THOMPSON HINE

Privacy & Cybersecurity Update

July 2023

California Investigates Employee/HR Data Processing in Privacy Enforcement Actions

On July 14 California Attorney General Rob Bonta announced that his office sent inquiry letters to certain California employers requesting information on their compliance with provisions of the California Consumer Privacy Act (CCPA) concerning employees' and job applicants' personal information. Organizations that are subject to the CCPA and have employees in California should be on heightened alert. This announcement is also a significant reminder that the CCPA is still enforceable until new California Privacy Rights Act of 2020 (CPRA) regulations enter into force in March 2024 in accordance with a recent court ruling.

Responding to CCPA Regulatory Inquiries or Notices

An organization that receives an inquiry or a notice from the California attorney general with respect to its CCPA compliance program should immediately consult its internal legal staff or outside counsel for guidance and to better ensure its response process is protected under the attorney-client privilege. Given the breadth of the CCPA's compliance obligations, a response will likely require significant coordination with multiple business stakeholders, including HR staff, IT security personnel, and ethics, privacy, and other compliance officers.

Compliance Measures

Although the CCPA entered into force in 2020, a majority (although not all) of its privacy requirements only applied to personal information that was processed in the traditional consumer context. This framework, however, changed in January 2023 when the CCPA's HR data exemption expired and the entirety of the CCPA applied to employees' and job applicants' personal information. Accordingly, covered businesses should ensure that they have implemented programs, policies, and procedures to address a broad range of privacy requirements under the CCPA, including the following areas that are central in the HR context.

Privacy notices. One area in which the CCPA always applied to employees' and job applicants' personal information was with respect to a "notice at collection" privacy statement. Businesses commonly comply with this requirement in the employment context by drafting and implementing an employee data privacy policy that addresses how the business collects, discloses, uses, disposes of, and retains personal information pertaining to its employees and contractors, as well as the rights they have with respect to such data. This privacy notice or statement is often furnished to employees during the hiring and onboarding process. Similarly, it is common for businesses to post employment positions on third-party platforms (e.g., LinkedIn, Glassdoor, Indeed) or directly on their public-facing websites or even on their own company intranets. In turn, businesses may draft a separate job applicant privacy notice to provide an applicant who submits personal information in connection with an employment opportunity or incorporate the notice at collection criteria in their public-facing privacy statements and provide a link to California-based job applicants during the employee recruitment and application process.

Translations. Privacy notices published under the CCPA, including in the employee and job applicant context, need to "[b]e available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale

announcements, and other information to consumers in California." This is especially important for organizations with a large consumer base in California to which they issue sales terms, warranties, or other disclaimers in the non-English languages common in the region, such as Spanish. Accordingly, organizations should consider whether they are required to publish their privacy notices with a non-English language translation.

Accessibility. The CCPA's regulations require certain privacy notices to be "reasonably accessible to consumers with disabilities." For notices provided online, businesses must "follow generally recognized industry standards, such as the Web Content Accessibility Guidelines," (WCAG) and in other contexts, they must provide information on how individuals with disabilities may access the notice in an alternative format. This is important for several reasons applicable to HR data processing. For instance, it is common for an organization to maintain all employee policies and manuals, including employee data privacy policies, on its internal website (e.g., company intranet) so that they are available only to the organization's workforce. In these situations, the use of an internal website to disseminate an employee data privacy policy likely implicates the "provided online" standard set forth in the CCPA's regulations, and therefore such policies and notices must follow generally recognized industry standards pertaining to accessibility, such as the WCAG. If a business is using a third-party platform to post employment positions, collect personal information on California-based applicants and disseminate its job applicant privacy notice, it must ensure that the third party's website is also able to provide its privacy notice in a manner that satisfies the CCPA's accessibility standard.

Data subject rights and requests. Organizations should also assess whether their employees are afforded rights under the CCPA, such as the right to access specific or general categories of personal information, the right to delete personal information, or the right to prevent the "sale" of their personal information. The CCPA's regulations set forth strict requirements with respect to how organizations must provide notice of these rights to employees and job applicants. (e.g., via web forms, toll-free numbers, dedicated privacy email addresses). They also mandate the time frames in which organizations must respond to these data subject requests, what information must be furnished (or is exempted) in such a response, the training requirements for individuals who are responsible for assisting in the response process, how to verify and authenticate the identity of the data subject making the request and/or their third-party agent, and any relevant compliance exceptions. Accordingly, organizations should ensure they have a documented and tested process to receive, process, and respond to a data subject privacy request in accordance with the law.

Data processing agreements. It is important from both a legal compliance and data security perspective that organizations implement contract terms (e.g., data processing agreements) with their third-party service providers that retain and process personal information on their behalf. These agreements are required to limit how a service provider can access, use, and disclose personal information that they process on behalf of a covered business. It has also become an industry standard and a best practice to ensure these data processing terms address data ownership, information security, indemnification, and cybersecurity insurance, among other areas.

Security controls. The personal data processed in the HR context is often sensitive in nature. For instance, it may involve employees' and job applicants' Social Security numbers, driver's license numbers, financial data, or personal and family health information, which is used for facilitating health and wellness programs, conducting background screenings, and similar administrative purposes. Accordingly, organizations should ensure they have implemented comprehensive technical, physical, and administrative security controls to protect such sensitive personal data from a security breach, and that they maintain an incident response plan in the event of a breach.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Megan S. Glowacki
513.352.6503
Megan.Glowacki@ThompsonHine.com

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Marla M. Izbicky
312.998.4253
Marla.Izbicky@ThompsonHine.com
Certified Information Privacy Professional/United States (CIPP/US)

Thora Knight
212.908.3971
Thora.Knight@ThompsonHine.com