California Employers Beware: Your 5-Step Plan as Attorney General Announces CCPA Investigative Sweep

Insights
7.19.23

California employers, beware: the state's top prosecutor just announced his office is conducting an investigative sweep of whether and how large California employers have complied with data privacy and consumer protection requirements as they relate to employees and job applicants. The July 14 announcement came just two weeks after a court put a hold on enforcement of the updated California Consumer Privacy Act (CCPA) regulations that became final in March, which may have lulled some businesses into a false sense of security. And while this recent initiative targets "large" employers – a vague reference in the AG's announcement without further explanation – all businesses nationwide that are subject to the CCPA and have one or more employees in California should heed this warning. Here is a summary of what happened and a five-step action plan for employers subject to this law.

1. Understand the scope: employees now have all the CCPA rights as other consumers under the law.

Your first step is understanding how far this law now ranges. While employees were always consumers under the CCPA, their rights at the inception of the law in January 2020 were limited. However, as of January 1, 2023, the CCPA provides all California residents – regardless of the context in which they interact with a covered business – with the exact same rights that other consumers under the CCPA would have related to data collected from or about them. This has nothing to do with your type of business (for example, whether you are a business-to-business operation interacting exclusively with other entities, such as manufacturers), nor does it have anything to do with whether you are in the business of selling data.

As a reminder, to determine whether the CCPA applies to your business, check out this recent FP Insight. If your business triggers any of the criteria for the CCPA to apply, then all of the following individuals are your "consumers" with full rights under the CCPA so long as they are California residents and you have any data about them:

- current and former employees;
- family members, dependents, beneficiaries, and emergency contacts of your current and former employees;
- job applicants; and

- independent contractors who are individuals providing services in their individual capacity.

Recognizing that your HR and recruiting teams are now at the epicenter of consumer privacy compliance is the first step to withstanding an AG investigation.

2. Provide employees and applicants with notices at collection and a privacy policy.

At its core, the CCPA is all about transparency. That is why one of the first things employers will be asked about in the event of an enforcement action or inquiry is whether you provided all your employees and applicants with the right notices and disclosures at the right time.

Employers subject to the CCPA should review all their privacy notices and policies and ensure they have been distributed properly. The following is not an exhaustive checklist, but can provide a starting point for an internal assessment:

- Do you provide a privacy notice to job applicants who are California residents at or before the point at which you collect any personal information?
- Have you updated your privacy notice since 2020? That is, since January 1, 2023, have you provided all your current employees who are California residents with a privacy notice that identifies all categories of data you will collect from or about them during their employment and all the purposes for which you will use or disclose the data?
- Do you have your privacy notice included in your onboarding documents for new employees who are California residents?
- Do you have a privacy policy that employees who are California residents can access at any time?
- Does your privacy policy inform employees about what data you have collected from or about them in the last 12 months, where you got the data from, how you use and disclose the data, whether you sell or share their data for targeted ad purposes and if you have done so in the last 12 months and to whom you sold/shared it for such purposes, and how long you intend to keep the data? Does your privacy policy also inform employees of what rights they have under the CCPA and how they can exercise those rights?

3. Implement an effective workflow to receive, respond to, and comply with CCPA requests from employees and job applicants.

Under the CCPA, California consumers (including employees and job applicants) may exercise certain rights in relation to their personal information – and employers have strict deadlines to respond to such requests.

For example, a California employee or job applicant has a right to know what personal information is collected about them, the right to access such information, the right to correct such information, and the right to delete such information (subject to certain exceptions, such as where the employer must

retain the information for legal compliance or to defend against or prosecute legal claims). An employer has 10 business days to confirm receipt of such a request, and 45 calendar days to respond (which may be extended to 90 calendar days).

In addition, employees and job applicants can request to opt out of the selling of their data or the sharing of their data with third parties for purposes of targeted ads – and while most employers usually do not engage in selling or sharing of employee data in this manner, some do, and many are often surprised by what it actually means to sell or share data under the CCPA. (*Hint*: it is more than just disclosing data in exchange for money.)

Employees and job applicants also have a right to request that the employer limit the use or disclosure of certain data that the law defines as "sensitive," but only where the employer is using or disclosing the sensitive data in certain ways. Businesses must respond to these requests within 15 business days. Read more about these obligations here.

It is critical that you implement a CCPA-compliant request process for employees and job applicants (in addition to other consumers). Your process should address all of these types of requests and enable you to respond by the statutory deadlines, as well as maintain a record of all requests and how you handled them for at least two years. When implementing such a process, there are two key points to keep in mind:

- You must implement at least two methods for CCPA requests (a toll-free number and an electronic method) and adhere to the strict response deadlines discussed above.
- You must implement a verification process to verify the identity of the person making requests to access, know, correct, or delete. (You are prohibited from verifying opt-out requests or requests to limit.)

4. Update your contracts with vendors that collect, process, store, or access employee or applicant data.

Employers often have contractual relationships with vendors that collect and use employee or applicant data – including for payroll operations, benefit administration, employment and salary verification, and other uses. But employers are the "stewards" of this information and therefore this puts the onus on you to ensure CCPA compliance as to that data. Consider that a third-party vendor's improper use and storage of employee or applicant data can create potential liability for your business.

As the responsible party for this data, this requires you to exercise proper due diligence on your vendors to ensure their data usage complies with the CCPA, including the requirement to use "reasonable security measures." In addition to exercising due diligence and asking the right questions when selecting a reputable vendor, you want to ensure your contract has strong language to address potential issues. Most significant of these include clearly articulating the scope of acceptable data use and deletion requirements.

The AG will likely seek to hold you liable as the "information stewards" for violations by your vendors, so reviewing your contracts with vendors is a critically important part of avoiding or reducing potential liability. The AG will also be looking to whether you have updated contracts with your vendors to include specific terms required by the statutory changes to the CCPA that took effect this past January 1.

5. If you receive a letter from the AG, do not panic! Call your FP privacy attorney.

The AG announced his office will initiate this investigative sweep by sending inquiry letters to large California employers and then scrutinizing their response. Receiving such a letter can be a scary proposition. But don't panic! Our knowledgeable team is ready to help you respond to any such inquiry you may receive. The Fisher Phillips Consumer Privacy Team can help you assess your current state of CCPA compliance and respond to any inquiry in a manner that best protects your business. And if your review of the key takeaways above illustrates you still have some work to do, we can assist with that as well.

Conclusion

The AG's investigation is meant to serve as a strong reminder to employers that, while there was a reprieve for the first three years of the CCPA's existence as to employee and job applicant data, that grace period has ended. It is important that businesses expand their CCPA compliance efforts to fully include employees and job applicants who are California residents within their scope.

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' 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

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