DATAGRAIL

CPRA

The Simple Guide

Untangling How the California Privacy Rights Act Impacts Businesses & Consumers

Introduction

On November 3, 2020, at the culmination of a historic US election in a historic year, data privacy advocates watched closely to see whether California voters would pass Proposition 24.

It did indeed pass, and we're here to help you make sense of the new California Privacy Rights Act (CPRA), ushered in by the passage of Prop 24.

If you're reading this guide, perhaps you already know the basics: the CPRA is an update that expands and amends 2018's California Consumer Privacy Act (CCPA), which just took effect in July 2020. You may also know that around the world, consumers and data privacy advocates are demanding more transparency and control over how companies use personal data, resulting in regulations around the world.

And you probably know that privacy is really hard—it's messy, complicated, and confusing to get right, and navigating regulations like the CPRA is no exception. There are a lot of nuances in the CPRA, and it's easy to get bogged down in the details. In this guide, we'll simplify what you need to know now about the CRPA by sharing our key takeaways, as well as going a bit deeper into its impact on businesses and consumers alike.

CPRA Key Takeaways

IT TAKES EFFECT IN 2023, BUT ORGANIZATIONS SHOULD START PLANNING NOW

The CPRA is the second privacy law passed in California, and will replace the CCPA. It takes effect in January 2023. But the lookback period starts in January 2022—meaning in 2023, consumers can make requests about their personal data collected from the prior year. Additionally, the Attorney General and the new California Privacy Protection Agency (CPPA) will be working on finalizing the CPRA regulations until July 2022.

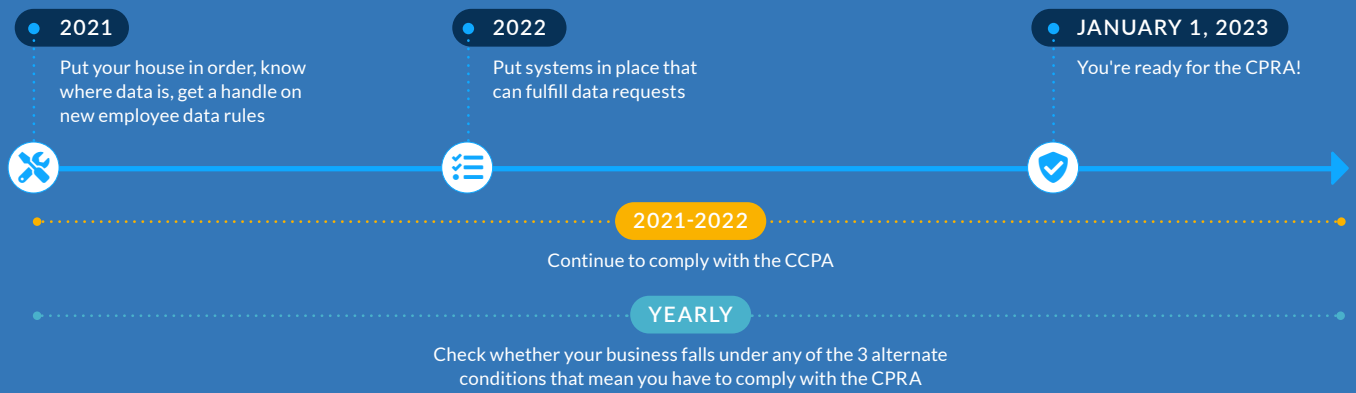
Essentially, companies need to spend 2021 making sure their data privacy compliance programs will be ready to comply with CPRA in whatever its final form will be, as well as continuing to comply with CCPA, which is in effect until then.

> "Companies need to spend 2021 making sure their data privacy compliance programs will be ready to comply with CPRA."

The Road to Privacy: CPRA Key Dates

Timeline for the CPRA

Timeline for businesses



IT DRAWS INSPIRATION FROM THE GDPR

The CPRA aligns more closely with its sister regulation in the EU—GDPR. It includes employees as data subjects and gives consumers more rights, but also clarifies some concepts lacking clarity in the CCPA. It also details specific obligations on service providers and contractors. The creation of the CPPA as an enforcement authority also mirrors the role of the European data processing agreements, which have been essential in interpreting the scope of the GDPR.

CPRA aligns closely with its sister regulation in the EU—GDPR.

IT HAS STRONGER ENFORCEMENT

The CPRA creates a new administrative agency, the Consumer Privacy Protection Agency (also known as CPPA, good luck not getting this acronym confused with the CCPA regulation) to help enforce and regulate privacy for Californians, which could lead to more regulations. Stronger enforcement is also highlighted by higher fines when minors' personal data are involved.

IT HAS STRONGER PROTECTIONS FOR CONSUMERS

For consumers, the CPRA provides stronger protection, giving them the right to further limit the use and disclosure of their information, including precise geolocation.

The CPRA also expands the definition of consent around personal information. The CCPA lets consumers opt out of the sale of their personal information. But even though the definition of a "sale" is rather large under the CCPA, companies could claim they were "sharing" your personal information for a "better experience," not "selling" it. And yet you still might have felt like that one meal kit ad was haunting you across the internet. The CPRA extends "do not sell" to include "do not share" personal info with third parties for "cross-context behavioral advertising, whether or not for monetary or other valuable consideration."

