osano

Prepare for California's next big privacy law:

The CPRA

Frequently Asked Questions

In January 2023, a large part of the California Privacy Rights Act (CPRA) will go into effect. But what does it mean? How does that affect your business — does it even affect your business? Find the answers to these questions (and more) in our FAQ.

What is the CPRA? 3

Why does it matter to me? 3

How should I prepare? 4

What are some of the big changes? 7

What does enforcement look like? 8

What do we start with? 9

Conclusion 10

What is the CPRA?

What is the CPRA?

The CPRA is the acronym for the California Privacy Rights Act, and, as the name implies, it extends a suite of privacy rights to the citizens of California. It passed by popular vote in California in November 2020, and a large part of it goes into effect in January of 2023.

Wait. I thought the CCPA was the California privacy law. Are the CPRA and CCPA the same thing?

The CCPA — the California Consumer Privacy Act — passed first in 2018. However, the Californians for Consumer Privacy (the group behind the CCPA) had misgivings about the law almost as soon as legislators passed it. They immediately started a campaign to make it stronger and more protective of consumer rights.

The CPRA builds upon the CCPA, changing some of the text, adding other text, and clarifying some questions around enforcement and who's actually covered by the law.

At this point, for all intents and purposes, the CPRA is the only law you need to worry about, as it's like the CCPA+, and it covers the entirety of the text you need for understanding the California privacy law. However, the California Attorney General's Office is still clarifying some of the operational mandates of the CPRA, and that text keeps getting pushed off down the road.

You should expect that the AG's office will continue to issue information about how to interpret the law and how they will enforce it for the next few years.

Why does it matter to me?

How do I know if I have to pay attention to the CPRA? I don't even have an office in California!

The CPRA covers every for-profit organization that "does business" in the state of California, collects the personal data of Californians or has it collected for them, and fits one or more of these criteria:

- Buys, sells, or shares the personal information of 100,000 people or households.
- Creates 50% or more of its revenues through the sale or sharing of personal information.
- Had $25 million in gross revenue in the preceding calendar year (so January 1, 2022 to December 31, 2023 to start).

Some caveats make it clear you can't just chop your business up into little companies to make it so you don't meet the thresholds.

If you're not sure whether you're subject to the CPRA, you should talk to a lawyer who does this for a living.

How should I prepare?

I heard you just have to put a "Do Not Sell" button on your website, and then you're basically good. Is that right?

That's a great line, but since you're reading this right now, hopefully, you understand the greater legal landscape surrounding privacy and your responsibilities are changing very quickly. Not only is the CPRA coming into force, but we're also seeing new privacy laws being discussed or passed in states like Colorado, Virginia, Washington, and even Utah.

The CPRA should be a big blinking-red light, with maybe an alarm, warning you that the days when you could do whatever you wanted with personal data in the US are coming to an end.

The CPRA creates the California Privacy Protection Agency, with a Chief Privacy Auditor. It's the first state agency dedicated solely to privacy enforcement, with no need to depend on an attorney general's office or the Federal Trade Commission. Other states will follow.

That means you need to have a good handle on what personal information you collect, why you collect it, and what you do with it once you've collected it. You need to know where you store it and with whom you share it.

If you've already done this exercise for the European Union's GDPR, you probably don't have to do much extra work for the CPRA. If you haven't, you'll need cross-team support throughout your organization to make sure you can confirm compliance now and going forward.

Okay, that sounds like more than a "Do Not Sell" button. But why do we need "cross-team support"? Can't our lawyer or privacy professional handle it?

You will definitely need some legal support, and it's a great idea to have dedicated privacy professionals overseeing your compliance efforts, but complying with the CPRA isn't just a one-time exercise or an annual review. It's an ongoing effort to make sure you're handling personal data correctly.

In broad strokes, you need to explain what personal data you collect, why you collect it, and then only use that personal data for the purpose for which you collected it. And you can only keep it on hand for the amount of time necessary to fulfill that purpose. That will likely be a big mind-shift for companies operating under the assumption that any data they collect is theirs to use and analyze and try to profit off of in perpetuity.

