The California Consumer Privacy Act – A Brief Guide for Covered Employers

Article By
Cynthia J. Larose
Jennifer B. Rubin
Mintz

- Communications, Media & Internet
- Consumer Protection
- Utilities & Transport
- California

Tuesday, October 29, 2019

The California Consumer Privacy Act becomes effective on January 1, 2020 with an amendment that impacts California employers. Covered businesses should, of course, already be in the process of preparing CCPA privacy notices and disclosures. And while the amendment carves out some of the direct CCPA provisions applicable to California employers, employee data – and how it is handled – should also be on every covered employers’ to do list.

Does the CCPA Apply?

The CCPA applies to your business if your business obtains the personal information of at least 50,000 “consumers”, households, and/or devices per year (which on average, is equivalent to about 135 separate interactions with California residents per day over a year) and the business generates gross revenues in excess of $25 million per year globally or the business derives 50% or more of its annual revenues from selling consumers’ personal information.
A consumer is a natural person who is a California resident as defined in the law and enabling regulations. A “California resident” is any individual who is (1) “in the state of California for other than a temporary or transitory purpose,” or who is (2) “domiciled in the state” of California and “outside of the state for a temporary or transitory purpose.” “Personal information” (“PI”) is “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”

**What does the CCPA Require?**

The CCPA grants California residents specific rights regarding their personal information (“PI”):

- **Access and Portability** - Right to request that a business collecting an individual’s PI disclose the categories and specific pieces of PI that the business has collected

- **Deletion** - Right to request that a business delete any PI about the individual

- **Opt-Out** - Right to direct a business that “sells” PI about the individual to third parties, not to “sell” that person’s PI (business must provide opt-out mechanism on homepage)

- **Non-Discrimination** - Right to non-discrimination (pricing, quality, or quantity of goods sold, etc.) by a business solely because the individual exercises CCPA rights

- **Notice/Disclosure** - Right to receive full notice/disclosure regarding (a) when collecting PI, categories of data (PI, sources, 3rd parties), business purpose, and specific PI and (b) if a business “sells” PI to third parties, or otherwise discloses PI for a business purpose, categories of data (PI collected/sold, 3rd parties sold to, business purposes)

The CCPA also requires notice, before or at the time of collection, that informs consumers the categories of Personal Information the business will collect, the purposes for which the categories of Personal Information will be used, and notice of the collection of any additional categories of information or use of collected information for any additional purposes taking place after initial disclosures have been made.

In addition to the notice requirement, there are privacy policy requirements that require a listing of consumers’ rights under the CCPA, including the consumer right to opt out of the sale of the consumer's Personal Information and a separate link to the "Do Not Sell My Personal Information" on the business's website; how consumers may submit requests to exercise their rights to the business; a list of the categories of Personal Information that the business has collected about consumers, sold about consumers, and disclosed about consumers for a business purpose in the preceding 12 months.

**CCPA and Its Amendment’s Impact on Employment of California**
Residents

As mentioned above, all covered businesses must provide their employees with compliant privacy notices. In addition, even though one of CCPA’s amendments, AB 25, which Governor Newsom signed into law in October, has three employment-related exemptions, businesses must analyze those exemptions to determine the source of certain “HR Data” and whether such information is collected separately from the employment relationship.

AB 25 exempts certain “HR Data” for California residents in their capacity as job applicants, employees, individuals who are independent contractors, and corporate officers and directors (“Exempted PI”). It also exempts personal information of California residents identified as an emergency contact connected to Exempted PI as well as personal information used to administer benefits for California residents who are entitled to benefits from the employer by virtue of their relationship to Exempted PI — for example, spouses or dependents of employees.

Importantly, AB 25 provides only a one-year moratorium for most CCPA requirements for “Exempted PI” – but only if that information is collected solely in the HR Data context. In other words, if an employee (or applicant, contractor, etc.) is also a consumer of a business outside the employment context, all personal data collected in the consumer context remains fully covered by CCPA.

In addition, data collected by third parties at the employer for “voluntary” activities (such as fitness programs and other “perks”) and is then used to offer the employee any sort of service outside the work context (including discounts), this information is not Exempted PI and remains fully covered by CCPA.

Here is a chart of the most common types of information collected by employers – which includes HR Data – but only if that information is collected solely as an incident to employment. Note the information collected pursuant to these broad categories of information are only exempt from CCPA coverage if the information would not otherwise be collected except to facilitate the employment relationship:

<table>
<thead>
<tr>
<th>Banking information</th>
<th>Beneficiary information</th>
<th>Health information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Educational information</td>
<td>Past employment history (CV/Resume/Job application)</td>
<td>Salary history (perhaps former employers but definitely current)</td>
</tr>
<tr>
<td>Retirement information/planning</td>
<td>Family details (dependents, ages, marriage, prior marriage)</td>
<td>Home address (current, past), home telephone number, cell phone number</td>
</tr>
<tr>
<td>Daycare arrangements</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To illustrate the foregoing, if an employer collects an employee’s driver’s license solely to document Form I-9 immigration status, that information is “exempt” from CCPA coverage. However, if the employer collects the driver’s license information because the employer provides the information to a third party auto insurer who may offer the employee certain automobile insurance discounts based on driving history, then that information is not exempt under the CCPA and remains subject to the fundamental CCPA rights listed above.

**CCPA Has No Impact on Other Employment Rights**

The CCPA has no impact on other substantive or ministerial employment rights – such as the right to request certain personnel records, the general state constitutional right to privacy under California law, or the right to be notified of certain employer monitoring of electronic communications.

**A Brief Summary and Checklist for Covered CCPA Employers**

1. Employers with California employees must provide employees with CCPA Section 1798.100(b) privacy notices on or prior to January 1, 2020. Consider where and when those notices are delivered – for job applicants and for employees.

2. Employers should determine how employee data is mapped and stored – is any of this data collected separately from the employment relationship?

3. The private right of action under 1798.150 applies whether or not the data is HR Data – review your privacy data breach responses procedures now to determine whether they are statutorily sufficient.

4. Do your security control procedures meet minimum standards set out in the 2016 California Data Breach Report? Have you reviewed all 20 of the Internet Critical Security Controls and implemented controls appropriate to your business? This will help to establish “reasonable security” in defense of the
1798.150 class action in the event your company experiences a breach of employee (or any other) personal information.

©1994-2020 Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. All Rights Reserved.