



## How Large Employers Can Prepare for CCPA/CPRA Obligations for “HR Data” in 2022

Get ready, large employers. After years of amendments exempting the personal information of employees and other personnel from the California Consumer Privacy Act (“CCPA”), covered employers now have a firm deadline by which to comply with the CCPA’s requirements in protecting employee and personnel personal information (“human resources data”). The deadline – January 1, 2023 – may appear far off, but certain provisions trigger obligations for 2022. Below are the steps large employers should take to comply with the CCPA.

### Step 1: Be familiar with the rights afforded to consumers under the CCPA.

The CCPA was enacted on June 28, 2018, creating one of the most comprehensive frameworks for regulating digital privacy in the United States. The law currently grants California consumers the right to know what personal information is collected, used and processed by covered businesses; the right to access the personal information; the right to request that covered businesses delete the personal information; the right to know whether and to whom the personal information is sold or disclosed; the right to opt out of the sale of personal information; and, the right to the same quality of service as that provided to consumers who do not opt out. The CCPA’s effective date was January 1, 2020.

### Step 2: Determine if the CCPA applies to the employers’ business.

The CCPA applies to for-profit companies that do business in California that either have an annual gross revenue of over \$25 million; buy, sell, receive, or share the personal information of at least 50,000 California residents, households, or devices for commercial purposes; or derives at least fifty percent of their annual revenue from selling California residents’ personal information (“large employers”).

### Step 3: Understand the extent of the CCPA’s current “employee” exemption.

Human resources data is largely exempt from the CCPA for the time being. Under the CCPA’s current “employee” exemption, the personal information of a job applicant, employee, owner, director, officer, medical staff member, or contractor of a covered business are exempt from the CCPA *as long as* the covered business collects and uses the personal information (1) in the context of the covered business’s relationship with the employee or personnel, (2) to maintain emergency contact information on file, or (3) to administer benefits.

Despite the employee exemption, employers should understand that there are existing obligations concerning human resources data. The CCPA requires employers to safeguard human resources data and to provide a notice to employees and personnel regarding the human resources data collected by the employer and how the information is used. Although no model notice has been provided under the CCPA, the notice must describe “the categories of personal information to be collected and the purposes for which the categories of personal information shall be used.” The CCPA privacy notice must be given to employees “at or before the point of collection” and provide a copy of, or link to, the employer’s privacy policy. Employers should also know that California residents can seek to recover statutory damages for certain data breaches, including those involving human resources data.

### Step 4: Understand the new obligations for human resource data under the CCPA.

Human resources data was exempt from the CCPA’s requirements until January 1, 2021. With the approval of Assembly Bill 1281 on September 29, 2020, the January 1, 2021 deadline was extended to January 1, 2022. California voters approved the California Privacy Rights Act (the “CPRA”) on November 3, 2020, which amended the CCPA and extended the employee exemption to January 1, 2023, the effective date of the CPRA.

The extra year is helpful for large employers, as the CPRA expands consumers’ rights. In addition to the CCPA rights, the CPRA grants California consumers the right to correct personal information; the right to limit the use and disclosure of sensitive personal information; and, the right to opt out of the sharing of personal information. Additionally, the CPRA has a 12-month “look-back” provision, meaning that employers should be tracking their collection, use, and

disclosure of human resources data up to twelve months before the January 1, 2023 effective date. Thus, employers should be prepared to provide information going back to January 1, 2022.

Enforcement of these additional rights lies with the ability of employees and personnel to seek to assert a private right of action for data breaches. The CPRA adds an additional enforcement mechanism by establishing the California Privacy Protection Agency, which administratively enforces the CCPA as amended by the CPRA.

### Step 5: Create an action plan to comply with the CCPA as amended by the CPRA.

Although the January 1, 2023 deadline seems far away, large employers should take steps to ensure compliance with the CCPA and CPRA concerning human resources data. These steps include: engaging in data mapping of human resources data; continuing to provide CCPA privacy notices to employees and personnel; ensuring the accuracy of privacy policies; evaluating physical, technical, and administrative safeguards concerning human resources data (which includes evaluating contracts with vendors such as payroll providers and benefit administrators); and implementing a plan to ensure the tracking of human resources data from January 1, 2022 and onwards.

As the effective dates of the CPRA loom on the horizon, Dorsey’s CCPA Team can effectively guide your organization through developing and implementing proactive California-compliant programs. Contact your Dorsey attorney for assistance.

**Gabrielle Wirth** is a Labor & Employment Partner at Dorsey & Whitney LLP. Gabrielle’s successful trial experience in a broad range of employment disputes including wage and hour, whistleblower, wrongful termination, discrimination, harassment, retaliation, breach of contract, and trade secret/noncompetition cases and her work with the corporate team on acquisitions and startups equip her to nimbly assess and provide legally compliant options, whether in the counseling or litigation defense role. She also represents employers before a wide variety of state and federal agencies. Gabrielle can be reached at (714) 800-1455 or [wirth.gabrielle@dorsey.com](mailto:wirth.gabrielle@dorsey.com).



**Melonie Jordan** is a Labor & Employment Associate at Dorsey & Whitney LLP. Melonie advises employers in various industries on a broad range of workplace privacy and information security issues. Melonie is certified by the International Association of Privacy Professionals (IAPP) as a Certified Information Privacy Professional (CIPP/US), a designation demonstrating her understanding of U.S. privacy and security practices and their applicability to the workplace. Melonie also defends employers before state and federal agencies and courts in a broad range of employment disputes. Melonie can be reached at (714) 800-1451 or [jordan.melonie@dorsey.com](mailto:jordan.melonie@dorsey.com).

