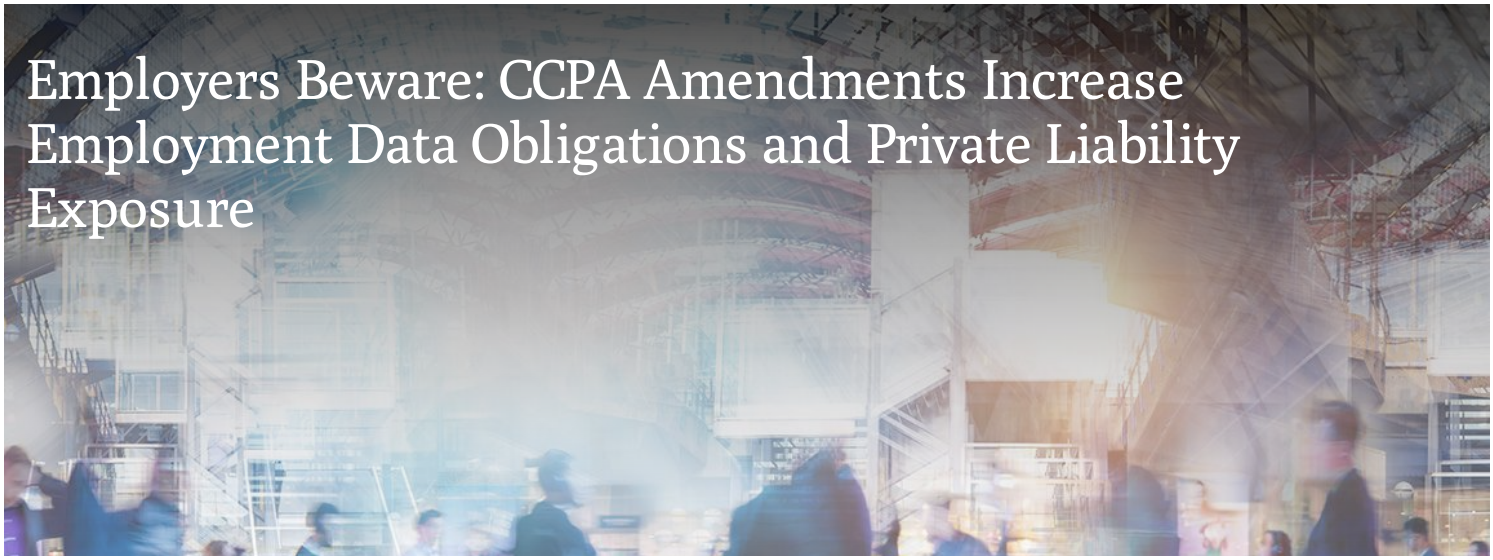
WINSTON & STRAWN LLP

BLOG



Employers Beware: CCPA Amendments Increase Employment Data Obligations and Private Liability Exposure

DECEMBER 9, 2022

KEY TAKEAWAYS:

- The CPRA amendments to the CCPA will place additional requirements on employers to respond to employee inquiries about the collection and processing of their personal information and provide employees with an enhanced notice of how employee personal information is handled.
- The CPRA amendments to the CCPA's private cause of action also increase employer exposure, primarily by expanding the definition of personal information to include email addresses in combination with a password or security question.

Beginning on January 1, 2023, the provisions of the California Privacy Rights Act ("CPRA") come into effect, thereby amending and expanding portions of the California Consumer Privacy Act ("CCPA"). The enactment of the CPRA will have significant ramifications for employers, mainly through (1) eliminating exemptions for personal information collected in connection with the employment context (e.g., for applicants and employees) and (2) revising the private cause of action to extend the theft or misappropriation of consumer email addresses in combination with a password or security question.

By eliminating an exemption that previously existed under the CCPA, the CPRA will impose additional obligations on employers collecting personal information from California employees. Among these changes, the CPRA will extend the CCPA's privacy rights to employees, including the right of employees to know what personal information the employer collects, the right to delete or correct such information, the right to opt out of the sale of personal information, the right to limit the use or disclosure of sensitive personal information, and the right to be free from discrimination arising from the exercise of these rights. In addition, employers will be subject to requests from employees to limit the use and sharing of certain sensitive personal information. "Sensitive personal information" is a new category of personal information introduced by the CPRA that implicates much of the data employers now collect on their employees, such as an employee's racial or ethnic origin, sexual orientation, union membership status, email addresses, and account log-in information.

Changes in the CPRA will also require that employers update their employment privacy notices. For instance, before collecting personal information, employers will need to inform California employees and applicants, among others, of their rights under the CPRA, disclose the types of sensitive personal information the employer collects, and identify certain information concerning the employer's treatment of such information. Moreover, the CPRA will require employers to enter into agreements with vendors processing employment personal information on an employer's behalf, which must include specific contractual clauses governing the service provider's use, treatment, disclosure, and retention of such information. While the CCPA imposed a similar contractual obligation, CPRA has expanded the provisions that must be in such agreements in order to avoid the data sharing arrangement being viewed as a "sale" of personal information.

An employer's exposure to the private cause of action under the CCPA has also increased. Previously, each consumer "whose nonencrypted and nonredacted personal information" was "subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures" could receive between $100 and $750 in statutory damages. While this is still true, the definition of personal information that triggers this potential liability has broadened to include an "email address in combination with a password or security question and answer." Although the private right of action is still limited to data breach events, and does not generally extend to other violations of the law, the type of information that can trigger a private suit following a data breach has expanded.

Employers who have California employees should consult their privacy and/or labor and employment counsel to ensure they remain up to date on the CCPA and to take all necessary steps to comply with the new requirements set to take effect on January 1, 2023. We note that the implementing regulations for CPRA are still under development and the law will not be actively enforced by the California Privacy Protection Agency until July 1, 2023.
3 Min Read

Authors

Sean G. Wieber

Alessandra Swanson

Tristan R. Kirk

Sophie R. LaCava

Christian W. Gray

Related Locations

Chicago | Los Angeles

Related Topics

CCPA | CPRA | Regulated Personal Information (RPI) | Privacy

Related Capabilities

Class Actions & Group Litigation

Related Regions

North America

Related Professionals

Sean G. Wieber

Alessandra Swanson

Tristan R. Kirk

Sophie R. LaCava

Christian W. Gray

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.