Should You Wait to Comply with Updated CCPA Regulations Now that Enforcement Is Delayed? 6 Top Questions to Consider

Insights
8.11.23

The first half of 2023 has been eventful for businesses subject to the California Consumer Privacy Act (CCPA), and the whirlwind of new developments may have left you confused about your current and pending obligations. In late June — just as the California Privacy Protection Agency (CPPA) was set to begin enforcing the updated CCPA regulations that took effect on March 29, 2023 — a California court issued an injunction delaying enforcement of those regulations another year to March 29, 2024. Most recently, on August 4, the CPPA and California Attorney General (AG) appealed this court decision delaying enforcement. While you may think you have a little breathing room due to the delay, you should note that the court's action has no impact on changes to the CCPA that already took effect on January 1, 2023. Those requirements are still in effect and can be enforced by both the CPPA and the AG. So, what exactly are your obligations today as a covered business, service provider, contractor, or third party? Here are the answers to the top six questions you should be thinking about — a*nd if you want to take part in an interactive webinar discussing this issue in more depth on August 29, you can register here*.

1. What does all of this mean for now if you are subject to the CCPA?

Generally, all your prior efforts to comply with the CCPA and CPRA amendment (effective January 1) should continue. This includes implementing the changes required by the March 29 regulations for which enforcement is now delayed until March 2024. Here is a quick review of what's in play:

- **The CCPA** – the statute passed by the California Legislature in 2018 and effective January 1, 2020;
- **The original CCPA regulations** – drafted by the AG and effective August 14, 2020, with amendments effective March 15, 2021;
- **The California Privacy Rights Act (CPRA)** - the California ballot proposition that amended the CCPA, with some provisions becoming effective December 16, 2020, and all provisions now effective as of January 1, 2023; and
- **The updated March 29, 2023, CPRA regulations** – these updated the original CCPA regulations, and enforcement of these updated regulations has been delayed until March 29, 2024.

The takeaway: *To be clear, the CPRA is not a separate law from the CCPA, but rather just an amendment to the CCPA. The March 29, 2023, regulations (Updated Regulations) expound upon the requirements created by the CPRA amendment now in effect and update the prior CCPA*

the requirements created by the CPRA amendment now in effect and update the prior CCPA regulations for cohesion. (Keep in mind that the California Privacy Protection Agency is still working on rules related to cybersecurity audits, risk assessments, and automated decision-making. Based on the court's ruling delaying enforcement of the Updated Regulations, these additional regulations cannot be enforced until one year after they are completed.)

2. With the delay in the Updated Regulations, has the definition of "consumer" changed to exclude employees, job applicants, and business-to-business relationships?

No. The CCPA has always (since January 1, 2020) considered employees, job applicants, and persons acting in the business-to-business context to be consumers. Those exemptions just temporarily limited what rights people acting in those contexts had under the CCPA — that is until the sunset date for the exemptions. (The business-to-business exemption covered people acting on behalf of a business; it essentially extended the employment-related data exemption to data of employees of other businesses.)

The sunset date for the exemptions was in the CPRA amendment, *not* in the Updated Regulations. **Therefore, as of January 1, 2023, job applicants, employees, independent contractors, and individuals acting in the business-to-business context have the same CCPA rights as all other consumers.** This means that everything you do to comply with the CCPA today with respect to all other consumer populations (such as website visitors, app users, individual customers, etc.) applies to these groups as well.

The takeaway: *Make sure your CCPA compliance efforts account for all consumers and that the requisite notices and disclosures are provided to all your consumers. If you are still using CCPA notices for employees and applicants that were drafted in 2020, you must update them.*

3. What consumer rights are in effect with the Updated Regulations being delayed?

The delay in enforcement of the Updated Regulations does not change that all consumer rights are in effect today, including the new rights to correct inaccurate personal information and to limit the use and disclosure of sensitive personal information. The timelines associated with responding to consumer requests remain generally unchanged, and businesses must now account for processing requests to correct and requests to limit.

So, what's the caveat with the Updated Regulations? The Updated Regulations provide significant details around how to implement and process the new rights. For a request to correct, those details include how to determine whether personal information is inaccurate, instructions on action items when a request is granted, and some (but not all) of the timeline information on responding to the request (which follows the same timelines for consumer requests to know, access, and delete).

For the right to limit the use and disclosure of sensitive personal information, the Updated Regulations add instructions on processing a request to limit, including a processing time of within

15 business days. They also expound upon the limited uses of sensitive personal information by a business with the addition of Section 7027(m) – articulating eight reasons to guide businesses on what sensitive personal information may be processed without needing to provide consumers the right to limit.

