Published on *The National Law Review* https://natlawreview.com

HR and B-to-B Data Compliance Deadline Looming – Legislative Efforts to Extend California Consumer Privacy Act Exemptions Fail

Article By:

Alan L. Friel

Kyle R. Dull

Niloufar Massachi

Gicel Tomimbang

The California Consumer Privacy Act (CCPA) currently has limited carve-outs for personal information (PI) collected from a job applicant, employee, owner, director, officer, medical staff member, or independent contractor of a business acting in such capacity (including, without limitation, communications, emergency contact and benefits PI) (HR data). An even broader exception applies to B-to-B communications and related PI (e.g., vendor, supplier and business customer contacts and communications) (B-to-B data). As a result, businesses subject to the CCPA are not currently required to honor CCPA rights requests received from persons concerning HR data and B-to-B data. These carve-outs are set to sunset on January 1, 2023, when the California Privacy Rights Act (CPRA), which substantially amends the CCPA, goes into full effect, at which point HR data and B-to-B data will be fully subject to all of the requirements of the CCPA/CPRA. Many business administrators had hoped that either the California legislature would extend the HR data exceptions (or maybe even make them permanent), or a federal law that limited data subject rights to traditional consumers would pass and preempt CCPA/CPRA. It is now clear that the former is impossible and the latter is highly unlikely. Accordingly, many companies have a lot to do by year-end to prepare to stand up a CCPA/CPRA program for HR data and B-to-B data.

California Legislature Fails to Act

Bills proposing to extend the CCPA/CPRA exemptions for HR data and B-to-B data were introduced in the California Legislature this session, including AB 2871, which proposed to extend the carve-outs indefinitely, and AB 2891, which proposed an extension through January 1, 2026. On August 25, 2022, six days before the legislative session adjourned, Assembly member Cooley proposed amendments (AB 1102) to the CCPA/CPRA that, among other things, would extend the HR carve-outs until January 1, 2025. As we have previously explained, the constitutionality of such

amendments is questionable. To address that, AB 1102 dropped any reference to B-to-B data, added certain protections regarding employee monitoring and charged the legislature to further develop privacy protecting terms especially suited for HR data. However, the California legislative session closed on August 31, 2022, with none of these proposals having passed. Therefore, businesses should be prepared to comply with all CCPA/CPRA obligations for HR data by January 1, 2023.

Do Not Count on a Federal Privacy Law Preempting Your CCPA/CPRA Obligations Related to HR Data or B-to-B Data

The American Data Privacy and Protection Act (HR 8152) (ADPPA), a bipartisan federal data privacy legislation, was first introduced in the US House of Representatives on June 21, 2022. We have been following the bill's advancement. On July 20, the House Committee on Energy and Commerce amended ADPPA, after which the bill became eligible for a full House floor vote, meaning that House members may debate the ADPPA before they vote on it. California has emerged as one of the leading critics of the ADPPA, notably with the California Privacy Protection Agency (CPPA) opposing the ADPPA's preemption provisions. In an August 15 letter to Speaker Nancy Pelosi and Minority Leader Kevin McCarthy, the CPPA opined that the ADPPA would "remove important protections and significantly weaken the privacy Californians currently enjoy under the [CCPA]," and presents Americans with a "false choice" by representing that strong state privacy rights "must be taken away to provide privacy rights federally." On September 1, Speaker Pelosi issued a statement on the ADPPA echoing California's concerns on the ADPPA's preemption provisions, and she has reportedly stated that she would not hold a vote on the ADPPA in its current form.

As currently drafted, the ADPPA would generally preempt any state laws that are "covered by the provisions" of the ADPPA, excepting, among other things, "[l]aws that govern the privacy rights or other protections of employees, employee information, students, or student information." See Sec. 404(b)(2)(C). Thus, even if the ADPPA were successful (which appears unlikely based on recent developments), state privacy protections for HR data would not be preempted, and therefore businesses would still be required to comply with the CCPA/CPRA requirements for the same. While the ADPPA, as drafted, would likely preempt most B-to-B data, it is unlikely to advance without Speaker Pelosi's support.

Complying with CCPA/CPRA – HR Data and B-to-B Application

A business's current HR data obligations under the CCPA will be expanded under the CPRA, and B-to-B data will, for the first time, come into scope. This is a game changer for B-to-B companies that do not touch traditional consumer data (e.g., as a result of consumer marketing, customer service or warranty processing, even if they do not themselves sell direct to consumers) and HR departments. B-to-C companies, and B-to-B companies that process traditional consumer PI other than as a service provider for another business, will be further along, but even they will need to take steps to apply their consumer notices and rights request program to fully include HR data and B-to-B data.