> "The CPRA extends 'do not sell' to 'do not share'."

SIMILAR FEDERAL LEGISLATION IS COMING

The GDPR and the CCPA created momentum for other US states to start crafting their own legislation, and federal data privacy legislation could follow in the coming years. The biggest question will be whether federal legislation will simplify or complicate compliance for businesses across the country. On the one hand, it could streamline compliance by removing onerous nuances between state regulations, but it could also complicate matters by serving as an additional nuance stacked on top of existing state laws. In any case, companies that have privacy programs in place now will ultimately be better positioned to manage future regulations down the road.

State Comprehensive-Privacy Law Comparison

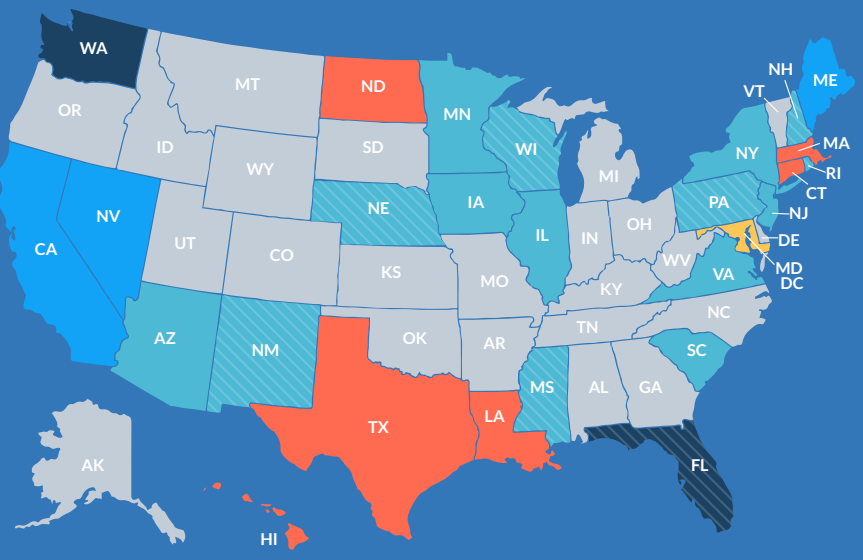
iapp

- Task Force Substituted for Comprehensive Bill
- Bill Died in Committee or Postponed
- None

Statute/Bill in Legislative Process:

- Introduced
- In Committee
- Cross Chamber
- Cross Committee
- Passed
- Signed

Last updated: 10/14/2020



From International Association of Privacy Professionals website

How The CPRA Impacts Consumers

POSITIVE IMPACTS ON CONSUMERS

New rights and definitions (that mirror GDPR)

The CPRA's alignment with GDPR offers consumers more control over their data privacy, including the following.

- Right to access information about automated decision making (for example, knowing why an algorithm shows you a certain kind of ad)
- Right to opt out of automated decision making technology
- Right to data correction
- Right to know the length of data retention
- Clear right to portability (separated from the right to know)
- Clearer definition of consent, with an emphasis on being freely given, specific and informed

Consumers are getting more control to limit the use and disclosure of sensitive information.

Even stronger protection for sensitive info

Consumers are getting more control to limit the use and disclosure of sensitive information. Sensitive information outlined in the text of the law includes but is not limited to: government identification numbers (e.g., Social Security numbers, driver's license numbers, and passport numbers); debit card and credit card numbers in combination with required security or access codes, passwords, or credentials; a consumer's precise geolocation, religious beliefs, racial or ethnic origin, biometric information, sex life or sexual orientation information; and contents of a consumer's mail, email, or text messages unless that business is the intended recipient. This widely aligns with sensitive data as defined in the GDPR. Note that geolocation is specifically mentioned—this aligns with concerns around app tracking, especially in the context of the COVID-19 pandemic.

An agency is born: the California Privacy Protection Agency

As mentioned in the key takeaways section above, the creation of the CPPA is one of the strongest benefits to consumers of CPRA. Right now under the CCPA, investigation, enforcement, and promulgation of data privacy regulations falls under the Office of the Attorney General (OAG). The OAG, unsurprisingly in a state like California, has a lot of competing priorities that result in limited capacity to deal with data privacy infractions. This new body should be able do a better job of protecting consumers, just from its ability to focus solely on data privacy.

Privacy for those who can afford it?

During the lead up to the November election that passed Proposition 24 into law, some privacy advocates campaigned against it. Even the Electronic Frontier Federation (EFF) declined to support it (though they didn't officially oppose it either). Opponents were concerned that for all the merits of the proposed legislation, businesses might pass the costs of increased compliance onto consumers who put in time to opt out of having their data sold or shared.

Jacob Snow, an attorney for the ACLU, told the San Francisco Chronicle, "It doesn't take into the account the burdens on poor communities and communities of color to pay for their privacy and to do the work to protect themselves." While Prop 24 passed, 7.2 million Californians still voted against it—though it remains to be seen if "pay for privacy" becomes the reality.

