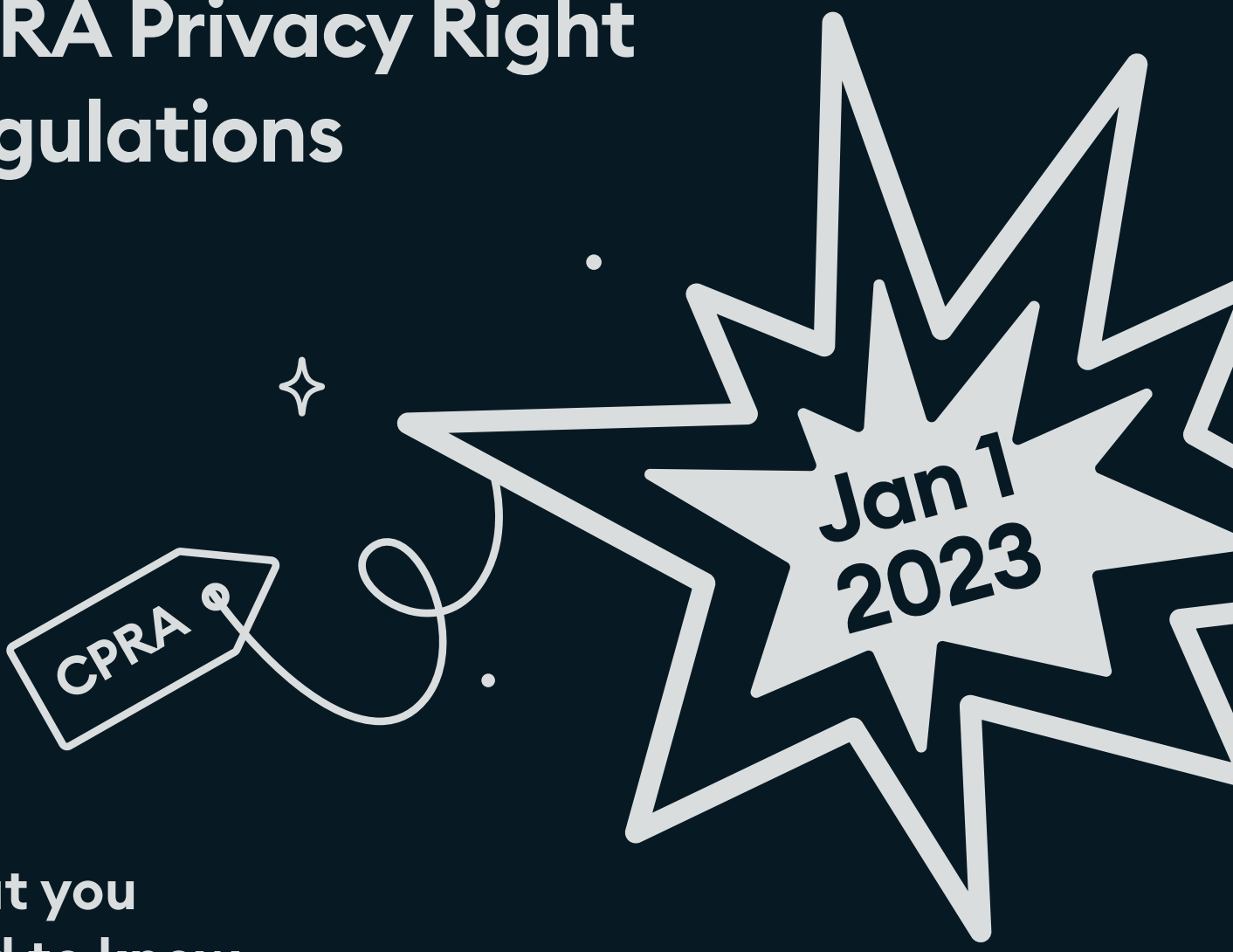
Ketch

Guide:

Complete Compliance Guide for the California Privacy Regulations

California's CCPA/ CPRA Privacy Right Regulations



What you need to know

Passed by the California State Legislature and signed into law on June 28, 2018, the California Consumer Privacy Act (CCPA) went into effect on January 1, 2020, to give California residents more control over how businesses handle their personal information.