- **Pre-collection notices to applicants, employees and contractors are still required.**

Covered businesses must continue to provide a pre-collection notice informing HR data subjects of the categories of PI to be collected and the purposes for collection. However, the CPRA's amendments to the CCPA, and corresponding new regulations (Regs), will expand a business's

obligations regarding HR data notices. This type of pre-collection notice is required both online and offline. The proposed Regs provide that the pre-collection notice to HR data subjects does not need to link to the business's privacy policy, suggesting a separate privacy policy for HR data subjects is permissible. However, the same proposed Regs describe mandatory HR data subject notices that will now be required in the business's privacy policy, suggesting that a business must have a single privacy policy. It may be that there is no conflict and the intent is that if – for HR data subjects – businesses want to satisfy pre-collection notice obligations by means of linking to a document that includes the required disclosures, that need not be the full privacy policy (as the Regs require for pre-collection notice to traditional consumers). However, the business's privacy notice needs to compressively cover all CCPA/CPRA data subjects. Given the difference between data practices related to HR data subjects and those related to traditional consumers, separate schedules, if not separate policies, will be necessary to distinguish between the two data subject types and avoid consumer confusion. Hopefully, the next set of proposed Regs will provide more clarity on this subject.

The pre-collection notice to HR data subjects must be easily understandable (i.e., written in plain language) and must inform employees of the statutorily enumerated categories of PI that are collected, including categories of sensitive PI (e.g., government ID number; race, ethnicity, religion, or union membership; contents of communications unless the business is the intended recipient; health-related information; sexual orientation; biometrics; and precise location), and the purposes for collection. Businesses must also disclose whether the categories of PI are sold or shared, the length of retention of the categories of PI, and if the business sells or shares PI, a link (or URL address) to the opt-out notice. If the business allows third parties to control the collection of PI (e.g., benefits providers), the notice shall also include the names of the third parties or information about their business practices. Accordingly, under CPRA, a much more robust notice at collection will be required compared to what was necessary under CCPA.

- **In addition, as to HR data, beginning January 1, 2023, covered businesses should also do the following:**

1. Perform a gap analysis.

As discussed, the expiration of the CCPA/CPRA carve-outs for HR data requires businesses to apply the full scope of CCPA/CPRA requirements to HR data. Therefore, businesses should conduct a gap analysis of their existing HR data privacy program, including, if not previously performed, completing a data inventory to determine where HR data is across business and vendor systems (including both structured and unstructured databases), and how it is obtained, used and disclosed, to determine how their current privacy compliance program can be built out to meet the requirements of the CCPA/CPRA. In doing so, keep in mind that HR data subjects who will soon have access rights include dependents and beneficiaries. Though the Regs are silent on the limitations on their access rights, the statute provides exceptions that may be the basis for limitation. In addition, businesses will need to accommodate new CPRA rights such as correction and limitation of certain processing of sensitive PI (e.g., for affinity and wellness programs). HR professionals will also need CCPA/CPRA training before next year.

2. Provide a full privacy policy to HR data subjects that incorporates all the content requirements for privacy policies enumerated in the implementing regulations.

The California Attorney General previously issued CCPA Regs, which went into effect on August 14, 2020, and that reflected the limited application of the law to HR data then in effect. When the CPRA amendments to the CCPA passed, the CPPA assumed CCPA/CPRA rulemaking responsibilities from the California Attorney General. At the end of May 2022, the CPPA published draft CPRA Regs and issued a notice of proposed rulemaking for the same on July 8, 2022, that was followed by a 45-day public comment period that closed on August 23, 2022. Once a revised set of Regs is issued, there will be a public comment period limited to the revisions.

As to privacy policies applicable to HR data, the proposed Regs would require, among other things:

- A description of a covered business's online and offline practices regarding the collection, use, sale, sharing and retention of HR data from the preceding 12 months, including the categories of sources from which HR data is collected and the recipients of disclosure by category of PI (this is far more comprehensive than what is required in current pre-collection notices).

- An explanation of the rights conferred by the CCPA/CPRA on HR data subjects; including the right to know what PI the business has collected about the data subject (both categories and specific pieces); the right to correct inaccuracies; the right to opt-out of the sale or sharing of HR data by the business; the right to limit the use or disclosure of sensitive HR data by the business (subject to certain exceptions that apply to some but not all HR functions – notably, diversity programs are not an exception); the right to delete PI (subject to a host of exceptions that are so far written to apply in a traditional consumer context and will need to be shoehorned into HR applications); and the right not to be retaliated against for the employee's or contractor's exercise of their CCPA/CPRA privacy rights.

- An explanation of how HR data subjects may exercise their CCPA/CPRA privacy rights and the process for the same, including how the business verifies an employee's request and how an authorized agent may submit a request on behalf of an employee.

3. Implement a mechanism through which HR data subjects may submit requests to exercise their CCPA/CPRA privacy rights.

As with traditional consumer rights requests, covered businesses must also develop and implement a mechanism for receiving rights requests from personnel seeking to exercise their CCPA/CPRA privacy rights. This means that businesses must complete a data inventory of HR data across their systems and identify outflows to vendors and others, so they can meaningfully respond to requests. Note that although the requirements for HR data do not go into effect until January 1, 2023, the CCPA famously has a 12-month lookback period, meaning businesses must be able to account for HR data throughout 2022, both as to notices and access rights (note, however, the lookback period for access will expand over coming years). Furthermore, the CCPA/CPRA requires businesses to provide at least two designated mechanisms through which individuals, including employees, may submit their CCPA/CPRA-related requests. Most businesses (other than the narrow group that operates exclusively online) must use a toll-free phone number as one of the two designated methods for receiving such requests. If a business has a website, the proposed Regs require that one designated method for receiving such requests be accessible through the website, such as via a webform. However, businesses will likely want a different request flow, or even request process, to

distinguish between HR data subject requests and traditional consumer requests. Businesses should also look at existing HR self-service tools and consider how these can be leveraged to, in part, fulfill HR data subject rights requests, keeping record-keeping obligations in mind. Of course, a "consumer" could make a request as both an employee and a customer, so if requests are segregated by data subject status, that, and how to make requests in another capacity, must be made clear.

