Employers May Catch Temporary Break On Impending California Privacy Law

Insights
7.16.19

Thanks to recent negotiations among state lawmakers, it appears that California employers may get a temporary reprieve on some of the more sweeping data privacy requirements that were set to take effect in just a few short months. However, the pending legislation that would provide the delay would not exempt employers from significant disclosure requirements that also comprise the California Consumer Privacy Act (CCPA) – meaning you should still be in the process of preparing for the new law at your workplace.

California Assembly Bill 25, which passed the Assembly in May and is currently pending in the Senate, was recently modified so that employers about to be covered by the CCPA would receive a one-year extension on the deadline to start tracking, responding to, and complying with employee requests for disclosure, copies, and deletion of the employee's personal information you collect and maintain. Rather than the originally planned January 1, 2020 deadline, the amendment's passage would push the effective date of this portion of the statute to the start of 2021. However, AB 25 would not exempt you from the January 1, 2020 deadline to start disclosing to employees the categories of personal information you collect and the business purposes for which this information is collected and used.

Background
Enacted in June 2018 and amended in September 2018, the CCPA will provide sweeping privacy protections for California residents as of January 1, 2020. A detailed summary of the new requirements for employers can be found in our prior report on the CCPA.

The only "covered businesses" that will be subject to the CCPA are those for-profit businesses that (1) have annual gross revenues over $25 million, (2) annually receive, sell, or share personal information about more than 50,000 or more California residents or households or 50,000 devices, or (3) derive 50 percent or more of their annual revenue from selling personal information of consumers.

While this may appear to only apply to larger businesses, the second category (50,000 consumers or devices per year) is expected to capture many small businesses. For example, a small business that has a website with 137 unique visits per day and collects data about the devices or consumers who are accessing the site is going to meet the threshold. Similarly, a small business that buys

consumer lists for marketing purposes, and those lists contain information about 50,000 or more California residents or households, will be subject to the CCPA.

Employee Data

The CCPA as enacted makes no distinction between employees and consumers. "Personal information" is defined so broadly by the CCPA that it potentially covers all information you collect, maintain, or share about job applicants and employees that could identify the individual or be used in conjunction with other information to identity the individual.

This includes, for example, the name of an employee in conjunction with the state or federal protected category they are in (such as age, race, gender, sexual orientation, religion, disability, etc.). It also includes network or internet activity logs on company computers assigned to employees that show user activity such as search and browser history. The definition of "personal information" also lists the broad category of "professional or employment-related information" without any definition or parameters of what this entails.

Without passage of AB 25, the CCPA would require covered employers to track and respond to "consumer requests" from employees. Such requests include a request for a copy of all the employee's personal information the employer has obtained, compiled or shared in the last 12 months. You would have to respond to these requests within 45 days, which can potentially be extended by another 45 days.

Since the definition of "personal information" is so broad, the CCPA (without amendment) may allow employees and their attorneys to request and obtain from you free of charge a lot more than what the law otherwise permits – a significant amount more than just an employee's personnel file and payroll records. To say that this permits potentially abusive and burdensome pre-litigation discovery would be an understatement.

The AB 25 Compromise

AB 25 was introduced by the same legislator who authored the CCPA. It initially sought to clarify parts of the CCPA and modify its scope to exempt personal information obtained from or about employees and job applicants in the course of their employment or application for employment. Part of the rationale for this bill is that personnel information is already subject to other privacy protections, and employers typically collect and use this information for legitimate employment purposes such as administering benefits and payroll and complying with state and federal laws.

AB 25 appeared to be swiftly moving through the legislative process and gaining support from privacy advocates and staffing agencies. However, relatively late in the process, organized labor and their supporters opposed the bill and stated that they were very concerned about "workplace privacy" and were concerned with exempting employment data from the CCPA. This opposition threatened to derail AB 25, which would have been a terrible outcome for all California employers.

Fortunately, a compromise deal was recently reached to allow labor to remove their opposition to AB 25. The bill was amended on July 11, 2019 to provide the following:

- A one-year "sunset date," meaning the exemption for employment data will expire on January 1, 2021 unless extended. This reflects a commitment by the business community to work with organized labor on legislation related to labor's concerns regarding workplace privacy (and especially workplace surveillance) over the next year, in exchange for extending or eliminating the sunset date.
- The exemption for employment data does not apply to the private right of action under the CCPA for a data breach resulting from the business's failure to implement reasonable security measures as required by the CCPA. If an employee suffers harm due to a data breach of their "personal information" as defined by the CCPA, the employee can file a lawsuit seeking between $100 and $750 per consumer per data breach incident or actual damages, whichever is greater.
- Most significantly, this compromise will require employers covered under the CCPA to disclose to employees and job applicants the categories of personal information you collect about employees and job applicants and the purposes for which the information will be used. You must comply with this disclosure requirement by no later than January 1, 2020.

Next Steps

The good news is that employers appear to have a one-year reprieve before the floodgates of pre-litigation discovery and fishing expeditions by plaintiffs' attorneys are opened. The bad news is that this issue is far from over, as 2021 is only a year and a half away, and there is no guarantee that the legislature would reach a more permanent fix.

Regardless, you should immediately work on preparing the required disclosure to employees and job applicants to implement it no later than January 1, 2020. This disclosure can be made to employees as a group in the employee handbook or through a memo to all employees. There technically is no requirement that employees sign an acknowledgment of receipt of the disclosure, but practically having their signature will be the only sure way to prove that they received it, as we often encounter employees who later deny receipt of policy documents in order to leverage an advantage in litigation.

As for job applicants, since the CCPA requires that the disclosure be made at or before the transaction in which the personal information is collected, the best approach is to include the disclosure with the job application.

Although the compromise on AB 25 was not ideal, it was necessary to preserve the status quo while the issue continues to be debated in Sacramento. We will continue to monitor further developments and provide updates regarding this situation, so you should ensure you are subscribed to Fisher Phillips' alert system to gather the most up-to-date information. If you have questions, please contact your Fisher Phillips attorney or any attorney in any of our five California offices.

This Legal Alert provides an overview of pending state legislation. It is not intended to be, and should not be construed as, legal advice for any particular fact situation.

Related People

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