# The California Privacy Rights Act: Determining if a Business Qualifies under New California Privacy Law Amendments

**Client Alert**
10.4.2022

More changes are on the horizon in the data privacy sphere for businesses and it is important for you to determine if your business is subject to California's new data privacy requirements. A shift in data privacy regulation in California is taking place by directly regulating business-to-business (B2B) and human resources personal information. The new requirements are strict and do not just impact businesses within California's borders.

In recent years, California has taken a strong stance on protecting consumers' personal information, enacting consumer-focused privacy protections in the California Consumer Privacy Act (CCPA) in 2018, which became effective January 1, 2020. While exempt from the CCPA's reach at that time, B2B companies and HR departments now must carefully examine the scope of the California Privacy Rights Act (CPRA), which amends the CCPA.

The previous B2B and employee-related exemptions expire at the end of 2022, and businesses around the country need to act quickly to ensure they are taking the necessary steps toward compliance.

On January 1, 2023, B2B and human resources personal information will be subject to the privacy and data protection laws under the CPRA. Both the CCPA and the CPRA provide consumers various rights, including the right to access, the right to know, rights to correction, and deletion rights. The addition of these categories of information to privacy protection will now subject many businesses to the complexities of privacy and data protection compliance under these California statutes.

## Related People

Jennifer A. Dukarski
Shareholder

Debra A. Geroux
Shareholder

Erin Malone
Associate

Claudia Rast
Shareholder

Maya Smith
Associate

## Related Services

Cybersecurity and Privacy Specialty Team

Three months is a short timeframe to align data collection and processing practices with California law. Businesses need to gear up to add B2B and HR data to their compliance efforts. The specifics will vary from company to company, but recommendations for compliance include efforts to: (1) identify systems that collect and process B2B and HR personal information; (2) determine what information is shared with third parties; and (3) update privacy policies and notices for employees, job applicants, and independent contractors.

**A GUIDE FOR ENTITIES**

**So how do you determine if your business needs to align their privacy compliance with these new amendments?**

The definition of businesses that are subject to the CPRA and CCPA comprises of many types of entities, so it is important to walk through all of the steps below to assess your potential need for compliance.

**Under the CCPA/CPRA, a business will be subject to these new requirements if any of the following apply:**

- **Step 1:** the business must meet one of the following parameters plus, an additional threshold requirement in **Step 2**:
  - Be a legal entity organized or operated for the profit or financial benefit of its shareholders.
  - Collect consumers' personal information or have such information collected on its behalf.
  - Alone, or jointly with others, determine the purposes and means of the processing of consumers' personal information.
  - Do business in the state of California.
- **Step 2:** if a business meets **one** of the above, then one or more of the following threshold requirements must apply to be deemed a business under the CPRA/CCPA:
  - As of January 1, of the calendar year, have annual gross revenues more than $25 million dollars in the preceding calendar year.
    - What is the notable change the CPRA made here?
      - The CPRA clarifies that revenue threshold of $25M should be calculated as of January 1 in relation to the revenue generated by the potential business in the preceding calendar year.
  - Alone or in combination, annually buy or sell, or share the personal information of, 100,000 or more consumers or households.
    - What is the notable change the CPRA made here?
      - The CPRA limits the threshold providing for a minimum number of consumer records by increasing the threshold from 50,000 to 100,000 and by removing from the scope of the threshold calculation of any personal information that the potential business had received

for the business' commercial purposes that had not otherwise been bought, sold or shared, and information about devices that are not identifiable to consumers or households.Derive 50 percent or more of its annual revenues from selling or sharing consumers' personal information.

- What is the notable change the CPRA made here?
  - The CPRA clarifies that the 50 percent revenue generation threshold should include the sharing of consumers' personal information for cross-context behavioral advertising.

**If both Step 1 and Step 2 apply to your business, then you are considered a business under the CPRA and CCPA and need to update your compliance regarding B2B and HR personal information.**

**Step 3:** However, if neither section seems applicable, you still must check if the two following definitions are applicable:

- **Step 3(a): your entity is *controlled* by a business that fits the parameters in Step 1 and Step 2 above AND:**
  - Not sure if your entity is "controlled by a business"? Your entity is controlled by a business if:
    - There is ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security **or**
    - There is control in any manner over the election of a majority of directors, or of individuals exercising similar functions

- **Step 3(b): your entity *shares common branding* with the business and with whom the business shares consumers' personal information.**
  - Common branding means:
    - A shared name that the average consumer would understand that two or more entities are commonly owned.
    - A shared servicemark that the average consumer would understand that two or more entities are commonly owned.
    - Or a shared trademark that the average consumer would understand that two or more entities are commonly owned.

If you still are unsure if your entity fits within the above tests, a last threshold may be applicable. If your entity is a joint venture or partnership composed of businesses in which each business has at least a 40 percent interest, then the entity is subject to the CPRA/CCPA. If that is the case, then each business that composes the joint venture or partnership is separately considered a single business.

Lastly, if none of the above steps are applicable to a business' activity, but a person does business in California and they voluntarily certify to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by the CPRA/CCPA, then a business is therefore clearly

subject to the acts and the new CPRA amendments.

If you are unsure if any of the above tests apply to you, or are concerned regarding the upcoming effective dates of these privacy laws, reach out to the authors of this client alert, or contact your Butzel attorney for more information and guidance to ensure that your business can meet these new compliance requirements.

**Other Key Dates to Bear in Mind**

Do not let the shifting patchwork of privacy law in the United States catch you off-guard. Keeping up to date on key timelines will ensure that your entity's endeavors remain compliant with the most recent iterations of privacy law.

The below are other key dates to bear in mind regarding comprehensive state privacy laws in the United States.

- **January 1, 2023**
  - **California Privacy Rights Act (CPRA):**
    - The CPRA, which amends the CCPA, will become fully operative. There will no longer be a right to cure, and the operative employee and business-to-business exemptions will expire.
  - **Virginia's Consumer Data Protection Act**
    - This Virginia's state privacy law will become effective on this date.
- **July 1, 2023**
  - **California Privacy Rights Act (CPRA):**
    - CPRA enforcement begins.
  - **Colorado Privacy Act**
    - This Colorado state privacy law will become effective on this date.
  - **Connecticut Personal Data Privacy and Online Monitoring Act**
    - This Connecticut state privacy law will become effective on this date.
- **December 31, 2023**
  - **Utah Consumer Privacy Act**
    - This Utah state privacy law will become effective on this date.
- **July 1, 2024**
  - **Colorado Privacy Act**
    - Starting on this date, Colorado's law will require a universal opt-out mechanism.
- **January 1, 2025**

- **Connecticut Personal Data Privacy and Online Monitoring Act**
  - This is the deadline for controllers to allow a consumer to opt out through an opt-out preference signal. The right to cure will also expire on this date, and the Attorney General will have discretion to grant a cure period.
- **Colorado Privacy Act**
  - The notice of violation and right to cure period will expire.

If you have any questions about the above issues, or if you need assistance, please contact the authors of this alert or your Butzel attorney.

**Erin Malone**
313.225.7063
malonee@butzel.com

**Jennifer A. Dukarski**
734.213.3427
dukarski@butzel.com

**Debra A. Geroux**
248.258.2603
geroux@butzel.com

**Claudia Rast**
734.213.3431
rast@butzel.com

**Maya Smith**
313.983.7495
smithmaya@butzel.com