The CCPA will be superseded on January 1, 2023, when the recently approved California Privacy Rights Act (CPRA) goes into effect. This guide is intended to help you understand how CCPA and ultimately CPRA apply to and impact your business and help put you on the path to ensuring and easing compliance.

What is the CCPA?

The first law of its kind in the United States, the California Consumer Privacy Act (CCPA) was initiated in the wake of Europe's even more comprehensive General Data Protection Regulation (GDPR) to improve data transparency in the most populous U.S. state. Signed into law on June 28, 2018, and taking effect on January 1, 2020, CCPA applies to any for-profit business anywhere in the world that meets any one of the following thresholds:

- ☐ **Annual gross revenue in excess of $25 million**
- ☐ **Buying, receiving, or selling personal information of more than 50,000 consumers or households**
- ☐ **Earning more than half of your annual revenue from selling personal information**

Under the CCPA, California residents have the following privacy rights regarding their personal information:

- The right to know what personal information has been collected, used, shared or sold and for what purposes
- The right to delete any personal information that has been collected, with some exceptions such as data needed to satisfy transaction, security, legal and functionality obligations
- The right to opt-out of a business selling any personal information via a required clear and easily accessible "Do Not Sell My Personal Information" option
- The right to non-discrimination for exercising CCPA rights, meaning that a business cannot deny or alter price or quality of goods or services for an individual exercising CCPA rights

Since CCPA was signed into law, the California State Legislature has already approved additional amendments that cover additional exemptions and provide further clarification, including:

- Exemptions for human resource data required for the purpose of employment and administering employment benefits
- Exemptions for information necessary to maintain a warranty or product recall, including vehicle information
- Clarification regarding the definition of "verifiable consumer request" and allowing a business to require reasonable authentication of a consumer's identity for the purposes of responding to a consumer request
- Clarification regarding the definition of personal information and the definition of "publicly available" information
- Consideration of the value of information to a business (in relations to nondiscrimination), allowing businesses to alter price or quality of goods or services if consumer data is directly related to the value provided to the business

What is the CPRA?

Coined CCPA 2.0, the California Privacy Rights Act (CPRA) was approved by voters on November 4, 2020, as a means to improve upon the existing CCPA. The new rights and requirements outlined in the CPRA will go into effect and supersede CCPA on January 2, 2023, resulting in a law more in line with the EU's GDPR and providing greater protection for consumers and additional compliance regulations for businesses.

One of the key provisions introduced in the CPRA is the establishment of the California Privacy Protection Agency (CPPA) that will be responsible for auditing and enforcing CCPA. Unlike GDPR that included a governing authority, the original CCPA lacked a dedicated "watchdog" to enforce the law and an advocate to provide businesses and consumers with an educational venue for public awareness and understanding of rights and obligations. The establishment of the CPPA fills this previous gap.

CPRA also doubles CCPA's 50,000 threshold to companies that buy, receive or sell personal information of more than 100,000 consumers or households. **Additional modifications that help eliminate ambiguity, better define who must comply and provide greater protection, include:**

- New requirements for service providers, contractors and third parties, requiring businesses that send personal information to these entities to ensure that they also comply.
- Expansion of the right to opt-out from "Do Not Sell" to "Do Not Sell or Share" personal Information
- Limitations regarding "sensitive" personal information (e.g., social security number, log-in credentials, health information, etc.)
- Limitations on the storage of information, preventing businesses from maintaining personal information longer than necessary and providing consumers with the right to know the length of time that each category of personal information will be maintained
- Limitations on the information businesses can collect, preventing them from collecting more information than is necessary for a particular business function
- Expanded consumer rights surrounding right to opt out, right to deletion, right to access and right to correct inaccurate data, including the right to right to opt out of advertisers using precise geolocation (< 1/3 mile)
- Additional restrictions on the transfer of personal information and additional penalties if information is stolen due to negligence
- Regular cybersecurity auditing and risk assessment requirements for businesses considered high-risk data processors

Does CPRA/CCPA Apply to Your Business?

