CPRA Compliance

How Osano Can Help

TABLE OF CONTENTS

Introduction

Pop quiz: How many times does the word “privacy” appear in the US constitution?

Zero.

Though many of its amendments evoke the concept of privacy and have been interpreted to provide for certain privacy rights, a literal and fundamental right to privacy does not exist in the text of the US constitution. Today in the US, that means citizens’ privacy rights are mostly a matter left up to the states.

California took an early lead in ensuring its citizens have a right to privacy. In 1972, the state amended its constitution to include a fundamental right to privacy. In 2004, it became the first state to require businesses to include a privacy policy on their website. And, of course, in 2018, it enacted the California Consumer Privacy Act (CCPA), soon to be amended by the California Privacy Rights Act (CPRA).

The CPRA isn’t the only privacy law in the US, but it does cover the citizens of the US’s most populous state, has served as a model for other state privacy laws, and will likely have a significant influence on an eventual federal privacy law.

Businesses that want to serve California residents and/or be prepared for the future of privacy in the US must become compliant with the CPRA.

Helping businesses comply with data privacy laws and develop a more privacy-conscious relationship with their customers is what we do at Osano.

Naturally, we’ve spent a lot of time determining the most impactful ways that we can help businesses become compliant with the CPRA. In this white paper, we’ll cover the most significant compliance needs created by the CPRA, walk through the biggest challenges businesses face when trying to meet those needs, and discuss how we can help make it easier.

Who Is Subject to the CPRA, and What Are Its Main Requirements?

It'll come as no surprise that within the law's ~19,000 words, there are a slew of requirements that businesses must adhere to.

First, it's important to understand which businesses are subject to the CPRA. For-profit organizations that do business in California are subject to the CPRA if they meet one of the following:

- Earned $25 million in gross revenue the previous calendar year.
- Processes the data of more than 100,000 California consumers.
- Earns more than 50% of revenue from the sale or share of personal information.

Clearly, that encompasses many businesses, from the very small to major enterprises.

While many businesses are subject to the CPRA's requirements, and while there are many individual requirements, businesses can become mostly compliant by focusing their efforts on just a few activities.

Namely:

- Cookie consent and consent management
- Data subject access rights (DSARs)
- Compliant partnerships with vendors

Let's focus on each of these activities, examine how they connect to CPRA compliance, and discuss how Osano can help.

While many businesses are subject to the CPRA's requirements, and while there are many individual requirements, businesses can become mostly compliant by focusing their efforts on just a few activities.
Namely:

- Cookie consent and consent management
- Data subject access rights (DSARs)
- Compliant partnerships with vendors

Let's focus on each of these activities, examine how they connect to CPRA compliance, and discuss how Osano can help.

Cookie Consent and Consent Management

For the unfamiliar, cookies are small text files that websites drop onto their visitors' browsers. These text files store data related to the users' behavior, actions, and personal information. Because they're stored on a user's browser, that information can be read later by that same website or another website.

As an example, users that click to add a product to their cart on an ecommerce website receive a cookie recording that click. That way, the website can remember and load up the relevant product when the user checks out their cart.

Or, if a user clicks on that same product, but doesn't add it to their cart and instead navigates away from the website, the cookie might be read by other websites participating in an advertising network.

Then, the user will receive targeted advertisements showing off the product they had displayed interest in, or a similar product.

Websites drop, on average, about 20 different cookies for a wide variety of purposes. They might:

- track user behavior for personalized advertising
- remember login info and user preferences
- track website usage
- collect analytics data
- and more

Some of these purposes can be pretty innocuous while others can feel like an invasion of privacy. If, for example, a healthcare organization shared data on your condition with a social media network advertising system, you would be pretty upset. As it turns out, this really happened, and similar examples of businesses being a little too liberal with their customers' data take place every day.

How Do Cookies Relate to the CPRA?

There are a few elements of the CPRA that limit how businesses can use cookies.

Personal Information and Sensitive Personal Information

Certain types of cookies could fall under the CPRA's definition of personal information, which it defines as information that "identifies, relates to, describes [...] or could reasonably be linked, directly or indirectly, with a particular consumer or household."

Among examples of what constitutes personal information, the CPRA includes:

Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.

Since cookies are primarily used to track information related to a consumer's interaction with websites, they fall under the CPRA's definition of personal information.

Furthermore, the CPRA provides a second category of personal information: Sensitive personal information. This includes info like social security numbers, genetic data, precise geolocation, ethnicity, and more.

If you collect this information (whether through cookies or any other means), then you'll have to treat it in certain ways — more on that below.

Cross-Context Behavioral Advertising

The law also explicitly calls out "cross-context behavioral advertising," or targeted advertising. For the most part, targeted advertisements rely on third-party cookies that are stored in the consumer's browser. When the consumer visits a website that displays advertisements, the ad network checks the browser for any cookies related to brands participating in its network.

