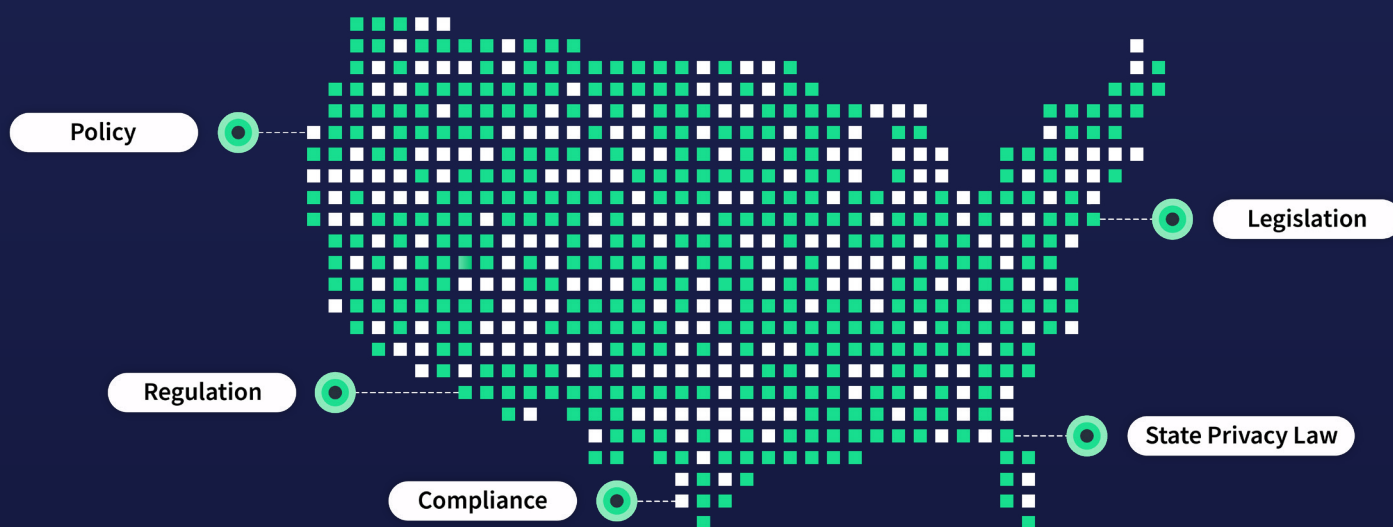


12/16/2022

2023 State Privacy Law Readiness Playbook

How to prepare for CPRA, CDPA,
CPA, CTDPA, & UCPA



Contents

Contents	2
Introduction to 2023's State Privacy Laws	3
State Privacy Law Commonalities	3
California's CPRA	4
Virginia's CDPA	5
Colorado's CPA	6
Connecticut's CTDPA	7
Utah's UCPA	8
What Your Business Needs to Do to Prepare	9
How Ethyca Can Help Your Business Stay Compliant	9

Provision	CPRA	CDPA	CPA	CTDPA	UCPA
Right to data access, deletion, portability	✓	✓	✓	✓	✓
Right to non-discriminatory behavior	✓	✓	✓	✓	✓
Right to opt out of the selling or sharing of personal information	✓	✓	✓	✓	✓
Right to correct consumer data	✓	✓	✓	✓	X
Private Right of action	✓	X	X	X	X
Right to appeal	X	✓	✓	✓	X
Processing of Sensitive Personal Information (SPI)	Opt-out	Opt-in	Opt-in	Opt-in	Opt-out
Universal opt-out mechanism	X	X	✓	✓	X

Disclaimer: This playbook is a general overview of what your business needs to do to prepare for the coming privacy regulations in 2023. It is not meant to be legal advice. We recommend you consult your legal team to review and approve any new privacy and business decisions for your organization.

Introduction to 2023's State Privacy Laws

The United States is gearing up to be a hotbed of privacy legislation in 2023. Five new state privacy laws will go into effect in the new year, including California's CPRA, Virginia's CDPA, Colorado's CPA, Connecticut's CTDPA, and Utah's UCPA.

While these new regulations will facilitate more privacy protections for American consumers across the U.S., what do these new laws mean for your business? How will you be able to stay compliant with each state's different privacy law? And how can Ethyca help?

This playbook will help you answer these questions and provide all of the information you need to get ready for each state's unique provisions in the new year.

State Privacy Law Commonalities

While these new regulations will facilitate more privacy protections for American consumers across the U.S., what do these new laws mean for your business? How will you be able to stay compliant with each state's different privacy law? And how can Ethyca help?

Although each state privacy law has its own provisions and nuances, there are a few commonalities between all five of them.

In each state, residents will have:

- The right to access, delete, and portability of their data.

- The right to non-discriminatory behavior based on exercising data rights.
- The right to opt-out of selling or sharing of personal data.

It's important to note that California is the only state that includes the additional right to opt out of the *sharing* of personal data. In practice, though, its definition of selling and sharing is in line with other states.

Businesses in each state are also obligated to:

- Publish privacy policies on their websites.
- Respond to a consumer's request within 45 days.