CCPA and CPRA are applicable to any for-profit entity doing business in California that meet any one of the following thresholds:

- ☐ **Annual gross revenue in excess of $25 million**
- ☐ **Buying, receiving, or selling personal information of more than 50,000 consumers or households**
- ☐ **Earning more than half of your annual revenue from selling personal information**

While that may seem clear in theory, many businesses are still not entirely certain if they need to comply. First, it's important to understand that your business does not need to be physically located in California, or even in the U.S. for that matter. Regardless of whether the processing of information takes place in California or not, you need to comply if you're handling personal data of California residents and meet any of the thresholds. Along those lines, it's also important to note that the annual gross revenue threshold of $25 million applies to ALL revenue, regardless of its source. In other words, even if only $3 million of your annual revenue comes from doing business with California residents, if your total revenue exceeds $25 million, you will still need to comply.

Considering that California is the most populous U.S. state with nearly 40 million residents and the fifth largest global economy, it is more likely than not that anyone conducting business at material scale in the U.S. needs to comply. Given the growth of the digital economy and ever-increasing e-commerce, CPRA/CCPA regulations are also set to impact more businesses than ever before. Smaller businesses that don't currently meet the thresholds may eventually find themselves needing to comply when they take their business online and open the door to provide goods or services to California residents.

Buying, receiving or selling personal information of California residents can occur through a myriad of obvious transactions, but there also some not-so obvious means that may require you to comply. For example, regardless of the goods or services your business offers, it is likely that you also rely on third parties to help with data storage and processing, purchasing and fulfillment, and other everyday operations. If you provide personal information to a third party required to comply with CPRA/CCPA, it's your responsibility to ensure that they comply. While large entities like Facebook make this easier by implementing features that limit the way user data is handled for California residents and new CCPArequired contract terms, it's important to identify all third-party vendors and determine compliance. Comprehensive data mapping and discovery can go a long way helping you identify all the actors with whom your business shares information and where that information resides.

Does CPRA/CCPA Apply to Your Business?

If your revenue is less than $25 million and you don't exceed the threshold for the number of consumers or households, that doesn't necessarily mean you are exempt–more than half your annual revenue may still come from selling personal information. Under CPRA/CCPA, the definition of "selling" is not confined to the classic sense of the word but rather broadly defined as "selling, renting, releasing, disclosing, disseminating, making available, transferring or communicating orally, in writing, or by electronic or other means, a consumer's personal information to another business or their party for monetary or other valuable consideration." This has caused quite a bit of confusion–even if you are not directly being paid for data, if personal information is provided as part of a sale, it is considered a sale. That essentially means that transferring information to third-party advertisers via cookies, which is a valuable consideration, is considered a sale.

There are of course exemptions, including the disclosing of information to service providers when necessary to perform a specific business purpose. However, to know if you need to comply, it's important to understand what constitutes a sale of personal information. You also need to know this information to effectively comply with any "opt outs."

The Price of Non-Compliance

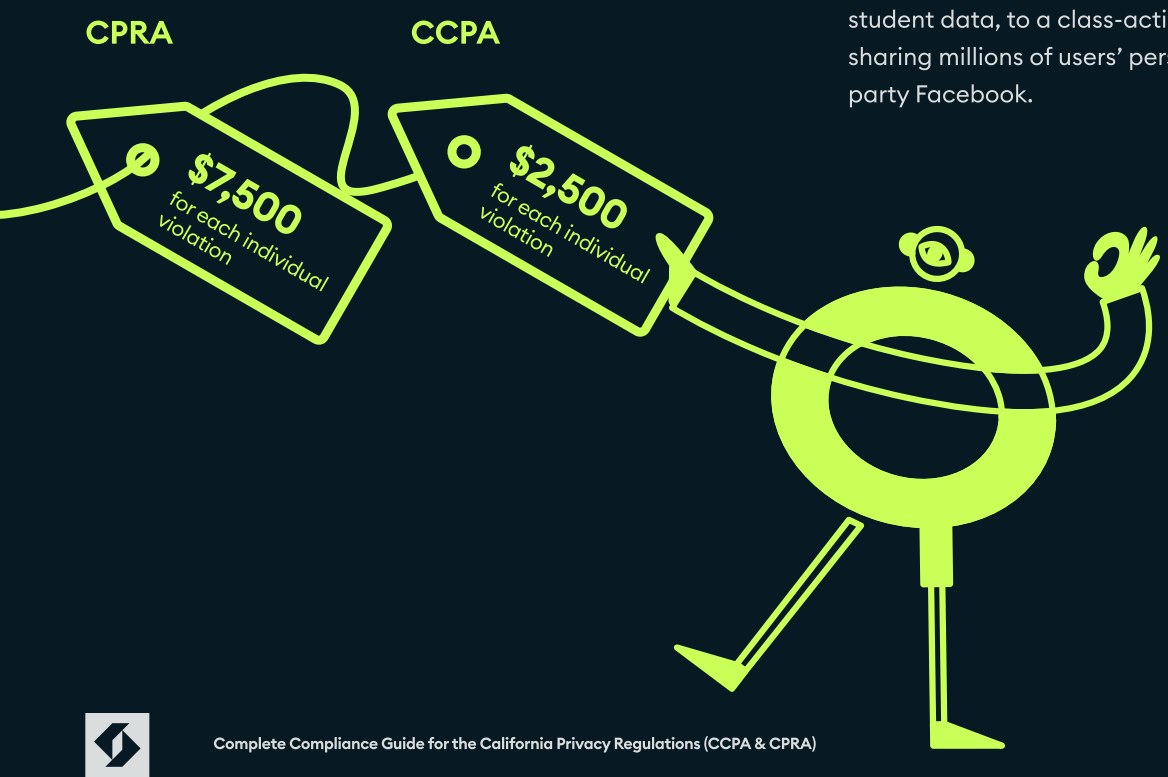
Like GDPR, businesses required to be CPRA/CCPA-compliant must provide notice to consumers at the time they collect personal data, allow them to opt out and disclose the reason for retaining, sharing or selling personal information. They also must allow consumers to access and delete their personal information, respond to consumer requests within specific timeframes, and maintain all records of requests for a minimum of two years.

Penalties violating CCPA can cost businesses $2500 for each individual violation (i.e., per consumer), with higher fees for intentional violations. While you can avoid liability if you cure the noncompliance within 30 days, there are some types of non-compliance that may not be capable of a cure. For example, if a data breach has already occurred, there's little you can do to fix it.

With the passing of the CPRA, the price of non-compliance has increased and the establishment of the CCPA is expected to result in greater enforcement. Most notably, CPRA triples the maximum penalty for an individual violation to $7500 for violations concerning minors.

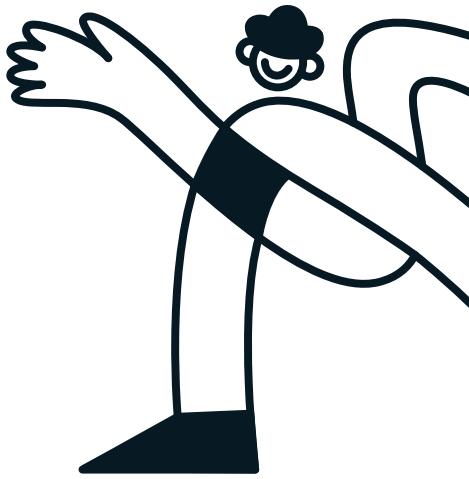
While these fees seem minor, a business faced with one individual violation may likely have hundreds, thousands or even millions of violations–and all it takes is for one individual to determine and publicize the violation for the fees to stack up. And CPRA/CCPA has NO ceiling on the number of violations. An online retailer doing business with a million Californians could quickly find themselves faced with $2.5 billion in fines.