4. View CCPA rights requests as if they were discovery requests.

Businesses should be careful when responding to CCPA/CPRA rights requests, especially in the context of HR data, given that plaintiffs' employment lawyers may use CCPA rights requests as a tool to circumvent formal discovery requirements and go on pre-litigation fishing expeditions. Regarding this issue, the California Attorney General previously opined that "there is no exception allowing businesses to refuse to respond to a verifiable [individual] for the [individual's] personal information while litigation is pending or allowing the business to deny [an individual] request on the basis that the business suspects the request was made in lieu of discovery." Thus, plaintiffs' lawyers are not prohibited by the CCPA/CPRA from using rights requests for such purposes. However, evidentiary privileges and the protection of trade secrets and/or the privacy rights of others are grounds for limiting access requests. Essentially, businesses should treat CCPA/CPRA rights requests as akin to responding to discovery requests. In the "Next Steps" section below, we provide a link to a webinar recording that goes into how to do this in detail, applying learnings from Europe, where employees have long had broad PI access rights.

5. Shore up agreements with service providers.

Covered businesses should also shore up their agreements with vendors that process HR data to ensure they meet the CCPA/CPRA's stringent requirements for "service providers." If CCPA/CPRA-required restrictions and provisions are not incorporated into contracts with service providers, a business's transfer of HR data to such parties may constitute a CCPA/CPRA sale or share, which is then subject to a consumer's right to opt out of that disclosure and claw the PI back. Some examples of vendors that may be processing HR data that businesses should keep in mind include those that process data for employee pay, security monitoring, benefits, timekeeping, and training. However, some of these vendors may act as data controllers in some regards and, accordingly, not qualify as service providers. In such cases, to avoid a "sale," an exception such as disclosure at the direction of the data subject will need to be constructed. Also of importance, businesses should monitor their service provider's compliance with the CCPA/CPRA's restrictions and obligations to not be responsible for a service provider's lack of compliance.

Even if a business updated its agreements with service providers who process HR data during its CCPA compliance program, the CPRA's amendments to the CCPA set forth new additional requirements of what must be included in the written contract between a business and its service provider.

- **Heed recent California Attorney General enforcement activities when building your CCPA/CPRA compliance program for HR data and B-to-B data.**

On August 24, 2022, the California Attorney General issued a press release announcing the first

public settlement involving alleged violations of the CCPA, which included a $1.2 million civil penalty payment. Among other things, the settlement emphasized the requirement for businesses to provide sufficient notice of data "sale" (or "sharing") in their privacy policy and honor opt-out requests, including when such opt-outs are made via user-enabled opt-out preference signals, especially as to third-party website cookies not contractually restricted to the kind of limited data processing permitted of "service providers" under the CCPA. While many B-to-C companies' websites remain out of compliance in this regard, most B-to-B companies have not even begun to think about tracking technologies and digital advertising as relates to CCPA/CPRA. For more information, see our recent post on the issue.

Concurrent with the announcement of its first public CCPA settlement, the California Attorney General also published 13 new "illustrative examples" of CCPA noncompliance supplementing the 27 examples provided in July 2021. Businesses should treat these illustrative examples as a guide for what the California Attorney General is looking out for when reviewing a business's compliance with the CCPA, including for CCPA compliance related to HR data. These illustrative examples highlight CCPA compliance related to failure to honor CCPA rights requests and failure to provide CCPA-compliant privacy notices.

And Do Not Forget About B-to-B Data

Companies will need to apply their CCPA/CPRA obligations to B-to-B data and provide B-to-B data subjects with all consumer rights as of the beginning of next year. In doing this, bear in mind that the current B-to-B exception is not for B-to-B businesses but for B-to-B data. Accordingly, even B-to-C businesses will have previously out of scope B-to-B data that will now be subject to consumer notices and requests. Most of what we outlined above regarding new requirements for HR data applies equally to B-to-B data. Companies will need to think about how to provide the new notice and process data subject rights in a way that takes into account the differences between these data subjects and traditional consumers. For instance, the need to protect trade secrets – a basis for rejecting an access request – is more likely to arise in the B-to-B data context than in traditional consumer requests.

Next Steps

Please refer to these webinar materials for more information on business obligations related to employee and other HR data under the CPRA. The webinar recording is accessible here.

Although the other four state omnibus privacy laws (CO, CT, VA and UT) going into effect in 2023 do not cover HR data or B-to-B data, they, too, need to be considered as companies determine what they need to do to be 2023-ready.

National Law Review, Volume XII, Number 251