BCLP. Client Intelligent

Insights

THE END OF THE HR DATA EXEMPTION UNDER CALIFORNIA LAW?

Jun 16, 2022

Unless the California legislature acts soon, the scope of information subject to the California Privacy Rights Act ("CPRA") will include all employee or human resource-related personal information on January 1, 2023. To date, California employers have been obligated to only provide a short form privacy notice to employees, contractors and applicants.[1] California employers are not required to fully comply with the California Consumer Privacy Act ("CCPA") for all personal information concerning their employees, contractors, job applicants, and other similar types of personnel (collectively, "HR Data"). But unless the California legislature amends the CPRA, the exemption for HR Data will expire on January 1, 2023,[2] and California employees, contractors and applicants will have the full panoply of rights available under the CPRA.

Several bills have been introduced to extend the exemption or to otherwise limit the obligations placed on California employers with regard to HR Data, but as of this writing nothing concrete has advanced. As such it is becoming less likely that the exemption will be reintroduced prior to 2023. Draft CPRA regulations released by the California Privacy Protection Agency on May 27, 2022 similarly remove the requirement of providing employees with a short form privacy notice,[3] presumably preparing for the fact that the entire set of regulations will apply to HR Data. With the window to extend the exemption closing, California employers should start preparing soon for the application of CPRA to HR Data.

Specifically, California employers should consider the following compliance measures in preparation of the CPRA's effective date of January 1, 2023:

- **Application of CPRA.** As a threshold matter, evaluate whether the organization is subject to the CPRA. The CPRA applies to any for-profit business that: a) has an annual gross revenue of at least $25 million; b) collects the personal information of at least 100,000 California residents; or c) derives at least 50% of its revenue from the sale or sharing of the personal information of California residents.[4] Note that the threshold for compliance differs slightly from the threshold for the CCPA – whereas the CCPA applies to any business collecting the personal information of at least 50,000 California residents, the CPRA raises that threshold to 100,000 California residents.[5]

- **Understand/Map HR Data Flows.**To determine the scope of obligations under the CPRA, California employers should prioritize mapping the collection, use, and disclosure of personal data of California residents within their organizations. Specifically, businesses should identify internal departments that process California HR Data and evaluate the categories of HR Data involved (e.g., names, dates of birth, governmental identification numbers, etc.), how that data is being processed, the systems such data is hosted on or accessible from (whether internal or external), and whether and to what extent third parties are processing such data. Since the CPRA imposes data minimization requirements on businesses, retention periods for HR Data should also be considered. Typically, starting with internal Human Resources teams and Information Technology teams to map out the use of HR Data provides broad insight on other departments that may have access to the data. This information will serve as the backbone for next steps (*g.,* content of notices, implementation of data subject rights infrastructure, *etc.*) and is critical for building a dynamic CPRA program for HR Data.

- **Prepare or Update Employee/Job Applicant Notices.** As noted above, businesses are only required under the CCPA to provide short form notices to personnel and job applicants that explain the type of HR Data collected and the purposes of collection.[6]Under the CPRA, these types of notices must be much more detailed and provide additional information, including information about data subject rights, retention periods and other issues. In practice, employee notices will include similar information as that required for consumer privacy notices under the CCPA, along with some further information mandated under the CPRA (such as the additional data subject rights created by the CPRA).

- **Expand Data Subject Rights Capabilities.** In addition to making sure to expand existing data subject rights infrastructure to address new data subject rights under the CPRA (such as the right of rectification[7]) for customer data, such infrastructure must also be expanded to include HR Data. As with the other steps, the data mapping exercise will be critical to understanding where HR Data is stored, how it is used and how requests to exercise data privacy rights can be addressed. For certain rights requests, California employers should prepare to maintain information on data usage from the prior 12 months in order to respond appropriately beginning on January 1, 2023.[8] This underscores the importance of mapping this data now to ease compliance requirements beginning in 2023.

- **Service Provider Agreements.** It will be important to confirm that agreements with HR service providers or other third parties that access HR Data meet the content obligations for service provider agreements under the CPRA,[9] and that such providers have implemented the technical infrastructure to assist California employers in meeting their obligations under the CPRA (*e.g.,* meeting access and deletion requests, implementing retention and deletion requirements). Businesses should consider addressing this issue with new contracts now, and develop a strategy for revisiting extant agreements.

- **Review Incident Response Policies and Procedures.**The private right of action for certain data breaches includes qualifying breaches of HR Data under the current language of the CCPA.[10] Businesses should review their incident response processes and procedures to ensure that such policies are current, and more generally businesses should take into account data minimization procedures to decrease the risk of exposure. Businesses should also review their cybersecurity policies to ensure they are adequate.

Though there remains some hope the HR Data exemption will be extended or made permanent, California employers should begin preparing for application of CPRA to all personal information, including HR Data.

---

[1] 11 CCR § 7012(f).

[2] CPRA § 1798.145(m)(4).

[3] 11 CCR § 7012(j) (draft).

[4] CPRA § 1798.140(d)(1).

[5] Compare CCPA § 1798.140(c)(1) and CPRA § 1798.140(d)(1).

[6] See footnote 1 above.

[7] CPRA § 1798.106.

[8] For instance, if an employee or job applicant requests access to the HR Data maintained by the business, the business must provide an explanation of the HR Data collected, used, or disclosed during the prior 12 months, or since January 1, 2023 for requests made prior to January 1, 2024. CPRA § 1798.130(a)(3) – (5). The obligation to maintain information on HR Data usage begins on the operative date of the CPRA and is not retroactive.

[9] CPRA § 1798.100(d), 140(ag).

[10] CPRA § 1798.150(c).

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Gabrielle A. Harwell

Chicago

gabrielle.harwell@bclplaw.com
+1 312 602 5143