While you might think you still have time since CCPA just went into effect in 2020 and CPRA won't go into effect until 2023, think again. Just six months into 2020, more than 50 lawsuits invoked the CCPA–everything from a student data management software company that failed to safeguard student data, to a class-action lawsuit against Zoom for sharing millions of users' personal information through third-party Facebook.



The Time is Now!

Not taking the appropriate steps to ensure compliance is a significant risk that can ultimately mean the difference between business success or business failure. Now is the time to become CCPA/CPRA compliant—and it all starts by following these simple steps.



01

Determine if your business needs to comply (using this guide)

02

Understand how it can affect your business

03

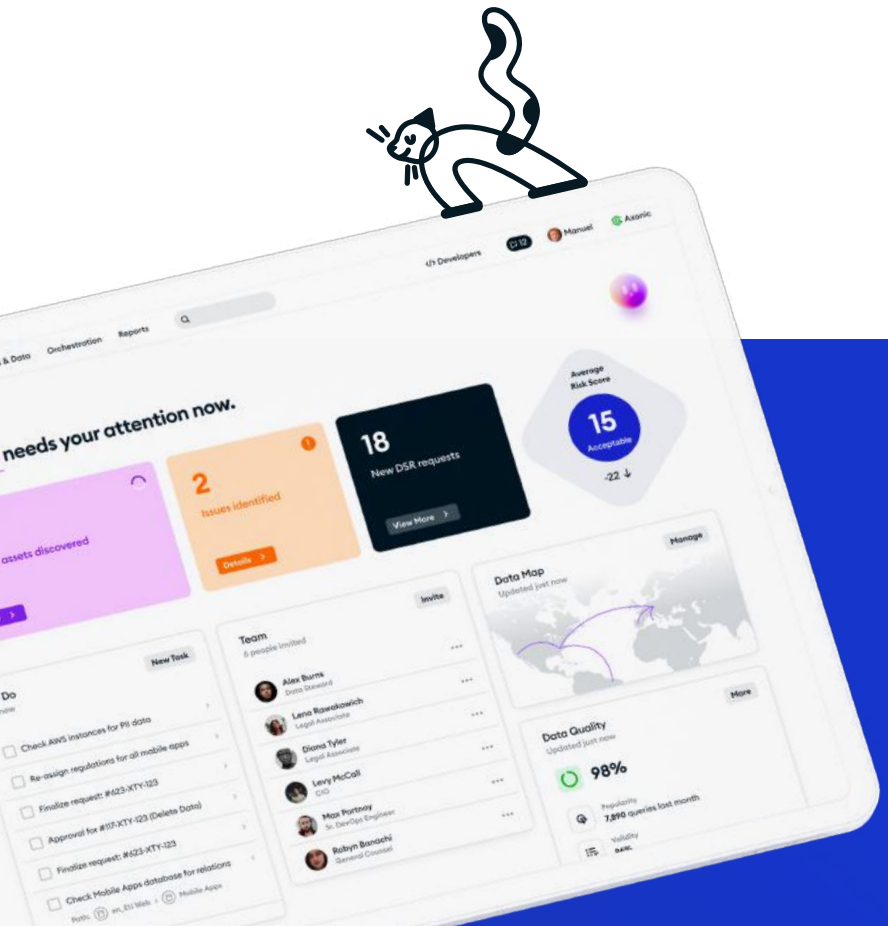
Map and discover consumer data across all systems, including third-party

04

Update your software, systems and subsystems for compliance and opt-out options

05

Streamline your policies and procedures for effective response and protection



Want to learn more? Schedule a custom demo

Request a Demo →

Visit us at **ketch.com** @ketch_digital