Now that you know the commonalities between the state privacy laws, let's go over what's arguably more important – the different provisions each state has.

As you'll see, some state privacy laws are determined by yearly revenue thresholds, while some aren't. Others require universal opt-out signals on business websites, while others don't.

To help you keep track of what's included in each law, this next section will go over each state privacy law in more detail in the order they go into effect.

California's CPRA

California's privacy law is one of the first privacy laws to go into effect on January 1, 2023.

Sometimes referred to as CCPA 2.0, the California Privacy Rights Act (CPRA) amends the California Consumer Privacy Act (CCPA). In this playbook, we'll refer to California's privacy law as CPRA to avoid confusion.

Under the amended law, Californians have an expanded set of privacy rights businesses must adhere to. One of them is the right for consumers to opt out of the selling and sharing of their personal data. This includes behavioral advertising as well.

In addition, Californian consumers have the right to correct their personal data.

Companies also must treat CPRA's new definitions of Sensitive Personal Information (SPI) accordingly.

Starting next year, SPI will be considered personal information that reveals a consumer's:

- Social security number, license number, or state ID number
- Account log-in, password, access code, or other information regarding their account
- Geolocation
- Racial, ethnic, religious, and sexual identity, or philosophical beliefs
- Non-business-related emails, messages, and mail
- Genetic and biometric data.

To manage users' consent choices properly, companies must provide explicit opt-out consent options to to process their sensitive data.

Provision	CCPA	CPRA
Right to access and delete data	✓	✓
Right to data portability and non-discriminatory behavior	✓	✓
Right to opt out of the selling of personal information	✓	✓
Right to correct consumer data	✗	✓
Right to limit use of Sensitive Personal Information (SPI)	✗	✓
Right to opt out of sharing personal information	✗	✓
Enforcement authority	California Office of the Attorney General (OAG)	California Privacy Protection Agency (CPPA)

Virginia's CDPA

The next state privacy law that will go into effect on January 1, 2023 is Virginia's Consumer Data Privacy Act (CDPA or VCDPA).

Although it borrows heavily from California's CCPA (before the CPRA amendments), there are a number of notable differences to keep in mind. One is the right for Virginian consumers to appeal to businesses that have failed to process a privacy request within 45 days.

Additionally, while CPRA identifies three different categories of data recipients, CDPA only has one definition of a data processor. Companies are

required to enter Data Processing Agreements (DPAs) with data processors, who are defined as **“a natural or legal entity that processes personal data on behalf of a controller.”**

Under CDPA, Companies must also produce Data Protection Impact Assessments (DPIAs) that examine the privacy benefits and risks of processing activities on the business itself, consumers, and other related stakeholders. This provision means your business needs to know not only where data lies in its systems, but also how and why it's there.

Keeping track of the data flows throughout your system will help your business ensure that it's collecting and processing data in ways that respect Virginia's rights.

Provision	CPRA	CDPA
Right to access and delete data	✓	✓
Right to data portability and non-discriminatory behavior	✓	✓
Right to opt out of the selling of personal information	✓	✓
Right to correct consumer data	✓	✓
Right to limit use of Sensitive Personal Information (SPI)	✓	✗
Right to opt out of <i>sharing</i> personal information	✓	✗
Right to appeal	✗	✓

Colorado's CPA

The summer will introduce another pair of privacy laws going into effect on July 1, 2023, starting with the Colorado Privacy Act (CPA).

Under CPA, businesses will have one year to set up Universal Opt-Out Mechanism on their websites, CPA requires Universal Opt-Out Mechanisms to be constructed in a way that **“clearly communicates a consumer’s affirmative, freely given, and unambiguous choice to opt out of the processing of personal data for purposes of target advertising or the sale of personal data.”**

Although the specific details have not been finalized yet, businesses must provide Universal Opt-Out Mechanisms by July 1, 2024.

Additionally, CPA employs a hybrid-consent model. This means that for specific types of personal data, like SPI, consumers will need to give explicit opt-in consent. Other personal data categories, however, require opt-out consent. It can be challenging for businesses to keep track of different consent requirements for users, let alone manage their consent preferences. We'll go over how Ethyca can help you manage such a vast range of user consent preferences in more detail later on in this playbook.

Provision	CPRA	CDPA	CPA
Right to access and delete data	✓	✓	✓
Right to data portability and non-discriminatory behavior	✓	✓	✓
Right to opt out of the selling of personal information	✓	✓	✓
Right to correct consumer data	✓	✓	✓
Right to limit use of Sensitive Personal Information (SPI)	✓	✓	✓
Right to opt out of <i>sharing</i> personal information	✓	✗	✗
Private Right of action	✓	✗	✗
Right to appeal	✗	✓	✓
Universal opt-out mechanism	✗	✗	✓

Connecticut's CTDPA

The Connecticut Data Privacy Act is the other privacy law that will go into effect on July 1, 2023.

Along with CPA, CTDPA will require businesses to add universal opt-out signals on their websites. The law states that users should be able to manage their opt-out preferences through a company-provided **“platform, technology, or mechanism.”** By January 1, 2025, businesses must state this in their privacy policies, as well as provide the opt-out mechanism on their websites.