If somebody recently visited a participating brand's website, that brand would drop a cookie on the visitor's browser, which would then be recognized by the advertising network on a future website. When the advertising network displays the participating brand's advertisement, that's considered personalized, targeted, or "cross-context behavioral" advertising.

Profiling and Automated Decision-Making

Lastly, cookies can be used to collect information for the purposes of what the CPRA calls, “automated decision-making,” which includes profiling. It defines profiling as:

> any form of automated processing of personal information [...] to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

When combined, the data collected by different cookies can build a profile of a consumer, which is another way in which cookies may be subject to the CPRA.

How You Have to Treat Cookies Under the CPRA

If a cookie can be construed as tracking users’ personal information, informing targeted advertisements, or contributing to a consumer profile, then you need to provide a way for users to opt-out.

Unlike other data privacy laws like the GDPR, the CPRA does not require you to show a “cookie” banner per se, nor does it require you to ask for your user's permission before dropping cookies on their website.

However, you are required to inform users that you will be using cookies and collecting their personal information first. Additionally, you have to provide users with a means of:

- Opting out of the sale or share of personal information (such as for targeted advertising)
- Opting out of the use of personal information in automated decision-making, including profiling
- Limiting the sale and disclosure of sensitive personal information (i.e., to limit the use of sensitive information to only what is necessary for the business to provide its goods and services to the consumer)

The CPRA only requires that these notices and opt-out mechanisms are prominently displayed. A cookie banner is a convenient way to do that.

How Osano Helps With Cookie Consent

If you're going to run a website for your business, then you're going to have to collect information that's regulated under the CPRA in one way or another. Your challenge, then, is fivefold:

- Disclosing to visitors that you collect personal information (and potentially sensitive personal information)
- Providing visitors a mechanism for withdrawing their consent for your collection of certain types of information
- Categorizing cookies based on whether they're essential for your website to function or if they collect personal information
- Acting on that consent preference to permit or block cookies based on their categories
- Remembering a visitor's data collection consent preferences for future visits

Doing this with a homegrown solution represents a significant investment of time and effort. Third-party solutions may represent less work, but they can also involve significant integration and maintenance work before you achieve compliance.

Osano's Consent Management solution meets all of the above challenges and does so without requiring significant implementation work.

New Osano customers just have to paste a single line of JavaScript into their website's HTML header.

Osano discovers new scripts and cookies on a website domain within a few minutes to a few hours — then, it automatically recommends classifications for those scripts and cookies in a way that makes them actionable for compliance with the world's data privacy laws (including CPRA).

Afterward, Osano displays a popup informing users about your data collection practices and their rights in a compliant way. That includes providing mechanisms to opt out of the sale or share of personal information, to opt-out of automated decision-making, and to limit the use or sale of sensitive personal information. If a user chooses to withdraw consent, Osano blocks those cookies and scripts classified as collecting personal information.

We also store users' consent data in a blockchain, so you can prove you've been compliant should the need arise.

Another unique feature of the CPRA compared to other state laws is: It's the only law that creates a data protection authority. Like other data protection authorities, cookies will likely be among the first things the California Privacy Protection Agency (CPPA) looks at when determining whether a business is compliant. Osano ensures both compliance and proof of compliance.

DSAR Workflow Automation

DSARs, also known as data subject access rights or subject rights requests, have been a mainstay of global data privacy laws. However, the CPRA is one of the first laws to really bring DSARs into focus in the US. As more consumers, employees, and businesses become aware of DSARs, they'll become more of a challenge to handle.

The term "DSAR" doesn't actually appear in the text of the CPRA, but whenever the CPRA refers to a consumer's rights, it's usually referring to DSARs. They're a set of rights that the CPRA grants consumers and requires businesses to respond to.

DSARs, also known as data subject access rights or subject rights requests, have been a mainstay of global data privacy laws. However, the CPRA is one of the first laws to really bring DSARs into focus in the US. As more consumers, employees, and businesses become aware of DSARs, they'll become more of a challenge to handle.

The term "DSAR" doesn't actually appear in the text of the CPRA, but whenever the CPRA refers to a consumer's rights, it's usually referring to DSARs. They're a set of rights that the CPRA grants consumers and requires businesses to respond to.
Under the CPRA, consumers have the right to:

- Know about what personal information the business collected and uses
- Access that information
- Request that the business delete their personal data
- Correct inaccurate information
- Limit the use and disclosure of sensitive personal information (as described above)
- Opt out of the sale or sharing of their personal information (such as sharing with advertising networks)
- Not have their personal data sold or shared without their explicit opt-in consent if the consumer is a child under 16

- Not to be discriminated or retaliated against when exercising these rights

It's clear there's a lot of onus on the business to not violate these consumer rights. How, for instance, can you be sure a consumer isn't a child under 16? What counts as discriminating against somebody exercising their rights? Do you really have to hand over all of a consumer's data if they ask? What if you don't know where all that data lives?