How the CPRA Impacts Businesses

POSITIVE IMPACTS ON BUSINESSES

Publicly available information doesn't count as personal information

The CPRA's definition of personal information specifically excludes "publicly available" information. Publicly available is defined as "lawfully obtained, truthful information that is a matter of public concern; information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience." While this will likely be clarified by the CPPA, a business could conceivably freely collect your first and last name, or information you share on a public social media profile.

Publicly available information doesn't count as personal information

Clearer and higher thresholds for who needs to comply

The CPRA improves on the CCPA's definition of who is covered under the data regulations. The $25 million revenue threshold is clarified to target the annual gross revenue threshold *in the previous calendar year.* Additionally, while the CCPA applies to companies that have data from at least 50,000 consumers, households, or devices in their databases, the CPRA updates the threshold to 100,000 or more consumers or households.

An agency is born, part two: the California Privacy Protection Agency

In addition to giving consumers a dedicated watchdog on their side, the CPPA will also be a boon for companies. It will help interpret and clarify any obscure or muddy parts of the law, which has been a sore point with CCPA so far.

New obligations on service providers and contractors

CPRA provides clear requirements for "service providers" which will assist businesses (and their controllers) in response to privacy rights requests. This is a big step up from the CCPA, which outlined rather unclear obligations on service providers and pushed controllers to rely on existing data privacy agreements in place with their service providers.

"Contractors" are also now included under the scope of these provisions. For example, service providers and contractors are required to notify businesses when they engage sub-service providers and sub-contractors. Additionally, service providers and contractors are also obligated to help businesses respond to privacy rights requests.

NEGATIVE IMPACTS ON BUSINESSES

Threshold now includes selling or sharing data

For determining whether a business falls under the CPRA, the third threshold has been updated in a way that will mean more businesses will have to comply. Now, companies will have to be compliant if at least 50% of annual revenue comes from selling or *sharing* personal information.

> "Businesses preparing to meet the CPRA requirements should be prepared for less wiggle room, and potentially more and higher fines."

Stricter enforcement

Businesses preparing to meet the CPRA requirements should be prepared for less wiggle room, and potentially more and higher fines. CPRA gives dedicated authority to the CPPA to enforce regulations, so potentially more businesses will be on the hook for violations. Additionally the CPRA removes the 30-day grace period from CCPA to fix or "cure" a violation.

And if a violation involves a minor, the fines are much higher with CPRA, up to $7,500 for violations involving children's personal information.

Employees and vendors as data subjects

The CPRA expands the scope of data privacy protection to employees and vendors, again aligning with the GDPR. While this is positive for employees' privacy, it also means more data in more systems to discover and map out to ensure compliance, given that HR data (anything from payroll information, to 401(k) participation) generally resides in different platforms from customer data. The CCPA exempted employee and certain business-to-business data until January, 2022, and the CPRA does extend that exemption until January 1, 2023, the same day the CPRA goes into effect. The lookback period begins the year prior—by 2023, businesses should be able to comply with employees' data requests pertaining to data from January 1, 2022 onwards.

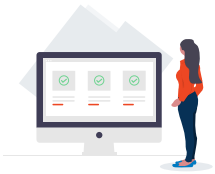
Expanded opt-out scope: "Do not sell or share"

Since consumers can now opt out of third-party sales and sharing for "cross-context behavioral advertising," more businesses (especially those that rely on targeted ads!) will need to determine how the law applies to them, and they'll need even tighter control and insight into their data processes.

Closing

Many companies have already sought to comply with the GDPR or the CCPA, and while that puts them on the right track for the CPRA, it doesn't mean they'll automatically be compliant. They need to ensure their privacy compliance programs are robust and agile enough to comply with any emerging regulation, including the CPRA.

And while more regulations mean more onus on businesses to pursue compliance, it's important to remember *how* we got here-it's because people are demanding transparency and control over how their data is collected and used. The end game is not checking the box on CPRA compliance. The end game is building customer trust. And DataGrail is here to help.



Does CPRA apply to your business?

Take our CPRA quiz

Stay up on the latest in data privacy

Subscribe to Weekly Grail

About DataGrail

DataGrail helps companies comply effortlessly with existing and emerging privacy laws, such as the GDPR, CPRA and CCPA. It was designed from the ground up to automate data discovery and streamline privacy programs to create less work for customers, while also ensuring a higher level of accuracy and reduced risk. DataGrail built its solution to directly integrate with an organization's internal databases and developed 250+ pre-built connectors with companies—such as Salesforce, Shopify, Adobe, AWS, Oracle, Okta, and many others. These connections provide organizations with an accurate, real-time view of the internal systems and third-party applications used and all the personal data that maps onto each of those systems. DataGrail also allows customers to manage their privacy request workflows and email preferences across applications.

To learn more about DataGrail, please visit www.datagrail.io or follow DataGrail on Twitter and LinkedIn

Request a demo