

CCPA/CPRA Will Apply to Employee AND B2B Data — Five Steps to Prepare for the January 1, 2023 Effective Date

WRITTEN BY

Sadia Mirza | Ronald I. Raether Jr. | Mark Payne | Kim Phan | James Koenig | Brent T. Hoard | Aaron Rothrock | Graham T. Dean

Exemption Extensions Failed. On August 31, California's legislature ended its 2022 session without adopting legislation to extend the California Consumer Privacy Act (CCPA) employee and business-to-business (B2B) personal information exemptions. In the absence of a special legislative session, these exemptions will expire on January 1, 2023.

History of the Exemptions. Under the current exemptions, covered businesses do not have to comply with certain requirements (e.g., consumer rights, such as access and deletion) when processing personal information collected in the employment or B2B context. First adopted in October 2019 after California's Governor Gavin Newsom (D) signed AB 25 into law, these exemptions originally were set to expire on January 1, 2021. On September 29, 2020, AB 1281 was signed into law, providing a one-year extension applicable only in the event that the California Privacy Rights Act (CPRA) ballot initiative failed. When the CPRA was adopted during the 2020 elections, the exemption was extended one final time to January 1, 2023.

Recent Attempts to Extend the Exemptions. During this year's legislative session, there have been numerous attempts to further extend these exemptions. Most recently, on August 16, Assembly Member Ken Cooley (D) introduced amendments to AB 1102 that would have extended the exemptions to January 1, 2025. This proposed amendment failed, as did other legislation introduced earlier in the session.

Five Steps to Start Preparing for Compliance by Year-End. Before the end of this year, businesses should take all steps necessary to extend their CCPA compliance programs to include personal information for employees and B2B contacts. For consistency and cost-efficiency, most companies plan to take an integrated view and will extend existing and/or planned privacy/program compliance policies and procedures developed for the CCPA/CPRA to employee and B2B data (including prospective B2B customers and vendors). That said, many companies are taking the following five steps to prepare for nuances specific to employee and B2B data:

1. **Data Mapping.** As a preliminary matter, businesses are preparing data inventories to ensure they have an accurate understanding of what information they are collecting/processing from employee/worker and B2B sources.
 - **Implementation Tip:** Many companies are coordinating this with tools and processes designed to develop a record of processing activities under the European Union General Data Protection Regulation (EU GDPR).

2. **Sensitive Information.** While the CPRA has a processing limitation and other provisions specific to “sensitive” personal information, in many instances, information collected for HR purposes may be considered sensitive, and thereby subject to greater protections under the CPRA.

- **Implementation Tip:** Many companies are amending the definitions in their data classification policy to align with the CPRA definition and/or developing procedures for handling sensitive personal information, including ethical collection, use, and sharing.

3. **Update Data Processing Agreements (DPAs).** Businesses may also need to update their contracts with vendors processing this previously exempted data, ensuring that the required contractual terms are in place to establish service provider or contractor relationships.

- **Implementation Tip:** Many companies are starting significant contract/DPA efforts to update them for both the CCPA/CPRA, as well as the EU GDPR, simultaneously and in an integrated way. Specifically, DPAs are being amended to (1) update all legacy contracts with the new versions of the EU standard contractual contracts by the deadline on December 27, 2022, and (2) to cover employee, B2B, and commercial data, while also clarifying data uses as a “service provider” (user rights for the vendor solely to provide the requested services) or a “business” (potential additional rights for secondary uses or sharing for the vendor’s independent benefit) under the CCPA/CPRA

4. **Extend Data Subject Rights Procedures to Cover Employee and B2B Data and Prepare for Requests.** If not already included under the EU GDPR and/or other applicable global laws, employers are preparing to receive data subject requests from employees, which in some instances may be used to gather information in anticipation of litigation. Also, on the B2B side, information regarding prospects (not just customer) are subject to the law.

- **Implementation Tip:** In some cases, the preparation is to test via a tabletop training exercise (similar to the ones conducted to train for incident response) the three key elements of a data subject rights response (*i.e.*, authentication, review of available exceptions, and defining the response/data to be given).

5. **Train, Train, Train.** Many companies are updating the CCPA training to cover the enhanced requirements under the CPRA. Now, the update should also expand the scope to cover employee and B2B data as well.

- **Implementation Tip:** Companies are creating marking and employee-specific modules or supplements to address AdTech and sensitive information processing that might be done in each area.

The risks associated with noncompliance are heightened under the CPRA, as businesses will no longer be guaranteed the right to cure violations.

Please contact Jim Koenig, Ron Raether, Kim Phan, Brent Hoard, Sadia Mirza, Graham Dean, or any member of our Privacy + Cyber Practice with questions.

To assist in preparing for compliance, Troutman Pepper has compiled a five-part series regarding the CPRA. The

series consists of the following sections: (1) introduction and overview; (2) consumer rights; (3) notice and disclosure obligations; (4) data processing obligations; and (5) litigation and enforcement and can be found at <https://www.troutman.com/insights/california-privacy-rights-act-series.html>.

RELATED INDUSTRIES + PRACTICES

- [Labor + Employment](#)
- [Privacy + Cyber](#)