HR Service Delivery

The CCPA and What it Means for Employers

In June 2018, California passed and signed the California Consumer Privacy Act (CCPA) into law. It is the first of a series of more stringent data privacy regulations to be passed in the United States at the state level in the wake of the European Union's General Data Protection Regulation (GDPR). The law protects California residents with new privacy-related rights that businesses and service providers must respect. The law encompasses a number of requirements and obligations intended to protect personal data, and notably it allows Californians to sue organizations directly, in a suit known as a private right of action, if their personal information (PI) is compromised in a data breach. While the legislation went into effect on January 1, 2020, confusion remains regarding who must comply and the steps required for compliance.

In November 2020, California voters approved Proposition 24, the California Privacy Rights Act (CPRA). The CPRA will amend parts of the CCPA and provide consumers with additional rights, narrowing the gap between the GDPR and the preeminent U.S. data privacy law. The new law becomes effective in January 2023 but includes a lookback period that will apply to PI retroactive to January 2022.

Who is affected by the CCPA and the CPRA?

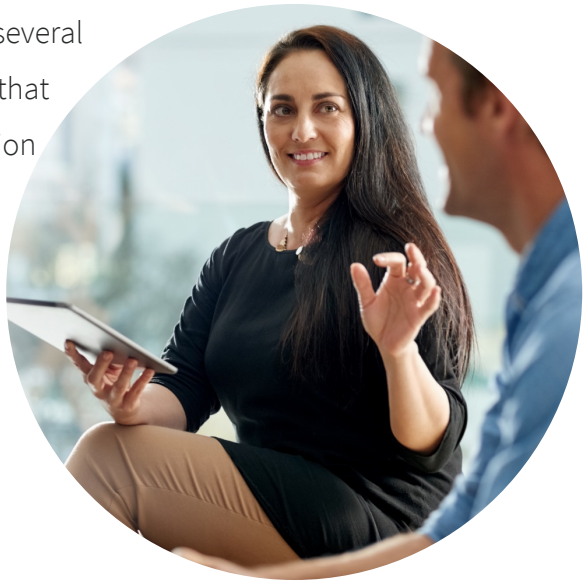
As a state law, the CCPA technically only applies to companies that do business in California or sell and/or collect data from California citizens. However, other states are likely to follow suit with the creation of their own data privacy laws.

The CCPA and CPRA apply to employers meeting one or more of the following criteria.

CCPA	CPRA
Companies with more than $25 million gross revenue	Companies with more than $25 million gross revenue in the preceding calendar year
Companies that store personal data of 50,000 or more consumers, households, or devices per year	Companies that store personal data of 100,000 or more consumers or households per year
Companies that derive 50% or more of their annual revenue from selling PI	Companies that derive 50% or more of their annual revenue from selling or sharing PI

The CCPA and CPRA requirements exclude many small and medium-sized businesses, but the likelihood of future legislation impacting these types of businesses creates a need for these organizations to start thinking about their data in terms of the expanded consumer rights established by these laws.

In September 2019, the California Senate and Assembly passed several bills that amended the CCPA and carved out an exception for PI that is used solely for employment purposes (i.e., recruiting information from applicants, personal information from employees for payroll and HR, etc.). PI collected for any other purpose is still covered by CCPA provisions. Employees are still covered by a portion of the CCPA, including a requirement for employers to provide their employees with a notice regarding the employer's privacy practices (such as informing the employee what information is being collected about them). This exception for employment-related data applies until January 2023, when the CPRA goes into effect.



What do affected organizations need to do?

The CCPA established several consumer rights for California residents, and the CPRA is expanding on those rights. Below is a comparison of certain key rights that may impact employees.

CCPA	CPRA
Know about all PI collected on them and to whom it was sold	Know about all PI collected on them, including sensitive personal information (SPI), with whom it is shared or to whom it is sold, and the intended retention period (or criteria used to determine that period)
N/A	Know about categories of SPI, and limit the use and disclosure of SPI
Opt out of the sale of their PI (or consent to sale for minors)	Opt out of the sale or sharing of their PI (or opt in for minors)
Request the deletion of all PI collected and maintained by the business	Request the deletion of all PI collected and maintained by the business
N/A	Have inaccurate PI corrected

Consumers may not be discriminated against for exercising these rights. The CCPA also entitles impacted individuals to sue following a data breach. The CPRA includes administrative fines for violations, with higher fines for intentional violations and violations affecting individuals under 16 years old.

By and large, the onus on affected businesses covers the following:

- **Providing notice:** At or before the point of collection, businesses must provide impacted individuals with a notice. In addition, they must also update their public-facing privacy notice to provide additional information.
- **Responding to requests:** Individuals may request that a business delete any PI collected about them; they may also request that PI not be sold to third parties. In addition, the CPRA includes a requirement to notify third parties of deletion requests, along with a new right allowing individuals to have inaccurate PI corrected. Businesses need a process in place to respond to and comply with these requests in a timely manner.
- **Improving security:** Due to the potential for costly lawsuits in the event of a data breach, it is a good idea to review your security control procedures in the wake of the CCPA. The CPRA includes a requirement that businesses help ensure the security and integrity of PI.
- **Minimizing data:** Under the CPRA, businesses are obligated to limit the use, retention, and sharing of PI to what is necessary and proportionate to the purposes that were shared with individuals.
- **Limiting the use and disclosure of sensitive personal information:** The CPRA creates a new right for individuals to limit the use and sharing of their SPI (such as driver's license number, passport number, account login with access code, genetic data, biometric data, etc.), with some exceptions. Businesses must notify individuals and obtain consent if using SPI for additional purposes.

The CPRA also enabled the creation of a California Privacy Protection Agency. In the future, the agency will be responsible for creating additional rules and regulations.

What can you do now?

There is a substantial amount of overlap between the CCPA, the CPRA, and the GDPR, so businesses that have already taken steps toward GDPR compliance are likely to be in a better position to comply.

Ensuring compliance with the CCPA and CPRA is simplified by dedicated technology and solutions from UKG HR Service Delivery (formerly PeopleDoc HR Service Delivery). The platform is designed to specifically address the unique and expanding needs of HR teams today and to help HR stay on top of its game while simultaneously improving employees' interactions with HR.

UKG HR Compliance Assist

UKG is dedicated to simplifying complexities for HR and easing compliance management. UKG HR Compliance Assist (formerly PeopleDoc HR Compliance Assist) is an online portal and alert service to help customers remain in compliance globally and easily navigate complex rules and regulations that vary by country.

UKG Document Manager

Employee files contain highly sensitive information; controlling access is critical. Further, the laws and regulations governing employee documents are extensive and vary by country. UKG Document Manager (formerly PeopleDoc Employee File Management) helps HR teams easily manage and comply with document regulations by supporting retention schedules, providing easy reporting on missing or expiring documents, and protecting sensitive information with secure, role-based access.

To learn more, connect with us online @UKG.com