GUNDERSON DETTMER

# California Consumer Privacy Act: California-Based Employees and Job Applicants

Insights
April 22, 2020

*This alert is the first in our series of Privacy Topics: Practical Guidance from Gunderson Dettmer – a collection of practical privacy and data security guidance and accompanying materials designed to facilitate your company's compliance efforts. Today's alert focuses on the rights of CA-based employees (including job applicants) under the California Consumer Privacy Act (CCPA) as it stands on April 22, 2020. For an overview of the CCPA, click here.*

***What is the current status of employees and job applicants under the CCPA?***

Employees and job applicants have a right to receive a CCPA-specific privacy notice, and have a private right of action under the CCPA in the event of a data breach that is due to their employer's failure to implement reasonable security measures. Beginning January 1, 2021, employees will also have the same data access and deletion rights granted to consumers under the CCPA. Note that "employees and job applicants" also includes individual contractors, consultants, agents, owners, officers, and directors.

***What steps should companies take to be CCPA compliant with respect to employees and job applicants before July 1, 2020?***

1. **Perform a data inventory to identify all employee and job applicant data collected**. The data inventory includes the categories of personal information

collected from employees and job applicants, the sources of the information, and any third parties with whom the data is shared.

2. **Perform a security audit to assess whether adequate security measures are in place with respect to employee data.** The level of security depends on the risk of the personal information held. For many companies, employee personal information (which typically includes social security numbers, financial account numbers, and health and benefits information) is going to be the most sensitive data the company collects and processes. At minimum, companies should follow the 20 CIS Controls published by the Center for Internet Security, as these have been endorsed by the California attorney general as evidence of reasonable security. Companies should audit the security of information on a regular basis, continually reviewing and updating the measures used as business and industry practices evolve. A security audit should also include a review of existing data breach response protocols and procedures.

3. **Create a CCPA-compliant privacy notice for employees and job applicants.** This notice must describe the categories of personal information collected, the purposes for which the personal information is used, and any third parties with whom the personal information is shared. It should also be consistent with the data inventory performed by the company as described above. The notice can be provided to existing employees via email, and should be included in a company's "new hire" materials, your employee handbook and/or any electronic folders or directories where you maintain similar information for employees.

   Many companies choose to create a separate notice for job applicants. Such notice can be posted on the company's "careers" web page and given to third party recruiters to provide to potential applicants.

   A template employee CCPA notice can be found here and a template job applicant CCPA notice can be found here. These forms are provided as examples, and we recommend that you contact your Gunderson Dettmer attorney to customize the forms for your business.

4. **Implement a vendor management program.** As part of the data inventory described above, you will identify which third party vendors process employee and job applicant data for you (e.g., for payroll and benefits administration purposes). You should take steps to ensure that your vendors have security measures in place to protect the personal information they process on your behalf. Depending on the risk profile of the personal information, this may include requiring vendors to obtain third party security certifications, or performing your own audits of the vendor's security measures.

Companies should also ensure they have in place CCPA-required contractual terms limiting what their vendors can do with the personal information. Your Gunderson attorney can assist in ensuring that your vendor contracts are appropriately amended to include the required provisions.

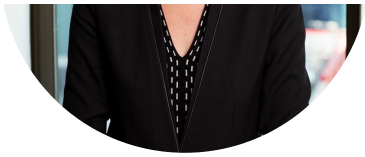
5. **Implement internal policies and training on how to handle employee data**. Make sure that your employees who handle employee and job applicant data have received appropriate privacy training, and that you have policies and procedures in place regarding the handling of employee and job applicant data.

***What are the potential consequences of non-compliance with respect to employees and job applicants?***

The CCPA will be enforced by the California Attorney General, who may levy fines up to $2,500 for each unintentional violation and $7,500 for each intentional violation. Additionally, the CCPA provides a private right of action (with the potential for class actions) for employees if their personal information is accessed, stolen, or disclosed without the employee's authorization, due to the failure of the business to implement reasonable security measures to protect the information. The private right of action provides for statutory damages ranging from $100–$750 per consumer per incident, or actual damages if greater.

## Related People

Anna C. Westfelt
PARTNER
P +1 650 463 5367



Katherine S. Gardner
PARTNER
P +1 212 430 3188

Brittany M. Nicely
ASSOCIATE
P +1 858 436 8067

## Featured Insights

FIRM NEWS

### Gunderson Dettmer Commemorates 2025 Asian American and Pacific Islander Heritage (AAPI) Month

CLIENT NEWS

### Brazilian Carbon Capture Company Mombak Announces $30M Financing

CLIENT NEWS

### Africa B2B OmniRetail Announces $20M Financing

CLIENT NEWS

### Glacier Announces Series A Financing to Expand Robot Recycling Fleet

CLIENT NEWS

### Datamin Announces $100M Investment Led by Fortress Investment Group

Datafinnir Announces $100M Investment Led by Fortress Investment Group

CLIENT NEWS

## Omnidian Announces $87M Series C for Renewable Energy Performance

INSIGHTS

## Splitting the Pie: How Savvy Founders Divide Ownership and Navigate Other Founder Equity Decisions

CLIENT NEWS

## Chainguard Announces $356 Million Series D Led by Kleiner Perkins and IVP

INSIGHTS

## Client Insight: California AI Transparency Act

INSIGHTS

## Client Insight: Prepare for BE-10 Benchmark Survey of US Direct Investment Abroad

INSIGHTS

## Tech Brew Interviews Aaron Rubin in “Where the legal battle stands around copyright and AI training”

CLIENT NEWS

## Latin America Fintech Belvo Announces $15M Funding