The CPRA requires a change in thinking. Arguably, a lot of innovation has come about thanks to data mining and research using personal data. Now you have to get permission for that first. Or you have to anonymize the data so no one can reconnect it back to the person who created it. You have to be thoughtful about what you're collecting, why, and what permissions you're requesting.

For example, IT and data analytics teams will need to work with legal and compliance and privacy teams to ensure data minimization and retention policies are in place, followed, and properly audited.

There are many resources out there for getting up to speed. But you might want to start at the CPRA's official site (https://www.caprivacy.org/cpra-resource-center/).

How should I prepare? (cont.)

Okay, okay. But that looks like a lot! Where should we focus as we get started?

Generally, your company is probably in one of two buckets:

1. Companies that haven't really done any California privacy yet, for whatever reason.
2. Companies that have already started with CCPA compliance and just need to tune-up for CPRA.

If you haven't started with the CCPA:

In short, you need to develop a privacy, data protection, or personal data compliance program. Whatever you call it, you need to create a series of roles that ensure you are correctly handling personal data and can accomplish the following basic tasks:

- Create an inventory of all the personal data your organization holds.
- Create an inventory of all the other organizations with which you share personal data, to whom you sell personal data, or from whom you buy personal data.
- Understand the permissions you have to use all of that data you hold, share, and sell.
- Create a process going forward for getting permission (consent) to use personal data in all the ways you'd like to use it.
- Create a process for identifying that a person is who they say they are. Then, when they ask you to do something, you don't delete or supply someone else's information, which would be a problem.
- Create a process for deleting data upon request.
- Create a process for supplying a person with all of the data you have about them upon request.
- Create a process for correcting personal data when asked to fix it.
- Create a process for making sure you don't sell or share data if you are asked not to share or sell it.
- Create a process for making sure you are not collecting the data of a child without parental consent.
- Create a process for identifying certain "sensitive" personal data, giving it extra protection, and making sure not to use it upon request.
- And more!

Suffice it to say, you need to do more than read this and do what it says. You will need to do significant research and invest in the people and time necessary to make sure you're in compliance.

How should I prepare? (cont.)

If you have started with the CCPA:

If you're already feeling good about your CCPA compliance, you're ahead of the game. The CPRA changes should be a matter of degree, not a significant wholesale change. To start:

- Employees and the data of business-to-business contacts are no longer exempt. All personal data is basically treated equally now.
- Everyone now has the right to correct their data with you, ask you not to share it in any way, and ask you not to use sensitive data at all. This is in addition to the right to ask you to delete it and ask you not to sell it.
- You now have to contract with the people you share data with and sell data to, ensuring that they treat the data the same way you would.
- "Public" data is now much more narrowly defined as "data released specifically by a government agency." And you can only use that public data for the purpose it was gathered and released by the government. Just because it's already on the internet doesn't mean it's "public" and fair game.

And the bad news is that the "30-day cure period" is gone. Before, the attorney general's office had to give you 30 days to fix anything you were doing wrong before they could enforce the law against you. No longer.

Companies now need to be a lot more risk-averse at the outset of any collection of personal data.

What are some of the big changes?

Wait, if employees ask to see everything we have about them, we have to show them? And we have to delete information they ask us to delete? And correct it?

Yes. True story. And you might have to commit a lot of resources, as a request could cover all emails you have on the server that mention an employee, as just one example. Some employees — even some former employees — could choose to use this right punitively. So you may want to re-examine just what information you wish to retain on employees in general.

There can be a lot of litigation with this specific piece — we've seen it in Europe since GDPR's implementation, which confers similar rights to employees.

Remember, though, that this only applies to employees who are actually working in California. Your whole company might be subject to the CPRA because you meet the thresholds above, but that doesn't mean employees working in Massachusetts get the same rights as people in California.

Whether it's practical to separate those two groups — employees in California or not—will be different from one business to another.

Well, that all sounds like a lot, but I guess it's good that we know the rules now and can start to figure them out, right?

Sort of.

What do you mean, "sort of"? That sounds bad!

Unfortunately for those who just want to know the rules, there are still more rules yet to come. The CPRA empowers the Attorney General's office and the California Privacy Protection Agency to conduct "rulemaking" in various areas. They can potentially change:

- What information is considered personal information.
- What "deidentified" actually means.
- The rules for allowing people to opt-out of selling and sharing their information.
- The definition of "easily understood" to make sure consumers are getting clear information about what you're going to do with their data and their rights.
- The monetary levels for when the law covers companies, every other year (for example, revenues of $30 million annually in a future year).

They can adjust plenty of other definitions, too! There are 22 different areas where rulemaking is allowed.

In short, you'll need to pay attention to press releases and news reports on new rules issued by the Privacy Protection Agency. They're supposed to be done by July of 2022, but sometimes the can is kicked down the road in California. If we're lucky, we'll get that full six months to digest and understand the rulemaking and regulations before the law comes into force in 2023.

What does enforcement look like?

Yikes. Well, what happens if we don't comply?

The stakes are pretty high, actually.

The new CPRA empowers the Attorney General, California's 62 different district attorneys, and the California Privacy Protection Agency to enforce the law.

The penalties include:

- $2000 per offense if you made relatively honest mistakes.
- $2500 per offense if you made negligent mistakes where you didn't seem to be trying all that hard.
- $7500 per offense if it can be proven you knew you were breaking the law and did it regardless.

And "per offense" means "per person whose data you mishandled." So if you have a database with thousands of people in it, and you broke the law in the same way with all of them, that adds up pretty quickly.

But how active do you think enforcement will be? Will it be like the FTC, where there are only one or two cases a year?

They hired Ashkan Soltani, a noted privacy advocate and technology expert, to be the Executive Director of the California Privacy Protection Agency. He won't mess around. You can expect them to hit the ground running and to look to make examples out of bad actors.

Some people expect initial company outreach to involve warnings and general notices to clean up non-compliant activities. Still, it's probably not a great idea to expect to get a warning letter before an enforcement notice. If you're actively breaking the law, and you don't appear to be doing anything to comply, they are unlikely to look kindly at that.

What do we start with?

At least we don't have to worry about this until January 2023. That's still a ways away.

MMmmmmmm.

What?

Well, there's this thing called the look-back period.

Look-back period?

Yeah. Essentially, because the law says you have to be able to supply all of a person's personal data to them going back to January 1, 2022, as soon as the law comes into force on January 1, 2023, you really have to start organizing and inventorying personal data now if you're going to comply on January 1, 2023.

For example, you maybe have been doing business with someone for 10 years. On January 1, 2023, they can say, "Please give me all the information you have about me."

When they do that, you have to supply everything going back to January 1, 2022. Could you do that? What if they asked you to delete all their data? Could you get rid of everything you have, going back to January 1, 2022?

If not, you'll be in violation of the law. That means you should tag and sort personal data right now (and figure out how to go back to January 1). Otherwise, January 1, 2023 will be a complete mess.

We have a whole article about this, https://www.osano.com/articles/how-to-comply-with-the-california-privacy-rights-act-look-back-provision, if you want to dive deeper into that one.

Blargh. Anything else I should know? What about this vendor-contracting stuff?

Well, you should work to improve your relationships with anyone you share data with — buying, selling, or just a basic vendor relationship.

Because you need to extend consumer rights to all of the vendors you work with, you need to make sure you have a way to get those vendors to delete or correct data in the same way you do.

For example, say you work with mail houses, email fulfillment services, or a host of other third parties where you upload contacts or do data analysis. You'd need to ensure that when you delete or correct a file, it is universally removed throughout, not backed up somewhere, not sold onward, or anything else.

It's important to have contracts with your vendors that define this relationship and what they're allowed to do with the data you supply them. Many large companies will have standard forms for this; young start-ups may not. And some large companies might see you as so small it's not worth their time to contract with you — at which point, it might be time to find another vendor.

And those small vendors may well think the CPRA doesn't cover them because they're so small, but because the CPRA covers you, all of the data you share with them is covered, so the vendors need to do what you tell them to do. If they won't? Again, maybe it's time to find another vendor.

Conclusion

This certainly isn't everything, but as you prepare for January 2023, we hope these questions give you a starting point in your journey to CPRA compliance.

Still not sure where to begin? Let us show you how Osano can help.

To see Osano in action

Schedule a Demo

or visit www.osano.com for more information.