to non-discrimination.
The CCPA also requires your Privacy Policy to disclose:

1. Explain how a consumer can designate an authorized agent to make a request under the CCPA on the consumer’s behalf;

2. Provide consumers with a contact for questions or concerns about the business’s privacy policies and practices using a method reflecting the manner in which the business primarily interacts with the consumer;

3. The date the Privacy Policy was last updated;

4. If your business annually sells the personal information of 4,000,000 or more consumers, include the required disclosures.

Other disclosures required by the CCPA
The CCPA goes into effect on January 1st, 2020, meaning that businesses have only a few months left to prepare for it and preparations for this law should commence right now.

If you are not certain of where to begin, you should start by completing the following:

- Understand what personal information you collect and what sources you collect it from;
- Determine whether you are collecting more information than what is really needed and practice data minimization;
- Determine who you share that data with and whether that sharing is truly necessary;
- Build your Privacy Policy and ensure that it has all of the required disclosures;
- Ensure that your Privacy Policy is displayed in the correct way;
- Build your notice and ensure that it has all of the required disclosures and is displayed in the correct way;
- Determine whether you sell data and whether contracts with your service providers are appropriate.

Conclusion

Preparations for the CCPA should start now.