Recent Amendments to the California Consumer Privacy Act Could Affect New England Businesses

Description

Effective as of January 1, 2023, amendments to the California Consumer Privacy Act of 2018 ("CCPA") went into effect that impose additional obligations on businesses to safeguard the privacy of consumers' personal information. The CCPA already provided consumers with a variety of rights, including the right to know the personal information collected about them, how the personal information is used and shared, and the right to request deletion of any personal information in a business' possession.

The California Privacy Rights Act ("CPRA") amends the CCPA and grants consumers additional privacy rights, including the right to correct inaccurate personal information in a business' possession and to limit the use and disclosure of sensitive personal information collected about the consumer. Under both the CCPA and CPRA, "personal information" includes any information that identifies, relates to, or could be linked with a particular consumer or household.

The CPRA also expands the definition of personal information to include "sensitive personal information," consisting of identifying data such as government identifiers, financial information, log-in credentials, geolocation, or health information. This additional definition now requires businesses subject to the CPRA to assess and safeguard information that is regularly collected as part of basic human resources functions.

The CPRA applies to for-profit entities that do business in California, collect personal information, determine why and how the information will be processed, and meet any one of the following conditions:

- have a gross annual revenue of over $25 million.
- buy, sell, or share the personal information of over 100,000 or more California residents or households.
- derive 50% or more of their annual revenue from selling or sharing California residents' personal information.

One notable change made by the CPRA is to remove the CCPA's exemption for certain employment related information. The CPRA extends the definition of a "consumer" to include California-based employees, dependents, job applicants, independent contractors, and board members (for the purposes of this article, "Service Providers"), resulting in non-consumer facing entities being covered under the CPRA. For example, if a Massachusetts company meets the above criteria to be considered a "business" and has Service Providers who are California residents or who work remotely from California, the company will be subject to the provisions of the CPRA even if the company is not consumer facing and only has a physical presence in Massachusetts.

As a result of the expanded definition of "consumer" and the addition of "sensitive personal information," companies that previously were not subject to the CCPA will now be required to assess, document, and internally provide notice of the personal information collected about their Service Providers.

If an entity meets the criteria to be considered a California "business," it should consider implementing the following list of best practices to help in complying with the CPRA:

1. Evaluate and document what categories of personal information and sensitive personal information (including employee and job applicant information) are being collected and the reasons for such collection.
2. For consumer-facing businesses, update and post the company privacy policy with a description of the sharing or sale of information (if any) and the right to limit or opt-out of the sale or share of personal

information or sensitive information. Ensure that the policy is easily accessible on the company website. Businesses are encouraged to read the statutory requirements for what needs to be included.
3. Display on the company website a conspicuous opt-out option for the selling or sharing of personal information with third parties.
4. Provide notices to employees of the categories of personal information that are collected, the purposes for which the information will be used, whether the information will be sold or shared, the length of data retention, and disclosures about the collection and use of sensitive information. These notices should be posted and kept with other company policies. Businesses are encouraged to read the statutory requirements for these notices.
5. Assess current data retention processes and establish clear data destruction policies to eliminate unreasonably long retention periods of personal and sensitive information.
6. Execute and maintain reasonable security procedures and practices for personal information.
7. Within 45 days, respond to verified requests from consumers relating to: (i) the disclosure of any personal information that it has collected about such consumer; (ii) the deletion of personal information it has about a consumer; or (iii) the correction of inaccurate personal information about the consumer.

If a business does not comply with the provisions of the CPRA, consumers have a private right of action, allowing them to bring a direct claim or a class action for the unauthorized access or use of personal information as a result of business's violation of the duty to implement and maintain security procedures to adequately protect personal information. For guidance on how to comply with CPRA and CCPA, and to avoid such violations, companies are encouraged to read the full text of the CPRA and the Attorney General's FAQ for more information.

Partridge Snow & Hahn's Business Group is ready to answer questions regarding this article. For more information, contact Brian J. Reilly.

Partridge Snow & Hahn's Litigation Group is ready to answer questions and to provide advice.

Date Created
February 16, 2023