Fisher Phillips Launches CCPA Resource Center After California Lawmakers Keep Employers on the Hook: 5 Steps to Take Now

Insights
8.30.22

When the California Legislature wraps up its 2022 session on August 31, it will do so without having extended an exemption that kept employment data from being part of the California Consumer Privacy Act's (CCPA) many requirements. That means that employers subject to the CCPA must be prepared to comply with the many data privacy obligations as they relate to employment and job applicant data starting on January 1, 2023. There is much to do and not much time to do it – but there's good news. To assist employers in meeting this deadline, Fisher Phillips' Consumer Privacy Team has launched its CCPA Resource Center with a menu of flat-fee starter kits, templates, packets, and other resources to jumpstart the process. We encourage you to start preparing now as compliance can take three to six months to complete – or even longer depending on how much time and resources your business has to dedicate to the effort. What are the five steps you should take now to position yourself for this significant undertaking?

How We Got Here – The CCPA's Employee Exemption

A little history lesson is necessary here to explain where things now stand. Way back in 2018 (yes, even back before COVID), to avoid a competing ballot measure, the California Legislature enacted the California Consumer Privacy Act of 2018 (CCPA) – the first comprehensive consumer privacy statute in the United States.

However, the original legislation to implement the CCPA had an important exemption for employment data – and a similarly important exemption for "business-to-business" data. In general, with two exceptions, the employment data exemption provided that the panoply of CCPA rights did not apply to personal information collected from or about employees, job applicants, and independent contractors (in the context of their roles as such).

But here's the catch: the CCPA employment data exemption was not permanent. Originally, it contained a "sunset date" of January 1, 2020. This was thereafter extended to January 1, 2021, meaning that the entire scope of the CCPA would have applied to employee personal information starting on that date.

Continuing to Kick the Can Down the Road with the CPRA

Before the employment data exemption could expire, however, a follow-up ballot measure was put before the California voters. In November 2020, California voters approved Proposition 24, also known as the California Privacy Rights Act of 2020 (CPRA). The CPRA made numerous significant changes to the CCPA, including the creation of a new state agency called the California Privacy Protection Agency to enforce the law.

What's important for our purposes here is that the CPRA also extended the employment data exemption an additional two years. Unless the sunset date was further extended, the full range of CCPA/CPRA rights and obligations would apply to employment data beginning January 1, 2023.

Subsequent Efforts to Extend the Employee Exemption Fail

All of this set up an epic legislative showdown for 2022. The business community articulated early on that one of the most important issues was to further extend (or hopefully make permanent) the employment data exemption contained in the CCPA/CPRA. However, after extensive negotiations with labor advocates, an agreement was ultimately not reached in time. Therefore, the legislative session will end on August 31 without an extension of the exemptions.

After a number of years – and despite some valiant legislative efforts – the full array of rights and responsibilities under the CCPA/CPRA will apply to employees, job applicants, and independent contractors who are natural persons and residents of California come January 1, 2023.

5 Steps that Employers Can Take to Meet the Compliance Deadline

Looking ahead to the CCPA's/CPRA's impending new requirements, the following are five immediate steps that you can take to begin your efforts to comply with the new rules for employee data.

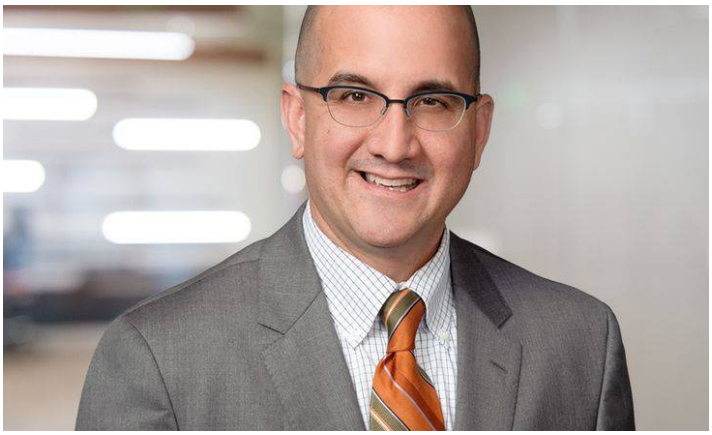
1. **Your business should update and assess its data inventory for employee and job applicant data.** A data inventory is a comprehensive list of all personal information held by the business. It should include from where the data was originally collected, where it is stored, what the data is used for, and who it is shared with (and why). In updating your data inventory, you should ensure that your data inventory is comprehensive, identifies which data is sensitive personal information under the CPRA, and includes all uses for personal information of employees and job applicants. This data inventory will be the foundation for drafting updated notices of collections for employees and job applicants and complying with their requests to exercise CCPA and CPRA rights.
2. **Your business should implement data minimization standards, including creating a data retention policy.** The new CPRA requirements mandate that notices to employees and job applicants must explain how long businesses will keep personal information. This, in turn, means you need to determine how long to keep personal information and then put that in a data retention policy. Once you have the policy, you need to determine how to securely purge stale data on a regular periodic basis.