Additionally, Connecticut will have multi-state enforcement with California and Colorado. Known together as the 3Cs, these states will have joint enforcement with each other, or “multi-state enforcement actions against entities that violate

comparable provisions of the three laws.” This means Connecticut will be able to participate in cross-state investigations and enforcements for privacy violations.

One of the main reasons for this is Connecticut’s limit on cure periods. Other state privacy laws, like Virginia’s CDPA allow companies 30 days to rectify any privacy violations after being notified by the enforcement authority. Connecticut will have an expiration date to its cure periods. The cure period will last only between July 1, 2023, to December 31, 2024. After that, the Connecticut Office of the Attorney General will decide how to proceed with violations.

Lawmakers set this provision in the hopes that companies will swiftly make their data privacy practices fully compliant with CTDPA by 2025.

Provision	CPRA	CDPA	CPA	CTDPA
Right to access and delete data	✓	✓	✓	✓
Right to data portability and non-discriminatory behavior	✓	✓	✓	✓
Right to opt out of the selling of personal information	✓	✓	✓	✓
Right to correct consumer data	✓	✓	✓	✓
Right to opt out of <i>sharing</i> personal information	✓	✗	✗	✗
Private Right of action	✓	✗	✗	✗
Right to appeal	✗	✓	✓	✓
Processing of Sensitive Personal Information (SPI)	Opt-out	Opt-in	Opt-in	Opt-in
Universal opt-out mechanism	✗	✗	✓	✓

Utah's UCPA

The last state privacy law that will go into effect next year is the Utah Consumer Privacy Act (UCPA) on December 31, 2023.

Arguably a more business-friendly comprehensive data privacy framework, UCPA has a number of differences with California, Virginia, Colorado, and Connecticut.

First, UCPA has a high revenue threshold that determines which businesses are subject to the

law. UCPA does not apply to businesses making less than \$25 million in revenue per year. This condition means that most small businesses will be exempt from Utah's privacy law.

Another big difference between UCPA and other state privacy laws is that users cannot opt out of **profiling** based on their data, whereas the other state laws include opt-out rights for targeted advertising and profiling together.

Furthermore, UCPA does not require explicit consent to process or collect SPI.

Provision	CPRA	CDPA	CPA	CTDPA	UCPA
Right to data access, deletion, portability	✓	✓	✓	✓	✓
Right to non-discriminatory behavior	✓	✓	✓	✓	✓
Right to opt out of the selling or sharing of personal information	✓	✓	✓	✓	✓
Right to correct consumer data	✓	✓	✓	✓	✗
Private Right of action	✓	✗	✗	✗	✗
Right to appeal	✗	✓	✓	✓	✗
Processing of Sensitive Personal Information (SPI)	Opt-out	Opt-in	Opt-in	Opt-in	Opt-out
Universal opt-out mechanism	✗	✗	✓	✓	✗

UCPA may be the last privacy law taking effect in 2023, but it's never too late to start preparing your business for compliance. This next section will show you what your business needs to do to prepare for the upcoming privacy regulations, and how Ethyca can help.

What Your Business Needs to Do to Prepare

It may seem daunting to start figuring out how to comply with so many different state privacy laws. That's why Ethyca has prepared this readiness plan. We'll show you how you can stay compliant with our services no matter what state you do business in. Here's what you can look forward to before the new regulations start on January 1, 2023,

New Consent Setup

During December 2022, we'll release feature updates that will help your business comply with new regulations. This includes changes to your consent configuration.

Training and Documentation

Ethyca will provide training documentation and an on-demand video to help you set up your new consent preferences. The training will take approximately 1 hour.

Setup and Configuration

For most customers, we expect configuration for California (CPRA), Virginia (CPDA), and Colorado (CPA) to take 4 - 8 hours of time.

Non-Ethyca Changes

In order to continue complying, you will need to make changes to your privacy policy. Consult your legal team to ensure your policy changes adhere to the new state privacy laws.

How Ethyca Can Help Your Business Stay Compliant

Ethyca will update its consent UX to provide an easier user experience to help your business adapt to the new consent requirements in each state.

First, we'll include an on-site footer update. Your business will be able to update its website footer to include one or multiple opt-out links. This will help fulfill California's "do not sell and share my personal information" consent requirement. Keep in mind that the official consent language is still being finalized state by state.

Second, we'll incorporate a user identity check via email or SMS into the Privacy Center. This will help confirm the user's identification if they want to edit their consent preferences.

Lastly, you'll be able to set single or multiple categories of opt-out consent. This will help your business adapt to hybrid-consent models like in Colorado's CPA.

We've also provided two ways for your business to set up opt-in SPI. You can either set it up in your Privacy Center, or set consent from your site via API.

If you have any more questions about the upcoming state privacy laws and how Ethyca can help, feel free to reference our [State Privacy Law Hub](#). Here, we go over more detail about each state's privacy laws, so you can get a better understanding of the new regulations in 2023.



License Apache 2

License CC BY 4.0

Developer tools for privacy.

Join the Fides community.
Let's fix trust in tech together.

ethyca.com/fides