LEGAL UPDATES

Employee and Personnel Personal information – Privacy and Employment Law Intersect

Come January 1, 2023, businesses that are subject to the California Privacy Rights Act (CPRA) will need to reconsider their privacy practices, not only with respect to their customers' personal information but also with respect to their personnel's information.

06/15/2022 | 4 minute read

Come January 1, 2023, businesses that are subject to the California Privacy Rights Act (CPRA) (which amended the California Consumer Privacy Act (CCPA)) will need to reconsider their privacy practices, not only with respect to their customers' personal information but also with respect to their personnel's information.

As a reminder, a company that does any business in California is subject to the CPRA if any of the following apply:

- the company had annual gross revenue above $25 million in the previous calendar year;the company collects, stores, analyzes, discloses, or otherwise uses the personal information of 100,000 or more California residents or households in a given year; or
- the company derives at least 50 percent of its annual revenue from selling (disclosing to a third party for monetary or other valuable consideration) or sharing (disclosing to a third party for cross contextual advertising) the personal information of California residents.

Note that the CPRA applies, even if the company does not have offices in California, if they meet any one of the above thresholds and do business in California.

Privacy Policy Notice

Businesses that are subject to the CPRA must draft new, or update existing, personnel privacy policies that disclose the personal information they collect in the employment context, including from employees and contractors.

Privacy policies will now need to include additional disclosures regarding data retention time periods or criteria used to determine periods and more detailed disclosures regarding types of data collected, including sensitive data. Updated privacy policies will also need to offer certain employee rights that formerly only applied to other types of consumers, such as corporate website users and/or customers, under the CCPA.

Related People

Chiara Portner, CIPP/US

Partner

Redwood Shores

650.804.7672

chiara.portner@lathropgpm.com

Related Services

Data Privacy & Cybersecurity Compliance

Labor & Employment

Corporate & Business

Businesses will need to consider where to display and disclose these privacy policies as they must be available at the time of collection. Thus, businesses would be well served to include the privacy policies on job applications, recruiting website pages, as well as making them readily available to existing personnel in internal personnel handbooks, and on the businesses' intranet.

Employee Rights.

Personnel will have various additional rights under the CPRA:

Right of Access – Personnel will be able to request access to data retained by the business as of January 1, 2022. Such personal information may be stored in various places within a business, including in employee emails and chats, as well as resumes and other personnel records. Businesses will need to consider the rights of other employees and may need to redact data about them that may be included in the requesting employee's personnel record. Businesses should consider how to verify requests, such as via text or email. Third party automated systems may be used to search and find all data that a company has.

Right of Deletion – Subject to certain exceptions and legal obligations to retain data, businesses will need to be able to act swiftly within the mandated 45 day period (with an optional 45 day extension) to delete certain data.

Right of Correction – Personnel may require businesses to correct inaccurate data about them.

Right to restrict use of Sensitive Information to certain specific purposes – Sensitive information generally is data that has a plus factor such that if it were accessed by an unauthorized third party, it would likely be considered a security breach under various state security breach statutes. For example, sensitive information includes biometrics, social security numbers, driver license or passport numbers. Sensitive information also includes data that is more in line with European standards of what is considered sensitive, such as racial and ethnic origin, membership in a union, precise geolocation, religion, and sexual orientation. Personnel will have rights to restrict use of their sensitive information for specific purposes.

Right to opt-out of Sale – With broad definitions of Sales under the CPRA, businesses will need to evaluate if they need to offer this right and/or include links on their sites to make these opt out requests. For example, if the company's insurance provider can market additional products to personnel in exchange for a better insurance rate to the company, this may be considered a sale of data. While the CPRA generally provides for additional rights to opt-out of sharing information, sharing is defined as disclosing personal information for cross contextual behavioral advertising which would not apply in the employment context.

Businesses with personnel across various states should consider if they want to offer the same rights to all personnel or only California based personnel. Other state laws may differ, further complicating the landscape and considerations.

What to do now

First, before starting to update any documents, businesses must have a clear picture and understanding of their data collection practices. A business must conduct detailed data mapping exercises so they know where their data is stored, not only to update their policies, but also so they can properly and efficiently respond to a user's request for access to their data.

Moving from the data mapping stage, businesses will need to update their privacy policies and their data retention policies and practices. Businesses may find it beneficial to limit the data they retain to reduce the volume of data to sift through in the event of an access request for data. For example, a business may determine they will no longer save chat logs or will retain them for a shorter time period.

Human resources departments will need to be brought into discussions and plans around updating policies and procedures. They will also need to undergo training to ensure they understand how to respond in the event a consumer makes a request.

Last but not least, data protection addendums or agreements with service providers and contractors need to be revisited. These contracts must include the proper language the CPRA requires.

For more information, please contact Chiara Portner.