3. **Update CCPA notices and draft privacy policies for employees and job applicants.** Current CCPA notices to employees and job applicants only need to include the categories of personal information collected and the business purposes for which the categories of personal information will be used. However, there will be many additional content requirements when the employee exemption expires. These requirements include, among other things, an explanation of how long various categories of personal information will be kept, identification of the categories of sensitive personal information that is collected, and if personal information is sold, a web address to exercise an opt of the sale of personal information. Additionally, employers will need to implement a privacy policy specific for employees and job applicants that complies with other content requirements.
4. **Implement processes for employees and job applicants to submit CCPA/CPRA requests.** Starting on January 1, 2023, employees, job applicants, and independent contractors will be able to submit CCPA/CPRA requests to know, delete, opt out of the sale of, and correct personal information, and to limit the use of sensitive personal information. Businesses will need to implement processes to receive and timely respond to these requests. Unfortunately, businesses cannot rely on the fact they have previously been able to respond to requests from consumers as evidence that they are prepared to respond to employee and job applicant requests. Responding to CCPA/CPRA requests from employees and applicants present special challenges, including the potential difficulties of locating personal information of employees within the business and determining how to respond to requests to delete.
5. **Visit our CCPA Resource Center.** Bringing a business into a compliance with the CCPA and CPRA can be a lengthy and daunting process that generally takes three to six months to complete, but it can be fast-tracked with some help from our Consumer Privacy Team. In order to help employers with their compliance efforts, Fisher Phillips has launched a **CCPA Resource Center** with a menu of flat-fee starter kits, templates, packets and other resources to jumpstart the process if you haven't started – or to give you the boost you need to meet the January 1, 2023 deadline to comply with significant changes to the CCPA.

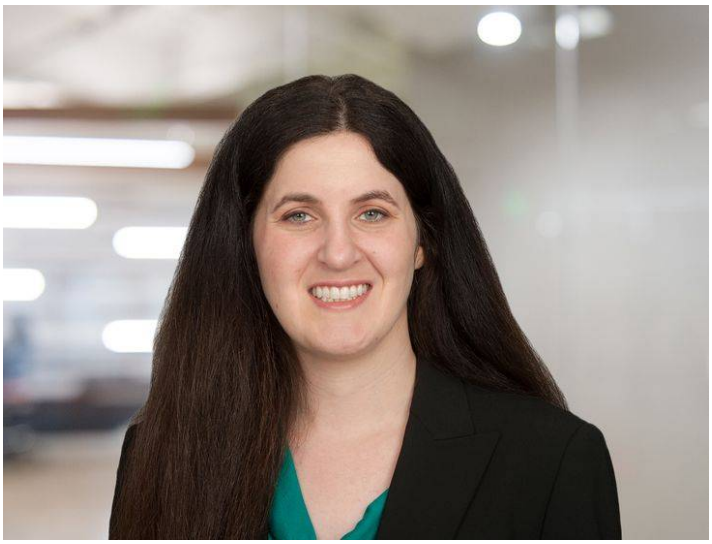
Conclusion

We will continue to monitor these developments, so make sure you are subscribed to Fisher Phillips' Insight system to keep up with the most up-to-date information. Please contact your Fisher Phillips attorney, the authors of this Insight, any attorney in our Consumer Privacy Team, or any attorney in our California offices should you have any questions.

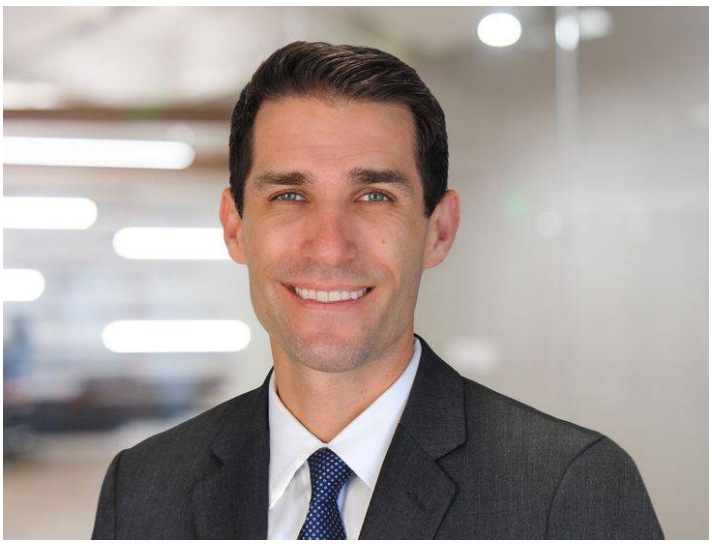
Related People



Benjamin M. Ebbink
Partner
916.210.0400
Email

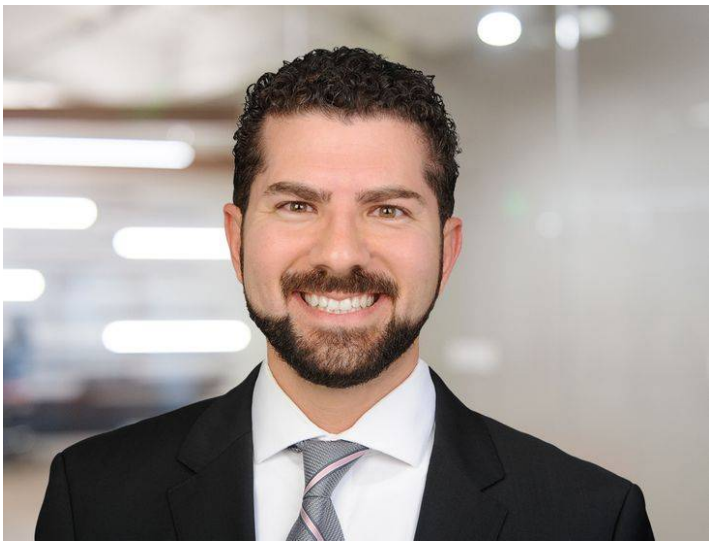


Darcey M. Groden, CIPP/US
Associate
858.597.9627
Email



Anthony Isola
Partner

415.490.9018
Email



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Service Focus

Consumer Privacy Team

Privacy and Cyber

Trending

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills