Breaking News: California Can Immediately Enforce CCPA Regulations – Your 7-Step Plan for Data Privacy Compliance

Insights
2.12.24

A California appeals court just pressed fast-forward and ruled that the state can **immediately** begin enforcing new regulations governing the state's cornerstone data privacy law instead of waiting until late next month. This February 9 decision means that you need to get your house in order when it comes to California Consumer Privacy Act (CCPA) compliance before prying eyes and website trolls take advantage of this confusion and take aim at your organization. This Insight will catch you up on the seemingly never-ending drama and provide a clear seven-step plan you should begin implementing today.

Quick Background

- New CCPA regulations took effect in March 2023, but regulators built in a grace period to actually start enforcing them until July 1, 2023.
- On the eve of that date, a California court delayed enforcement of those regulations and concluded they could not be enforced until March 29, 2024.
- The California Privacy Protection Agency and the California Attorney General appealed the decision. Last Friday, an appellate court determined that the Agency and the AG in fact have authority to **immediately** enforce the regulations and don't have to wait until late next month to begin enforcement.
- It is unknown whether this decision will be appealed to the California Supreme Court. Employers and businesses, however, cannot risk waiting to see whether the regulations will once again be delayed and need to finalize their preparations **today**. **[Editor's Note: The California Chamber of Commerce filed a request with the California Supreme Court on February 20 to overturn this decision, which you can read here. We will monitor this appeal and provide an update should your obligations change – but you should continue your compliance work in the meantime.]**

Your 7-Step Compliance Plan

Now, covered businesses must press rewind to March 29, 2023 and implement the necessary changes required by the now-enforceable CCPA regulations. Here are the next *immediate* seven steps that your business should take.

1. ***Do Not Ignore CCPA Requirements Already in Effect***

While you may feel the need to scramble to comply with these new regulations, do not forget that there are already portions of the CCPA that have been in effect since January 1, 2020. Focus on ensuring compliance with *all* CCPA requirements, and do not overlook any aspect of your global privacy needs (compliant notices, privacy policies, opt-outs, contractual obligations, etc.) to focus all your attention on the new regulations.

While the Agency may now enforce those new regulations, it does not mean that it will ignore other aspects of the CCPA – and neither should you.

2. *Audit The Contracts You Currently Have in Place and Update them to Comply with all of the CCPA*

It is always good practice to continually review the terms of any agreements you have in place with your service providers, vendors, subcontractors, and other third parties that process, store, or access any of your employee or consumer data. The CCPA regulations require, among other things, that covered businesses include in their contracts with vendors and third parties certain contractual terms depending on the relationship and how the data is being used.

Some vendors may claim they are exempt if the data they process or receive is entirely for a purpose that is regulated by HIPAA, GLBA, FCRA, or other laws that are identified in the CCPA. (And, to be clear, those exemptions do exist to the extent those vendors are only processing data for exempt purposes.) Some vendors may have proactively added CCPA terms to your contracts. But the obligation remains yours. Have you confirmed that you have all the CCPA required terms in all your contracts that are subject to the CCPA?

3. *Update Notices Need to be Provided to Job Applicants, New, and Current Employees*

Another low-hanging-fruit step to comply with the CCPA regulations is to ensure you have updated notices for employees and job applicants.

- The new regulations include requirements that businesses provide notices that list each category of personal information and sensitive information collected, the purpose for each category, any category that is sold or shared, the retention period for each category of personal information (unless it is literally impossible for you to determine at the time you collect the data how long you will keep it), and how a consumer can exercise their CCPA rights.
- These notices must be simple and easy to understand with minimal to no "legalese."
- Further, businesses must provide the notice in many contexts, including online, through mobile apps, at physical locations, and even over the phone.

Given this all-encompassing approach to the notice requirement, businesses must be especially wary when collecting information regarding employees or potential job applicants and providing the requisite notice. Of course, personal information will always be collected in an employment

relationship, and a covered business must make sure that it provides notice not only to its customers, but also its employees that interact with its customers, or any other aspect of the business.

Among the new content requirements for the notice at collection is to state how long you will retain each category of personal information, meaning there has to be a defined retention period for every category of data you collect. Simply stating that you will keep all data "as required by applicable law," "for as long as needed for the purposes for which the data was collected," or any other generic phrase is insufficient. The only exception is if it is literally impossible to determine at the point of collection how long you will need to retain the data, in which case the notice must describe the criteria that will be used to later determine how long you will retain the data.

Have you updated your CCPA notices to define the retention period for each category of data? If your website privacy policy is doubling up as both the "notice at collection" and the "privacy policy" (which the regulations permit if the interaction is primarily online, or for in-person interactions you utilize a poster or sign with the URL address or QR code to the website privacy policy), have you updated your policy to include the retention period for each category of data listed in the policy?

To put things in perspective, if you have not updated your CCPA notices since 2022 or earlier, the update to comply with the 2023 CCPA regulations may almost double the length of your notice. There is just a lot more to cover. This is usually a full re-write, not a simple edit.

Bottom line – if you have not updated your CCPA notices since 2022 or earlier, or if you have never provided CCPA notices, you must act quickly to implement new CCPA notices.

4. *Update Your Privacy Policies*

Even for businesses that have already complied with the most recent CCPA regulations – and, if you have not, there are updates that you should make – the regulations require an annual refresh. Because privacy policies must specifically state their last updated date, it is only a matter of looking at the policy to tell whether it has been updated within the last 12 months.

Even aside from spotting the last updated date of the policy, there can be tell-tale signs that privacy policies have not been updated for the 2023 CCPA regulations. For example, does your website privacy only address the collection of data online through the website? If yes, then it is definitely not compliant with the CCPA regulations, as your website policy must address collection of data through any source, whether online, offline, in-person, through phone calls, by mail, etc., as well as indirect collection of data where you obtain data about consumers through vendors and third parties instead of directly from the consumer.

Additionally, does your privacy policy address employees, job applicants, independent contractors, and individuals you interact with in the business-to-business context (all consumers who were partially or completely exempt from the CCPA prior to 2023, and who did not have to be addressed in

the privacy policy before 2023)? Does your privacy policy address the new consumer rights under the CCPA that became part of the law in 2023 – that is, the right to correct inaccurate personal information, the right to limit the use or disclose of sensitive personal information (if applicable), and the right to opt-out of sharing of personal information with third parties for targeted ad purposes (if applicable)?

If you have looked at your privacy policy, and it is more than a year old – or you cannot answer the above questions in the affirmative – it is time for an update.

5. *Confirm that Your Website's Cookie Banner and Cookie Management Tool Are Compliant*

Your website most likely collects personal information about website visitors. You may not think it is personal information, but it is – even if it is just an analytics tool counting unique visitors. You may not be able to trace the individual visitor yourself from just their IP address or other electronic fingerprint your website collects automatically, but the CCPA still considers this information to be personal information even if you do not yourself have the tools to use the information to identify and track the individual visitors.

- If you have any cookie, pixel, beacon, or tag from a third party on your website, that means you are allowing that third party to collect personal information about your website visitors on your website. If that is the case, the CCPA would require you to have a robust cookie management tool to give users the ability to opt-out of unnecessary cookies and opt-out of the sharing of their data with third parties.
- But, the first step is figuring out what is going on with your website – and what cookies, pixel, beacons, or other tracking tools are on it. That means someone with the right expertise should look under the hood.
- Among the new requirements of the CCPA regulations is that the cookie banner provide consumers with choices that are symmetrical, meaning if you have an "Accept" or "Ok" button, you must also have a "Reject" button. A cookie banner that simply says "we're collecting data and you have no choice other than to leave the website" may run afoul of CCPA regulations.
- Likewise, your cookie banner should not simply have an "X" button for consumers to close out of the banner or make it go away, as it will not be clear that clicking the X or exit button effectuates consent to your use of cookies. Consumers may think the X button is for rejecting cookies, the opposite of consent.
- Does your cookie banner have the right buttons and links? Is your cookie banner set up in a way that prevents collection of data through cookies and the disclosure of any data to third parties until the user clicks on a consent button? Not that this is required for every business, but it may be required. If you don't know the answer to these questions, that means you need expert help immediately.