Adding to this complication is the fact that the CPRA defines "consumer" rather broadly, and therefore extends these rights to more classes of individuals than other state privacy laws. Specifically, other laws exclude the personal information of employees from their regulation. The CPRA, however, extends data rights to any "consumer," which it defines as any California resident — including employees, former employees, job applicants, and so on.

Looking at other jurisdictions where employee DSARs are in play (i.e., the EU), we can anticipate that many DSAR requests will come from employees and that the intricacies of employee data will be a particularly complex issue for businesses.

Pitfalls to Avoid in Executing DSAR Requests

Businesses that haven't had to deal with many DSARs before tend to fall into a trap; they rely on emails and spreadsheets to receive, manage, and execute DSAR requests.

When they're receiving one DSAR request every few months, this can be a sustainable practice. But as that volume grows, the manual approach causes issues:

- Handling DSARs creates yet more consumer data in different systems (emails, cloud storage, etc.) that need to be tracked and managed in the future
- Manually going through each data store where a given individual's data might be located (e.g., customer relationship management software, sales software, enterprise resource platforms, etc.) is tedious and needs to be repeated on a per-DSAR basis
- It's easy to miss a data store or an instance of consumer data

Gartner research shows that this manual approach costs businesses $1,400 to respond to a DSAR request. Note that this figure excludes the financial penalties associated with noncompliance should a consumer file a complaint with a data protection authority.

The same research indicates that the majority of businesses struggle to execute a DSAR request within two weeks. Given that businesses must complete a DSAR request within 45 days, it's easy to see how handling large volumes of DSAR requests in a manual way could very quickly put a business out of compliance.

How Osano Helps With DSARs

Responding to DSAR requests, tracking down user data, and executing the request in a manual way is prohibitively time-consuming. But at the same time, fully automated approaches run the risk of delivering inaccurate results to DSAR requests — if a fully automated DSAR process delivers privileged information or exposes another user's data, it can become an easy target for compliance complaints.

Thus, the best approach is a hybrid one.

Osano's Subject Rights Management and Data Discovery tools automate the workflow of responding to a DSAR request while keeping the human in the loop, balancing the accuracy of a human with the speed of a machine.

With Osano's Subject Rights Management and Data Discovery tools, businesses follow three basic steps when processing DSARs:

1. Identify Where Your Data Lives

As a foundational step, Osano users can add the various data stores in use across the organization to the platform. We have over 100 pre-built integrations, enabling you to quickly add commonly used applications like Stripe or ADP into the Osano platform. Once added, Osano will identify the various data fields used in the application and the various actions to take in association with a DSAR request, like delete, update, summarize, and so on.

Osano allows you to assign owners to each data store so that they can be assigned to complete DSAR tasks later on in the process. And if you have a niche or in-house application that isn't included in our integrations, it's easy to build custom data stores within Osano.

2. **Securely Communicate With Data Subjects**

Osano provides one-click codes that allow you to embed a DSAR request form, which you can style to your brand. These forms allow data subjects to self-identify as employees or consumers, submit identity verification like driver's licenses, send and receive files, and select a request type as afforded to them by the CPRA (or any other data privacy regulation). After a data subject submits a request, you can securely communicate with them through the Osano platform.

3. **Automate Action Items**

After receiving and verifying a DSAR request, Osano's Data Discovery tool automatically searches your data stores for fields that correspond to the given data subject. Then, Osano sends recommended actions for each data field to the assigned data store owner. They can update the action item status to indicate their progress in completing a task. Data store owners can send data to the administrator, who can then send it onto the data subject if they requested access.

As an example, say an employee requested a summary of all payroll data you have on them. They would access your website's DSAR form, upload identification information, and make their request. That request would make its way to the Osano administrator.

Since they've already added the integrated Rippling application, they simply verify the data subject's identity and let Osano search for data fields associated with that data subject.

Then, they pass the data fields and recommended actions to the owner of the Rippling application (likely an HR professional).

The data store owner receives the request, exports the relevant data from Rippling, and sends it back to the administrator, who in turn sends it to the verified data subject.

Compliant Partnerships With Vendors

Many data privacy regulations hold businesses liable for the data privacy violations of their vendors, service providers, contractors, and other third parties. You could do everything right, but if your payment processor retains your customers' data and uses it for targeted advertising, you'll be just as liable to noncompliance fines as they are.

Fortunately, the CPRA isn't one of those data privacy regulations. The CPRA does require that you have an agreement with a third party, service provider, or contractor indicating that they'll exercise the same level of protection for your consumers' data as you do. So long as that's in place, the CPRA states:

> A business that discloses personal information to a service provider or contractor in compliance with this title shall not be liable under this title if the service provider or contractor receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider or contractor intends to commit such a violation.

So, the CPRA exposes your organization to less risk than, say, the GDPR does in regard to your vendor relationships. But that doesn't mean you shouldn't factor in your third parties' privacy practices when selecting vendors or commercial partners.

Consider the following:

1. Healthy data privacy practices are inherently good.
2. Businesses with better data privacy practices are less likely to suffer data breaches (and thereby disrupt your business, expose your consumers' data and damage your brand, and so on).
3. The CPRA requires you to collaborate with your vendors for certain data privacy tasks, like executing DSAR requests for data that spans organizations. That'll be easier to do when your partner understands their data privacy requirements.
4. Even though the CPRA exposes you to less downstream risk doesn't mean you're exposed to zero downstream risk. It could be argued, for instance, that your organization had knowledge or reason to believe your partner wouldn't faithfully adhere to their contractual obligations.

How Osano Helps With Vendor Monitoring

Businesses that face a high regulatory burden often have full-time privacy professionals on their payroll. One of the most critical and time-consuming parts of their job is vendor onboarding.

You can do quite a lot at your own organization to improve data privacy practices, but your ability to control and influence outside parties is limited. Thus, they are a major source of risk, and privacy-minded organizations need to spend time vetting them and being selective about who they work with and who they don't.

Cognizant of this need, Osano developed our Vendor Risk Monitoring solution. It's a regularly updated database of over 14,000 vendors, including companies like Slack, Amazon, and Mailchimp.

Each vendor receives a rating based on our three-step risk calculation process:

1. Osano privacy attorneys, assisted by machine learning technology, review a vendor's privacy policies and compliance documents according to a proprietary, objective ontology based on 163 distinct factors.
2. Based on the results of the attorneys' survey, Osano calculates a risk score in each important area of privacy practices relative to all other companies in the database. The score is recalculated each night.
3. Every night, Osano's search spider crawls companies' public compliance documents. If the company changes its practices, our spider identifies the change and determines whether the change is substantial, which prompts our attorneys to re-review the company.

Using Osano's Vendor Monitoring solution, businesses that want to minimize their noncompliance risk gain a means of vetting their third parties' privacy practices without having to hire a full-time privacy professional. For businesses that do have privacy professionals on the payroll, those professionals gain more time to focus on more proactive privacy initiatives and scale their vendor onboarding.

Streamlined Compliance Through Data Mapping

Like most data privacy regulations, the CPRA does not directly require you to map your organization's data. However, if you knowingly refuse to map where, how, and why your organization processes personal information, then any violations that take place associated with unmapped (and therefore unknown) personal information under your control could be construed as negligence.

If you don't map your organization's personal data processing activities, it will be significantly more difficult to:

- Respond to consumers' subject rights requests for a summary of their personal information under your control.
- Delete a consumer's personal information upon request.
- Know which service providers, third parties, and contractors are handling personal information, and therefore which contracts require data processing addenda.
- Ensure that you're processing the minimum amount of data necessary—and are therefore taking on the minimum amount of risk.

How Osano Helps With Data Mapping

Osano Data Mapping enables you to know your data, inside and out. Use it to:

- Automatically discover systems and classify data via your Single Sign-On (SSO) provider and our library of pre-built integrations.
- Integrate proprietary or niche systems with Osano's RESTful APIs.
- Identify high-risk, high-priority data stores by analyzing them based on a variety of criteria, such as their likelihood of storing PI, the vendors they export data to, and other factors.
- Visualize your data map and data flows to understand the relationships between data stores, as well as to drill down for greater detail or to zoom out to see the big picture.
- Streamline workflows and collaboration for any unavoidable manual processes at your organization.

Simplify Compliance and Meet Your Needs

Even though they're all subject to the CPRA, California-based businesses all have drastically different compliance needs. After all, no two businesses are alike; their data privacy programs shouldn't be either.

Without support, compliance is a complicated and multifaceted process. And it is very much a process, too — privacy programs need to be maintained, laws change and require commensurate changes from businesses, new data is collected and stored, new data sources are created, and so on.

Schedule a Demo

Build the foundation of your organization's compliance processes with Osano.

Schedule a Demo

osano

@osano

linkedin.com/company/osano

http://facebook.com/osanoatx

osano.com

About Osano

Osano is a complete data privacy platform trusted by thousands of organizations around the world. Its platform simplifies compliance for complex data privacy laws such as GDPR, CCPS, LGPD, and more. Features include consent management, subject rights management, data discovery, and vendor risk monitoring. Osano is the most popular cookie compliance solution in the world, used on over 900,000 website to capture consent for more than 2.5 billion monthly visitors.