The takeaway: *You need to account for both the right to correct and right to limit the use and disclosure of sensitive personal information in your documentation and processes. Because of the delay in enforcement of the Updated Regulations, there will be some wiggle room in how you implement these rights until enforcement of the Updated Regulations can begin as long as you comply with the portions in the CCPA statute that took effect January 1, as enforcement of the statutory requirements has not been put on hold. However, the best practice is to try to get it right from the beginning.*

4. With the delay in enforcement of the Updated Regulations, do I still need to respect opt-out preference signals?

The opt-out signal is still a must-have right now and cannot be delayed. The CCPA provides instructions for a business's processing on its website of opt-out preference signals (e.g., global privacy control or GPC). Additionally, the California Attorney General has – even prior to the CPRA amendments going into effect – taken the position that the CCPA requires a business that sells or shares data through cookies or pixels on its website to make sure that its website complies with opt-out preference signals that a user can set on their browser.

While the Updated Regulations articulate in greater detail not only the definition of an opt-out preference signal, its purpose, and what it means for a business to process an opt-out preference signal in a "frictionless manner," none of that changes that a GPC is still mandatory now for businesses that disclose data through cookies or pixels to third parties that are not service providers.

Because there still seems to be some confusion as to what constitutes selling or sharing, it is worth emphasizing that a business's website – for most businesses – is where this is happening. As the terms are defined, selling or sharing can include the use of analytics or targeted advertising, even where the business is not receiving money in exchange for the data disclosed to third parties. Businesses that have third-party cookies on their websites should take a close look at what the cookies are doing to determine whether they are selling or sharing data.

The takeaway: *If you are a business that is selling or sharing personal information (as those terms are defined in the CCPA), you must still process opt-out signals, including responding to GPCs. Work with your IT/web developer and marketing team to understand the implications on your website and related web presence.*

5. What's the deal with CCPA compliant contracts? Can I delay updating those until March 2024?

The obligation to have CCPA-compliant contract language is already in effect. While the statute identifies some specific terms that must be in a contract with a service provider, contractor, and/or third party (as those entities are defined in the CCPA), the Updated Regulations flesh this out in further detail. While a business could just go with a contract compliant with the statute but not the Updated Regulations, that is going to be a lot more work in the long run, as new contract addenda would have to be rolled out by March 2024.

***The takeaway**: Continue to ensure you have CCPA compliant contracts with vendors. There is no harm in meeting the Updated Regulation requirements today - otherwise you may find yourself attempting to renegotiate in eight months. Also, while you may want to find shortcuts to sending off your vendor contracts with ease, given the volume of vendor relationships, do not forget that basic contract principles will still apply.*

6. What security measures do I need in place? Is there anything I can delay until March 2024?

Under the CCPA, a business, service provider, contractor, and third party must implement reasonable security procedures appropriate to the nature of the personal information to ensure the security of the data. This is in place in the current set of CCPA regulations but reiterated in the Updated Regulations. Also, we know the CPPA has both cybersecurity audits and risk-assessments on their agenda for adopting further regulations, so expect more to come.

***The takeaway:** There are a multitude of areas to consider when reviewing a business's security procedures and practices, including but not limited to identification of high-risk areas and the sensitivity of data collected, conducting gap assessments, and whether to implement third-party audits. This area should not be on the backburner but a top priority.*

Conclusion

While the delay in enforcement is welcomed news, it is not a wholesale delay and the obligations to comply are vast and complicated. Compliance efforts should account for the detailed Updated Regulations in the drafting of any notices and disclosures and with the buildout of internal processes. The training requirement is also unchanged, and businesses must still conduct training for those responsible for CCPA compliance. Stay vigilant, as enforcement of the Updated Regulations will be here in no time.

We recommend you register for our upcoming webinar on August 29 where we'll examine these issues in an interactive format.

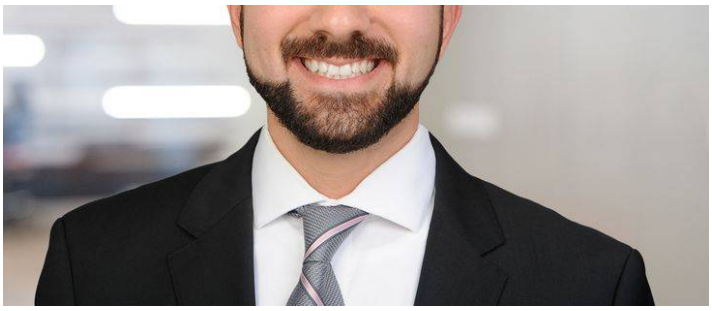
Fisher Phillips will continue to monitor CCPA obligations and enforcement efforts and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. For further information, contact your Fisher

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

Anne Yarovoy Khan
Of Counsel
949.798.2162
Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Trending

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

Woodland Hills