In addition to the cookie banner, it is critically important that your website – if it is selling or sharing personal information, as those terms are defined in the CCPA – honor Global Privacy Controls (GPCs). This has been a must-have since before the CCPA regulations have gone into effect, but it is worth reiterating again.

You may be thinking, "But we don't sell or share date for targeted ad purposes." If your website has any third-party cookies, pixels, beacons, or tags that result in any data being disclosed to or collected directly by the third party on your website, and you have not entered into a service provider contract with the third party that contains at least the 10 contract terms required by the new CCPA regulations, then you are probably selling or sharing data with third parties.

Policies and notices that comply with the CCPA are of course a requirement, but – except for businesses with no websites or extremely basic websites – it will be hard to comply without working out the nuts and bolts of how your website works.

6. *Ensure Your Process for Receiving and Enforcing CCPA Rights' Requests Comply*

The new regulations provide significant overhaul of the requirements for processing rights under the CCPA. Have you implemented at least two methods for receiving CCPA requests? Have you tested out your process to confirm it works? Have you confirmed your consumer request management process can handle the new CCPA rights? If you have not updated your CCPA process to take into account the new regulations, now is the time.

7. *Evaluate Your Practices – and Especially Your Website – for Dark Patterns*

One key issue in the new CCPA regulations is what are called "dark patterns." A dark pattern is a design that effects to substantially subvert or impair user autonomy, decisionmaking, or choice. To fall afoul of being a dark pattern, you need not trick or mislead consumers – practices which are thought to make it even marginally harder for a consumer to exercise privacy rights or which are meant to prod consumers in a particular direction can be in the crosshairs.

The regulations flesh out five principles that need to be following to not have a dark pattern – easy to understand, symmetry in choice, not confusing, straightforward choice architecture, and easy to execute. These principles come with examples of things that are and are not acceptable. While you may believe that your practices are not intending to interfere with anyone's rights, the regulations in fact bar some common practices surrounding cookie banners and opting out of selling personal information. If you have not reviewed your website for compliance with the regulations, now is the time.

Biggest Impact May Be Yet to Come

While the Court of Appeal's February 9 decision was surprising, the brief period between now and the original enforcement date of March 29 may not have a huge impact on most California

businesses. After all, the Agency and the AG do not have unlimited enforcement budgets. It seems likely that any "early" enforcement during the next six weeks will be focused on big targets or egregious noncompliance.

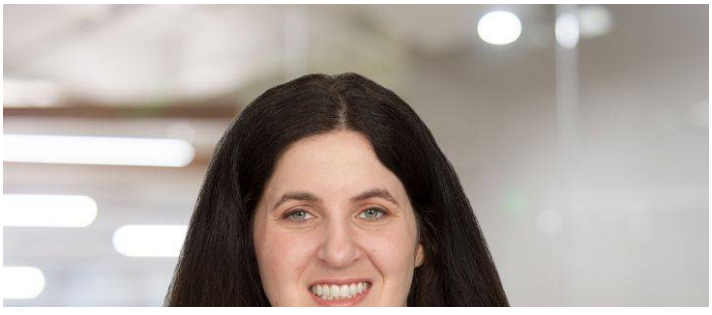
However, the biggest impact from this ruling may be the effect on current and future Agency rulemaking. If the ruling stands, the Agency and AG could be able to enforce any future regulations upon completion of the regulatory process rather than have a one-year enforcement delay. Those future regulations might include things like Agency's current (and controversial) proposal to regulate artificial intelligence and automated decisionmaking tools.

Conclusion

Fisher Phillips will continue to monitor CCPA obligations and enforcement efforts and provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insights to get the most up-to-date information direct to your inbox. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or an attorney on the firm's Consumer Privacy Team. You can also visit our firm's CCPA Resource Center at any time.

Related People

Benjamin M. Ebbink
Partner
916.210.0400
Email



Darcey M. Groden, CIPP/US
Associate
858.597.9627
Email

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Service Focus

Consumer Privacy Team

Privacy and Cyber

Government Relations

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills