SQUIRE
PATTON BOGGS

California Employers Face New Challenges for HR Data Processing

August 2025

On June 30, 2025, the California Civil Rights Council (CRC) secured final approval for regulations addressing employment discrimination resulting from the use of artificial intelligence and other algorithms that it collectively refers to as Automated-decision Systems (ADS).

Shortly after that, on July 24, 2025, the California Privacy Protection Agency (CPPA) board approved its own long-anticipated regulations on cybersecurity audits, privacy risk assessments and automated decision-making technology (ADMT) under the California Consumer Privacy Act (CCPA). See our blog posts on the regulations and their edits and additions. While much of the focus on the CPPA's CCPA regulations has been on traditional consumer data, the implications of this double-barreled rulemaking for human resources (HR) data may be even more significant.

The CCPA remains the only US state comprehensive privacy law (CPL) with compliance obligations for HR personal information. This opened a challenging frontier for businesses that collect, analyze or automate employment-related data, and the latest CCPA regulations further complicate HR operations.

Because HR data is not generally regulated by other state CPLs (Colorado's CPL applies to biometrics in the workplace), and there are only a smattering of labor and employment laws directly on point (e.g., NYC Local Law 144 of 2021 (requiring transparency and bias audits for automated employment decision tools) and a recent amendment to the IL Human Rights Act (requiring notice of AI for HR decisions, prohibiting discriminatory effect, and banning use of zip codes as proxy for protected classes)), most companies have not begun preparing for AI/ADMT-related compliance in the workplace, notwithstanding that these practices could implicate equal employment and nondiscrimination laws of a general nature.

Under the CRC regulations, starting October 1, 2025, employers utilizing ADS will face far stricter scrutiny of the resulting decisions. Most significantly, employers will need to conduct antibias testing or other measures to eliminate the risk of discriminatory decisions made or facilitated by ADS. They will also need to maintain records related to the employment use of ADS for four years. There is no opt-out or appeal right, but the California legislature is considering a bill that would require employers to give written notice and a right to appeal if the employee has been affected by an employment-related decision made by an ADS. The draft legislation defines "employment-related decision" to include everything from hiring to setting schedules and wages, potentially creating a morass of appealable decisions.

And, just to keep things interesting, the current draft uses a different definition of ADS from both the CRC and CCPA regulations. Another bill would require public disclosure to the Department of Industrial Relations regarding all workplace surveillance tools utilized, including the specific models and capabilities of equipment utilized and information collected. Whether these laws are passed this session remains to be seen, but they highlight the ongoing popularity of workplace privacy regulation in Sacramento and anticipate future challenges for employers.

Under the CPPA regulations, effectively starting in 2026 (potentially as early as October 1, 2025), but phasing in over time in many respects, organizations will be expected to:

- Identify and assess ADMT tools used in HR
- Evaluate whether those tools involve "significant decisions" and the degree of "human in the loop" decision-making
- Conduct and document data processing "risk assessments," and file annual compliance attestations with the CPPA
- Provide notice and opt-out rights to job applicants and employees, where required
- Maintain data and software and hardware inventories, apply robust security protections and obtain annual independent security audits, including attestation filings with the CPPA

ADMT – Narrowed Definitions, but High Stakes for HR

One of the most hotly debated developments during the CCPA rulemaking process was the narrowing of the definition of ADMT, at least in the context of transparency and choice obligations. Early drafts of the regulation adopted an expansive view, potentially sweeping in virtually any algorithmic processing that informed decision-making. In contrast, the final version limits ADMT to systems that "replace or substantially replace human decision-making" in high-stakes contexts.

This shift has been broadly welcomed by industry, as it reduces ambiguity and lowers enforcement risk. However, it has also drawn strong criticism from privacy and labor advocates, who argue that the final rules eliminate vital protections for transparency fairness, and accountability in automated systems.

Still, despite the narrower scope, the implications for HR functions remain substantial. The rules apply to significant decisions, a category that includes "a decision that results in the provision or denial of … employment or independent contracting opportunities or compensation," which implicates virtually every core employment decision – hiring, termination, promotion, demotion, compensation, benefits, scheduling and work assignments, among others.

Many employers already use algorithmic tools across these domains, including to:

- Screen resumes for job qualifications
- Monitor performance using productivity or behavioral metrics
- Determine eligibility for raises, bonuses or shift assignments
- Assess conduct or flag anomalies in internal communications

Under the new CCPA rules, HR systems may now trigger risk assessment requirements – and in some cases, employee opt-out rights – if they meet the threshold for ADMT.

While the regulations include certain carve-outs, these may not apply to HR tools, depending on how the technology functions and the specific context in which it is used. Even if a carve-out appears to be available, organizations should still conduct a baseline assessment to determine applicability. Where appropriate, they should also develop internal policies governing the use and training of ADMT tools in HR, ensuring those tools are developed and deployed in a compliant manner. Businesses will have until January 1, 2027, to implement the ADMT provisions, including preprocessing notice and a right to opt out.

Beyond ADMT notice and opt-out rights, risk assessments under the new rules are required before initiating any processing of personal information that presents a "significant risk to consumers' privacy," which includes using ADMT for a significant decision. A "significant decision" in the HR context specifically includes decisions about hiring; allocation or assignment of work for employee; salary, hourly or per-assignment compensation, incentive compensation such as a bonus or another benefit; promotions; and demotions, suspensions or terminations. Assessments are also required for the processing of sensitive personal information, which is commonplace in the HR context, regardless of use of ADMT, as well as processing of personal information to train ADMT for significant decision making. In addition, "using automated processing to infer or extrapolate a [Californian]'s intelligence, ability, aptitude, performance at work, economic situation, health (including mental health), personal preferences, interests, reliability, predispositions, behavior, location or movement, based upon systematic observation of that [person] when they are acting in their capacity as [a] … job applicant, … employee, or independent contractor for the business" triggers a risk assessment. Although businesses will have until December 31, 2027, to fully document the assessments, they will need to do so on high-risk processing activities occurring on and after the effective date, which could be as early as October 1, 2025 (though could slip to January 1, 2026). For risk assessments conducted in 2026, business will have until April 1, 2028, to file corresponding annual risk assessment attestation information. Despite the delay in the documentation and filing requirements, it is clear that assessments will be required on new and ongoing high-risk processing starting in late 2025 or the beginning of 2026. This will be a new task for many companies, and the CCPA risk assessment operational and documentation requirements are very detailed.

In addition, cybersecurity audits will be required for certain businesses. The timing for completion of a first annual cybersecurity audit and filing an audit report with the state will depend on the size of the business:

- April 1, 2028 – Over US$100 million gross revenue
- April 1, 2029 – Between US$50 million and US$100 million
- April 1, 2030 – Under US$50 million

However, keep in mind that the audit is for the prior calendar year and will include assessment of data, hardware and software inventories, and policies and procedures to protect those assets, and many companies will need to make substantial improvements to their data governance programs to be ready to undergo an audit.

New California Regulations To Police Employment Discrimination by ADS

While the final CCPA regulations narrowed the definition of ADMT, the CRC regulations utilize an expansive definition similar to what the CPPA had originally proposed. An ADS is a "computational process that makes a decision or facilitates human decision making" regarding employment matters. The CRC regulations state that an ADS "may be derived from and/or use artificial intelligence, machine-learning algorithms, statistics, and/or other data processing techniques." Perhaps appreciating how expansive that definition is, the CRC actually included a section explicitly excluding word processing, spreadsheet navigation and several other categories of standard business software. The fact that they thought they needed to specifically exclude even the humble calculator underscores just how expansive they intend to be.

Employers who utilize ADS will need to be prepared for several requirements going into effect October 1, 2025. First and foremost, employers now bear the burden to engage in proactive efforts to avoid discriminatory outcomes by conducting antibias testing or other measures to eliminate the risk of discriminatory decisions made or facilitated by ADS. The regulations explicitly state that the absence of such testing will be considered to support a claim of discrimination. The new regulations also extend to four years the obligation to maintain records related to the use of ADS in making decisions. Some of those records may constitute personal information subject to access and copings by the data subject under CCPA, demonstrating the impact of the interplay of these two different sets of regulation in the HR context. The final version of the regulations also expands liability to third parties acting as agents of an employer. This may result in liability for vendors who supply ADMT products that turn out to discriminate (or are not adequately tested and are presumed to discriminate.)

Bring Together CRC Evaluations and CCPA Assessments

There is significant potential overlap between the CRC ADS bias diligence obligations and the new CCPA requirements to conduct risk assessments. Businesses would be well advised to coordinate compliance efforts under both frameworks, potentially documenting them within the same assessment process. While the privacy risk assessment obligation under the CCPA is broader in scope, one of its core components – avoiding discrimination – will likely be shaped by the industry standards established under the CRC's ADS rules.

To meet the CCPA's standards, a risk assessment must:

1. Clearly define the specific purpose of the processing (generic descriptions like "improving services" are not permitted)

2 Identify the categories of personal and sensitive information used

3 Explain how the data is collected, used, retained, and shared, including the duration of retention, number of data subjects affected, mode of consumer interaction, and any third-party disclosures and their purposes

4. Describe the logic and outputs of any ADMT tools used to make significant decisions

5. Identify the specific benefits of the processing (not in generic terms)

6. Assess the risks and harms to data subjects, including risks such as discrimination, coercion, economic loss and psychological harm

7. Outline the safeguards implemented to mitigate or eliminate those risks

8. Document the business's decision to proceed with the processing; list contributors to the assessment; and name and identify the roles of individuals who approved the assessment (excluding legal counsel)

All but items 5 and 6 (likely to try to avoid constitutional challenge) must be documented in a summary report to be retained and available on request by the state for review, and annual compliance attestations must be filed with the CPPA. This will be a big operational lift for many companies that have not already implemented privacy-by-design as part of a robust information governance program. We have developed assessment tool kits that can help you jump-start a data processing impact assessment program. See our Tools and Guidance Materials to Aid AI & Data Governance for more information.

Conclusion

The final CCPA rules may have softened in scope, but the road ahead for HR data governance is anything but simple. California's leadership in regulating workforce data – combined with the looming operational complexity of AI/ADMT governance – means that employers must move swiftly to address the evolving legal and business risk landscape while responsibly meeting business imperatives to increase efficiency through new technologies. Organizations are well advised to take a risk-attuned and rights-based approach to workforce automation, including:

1. **Initiate an overall legal assessment** – Begin by consulting legal counsel to evaluate the organization's use of ADMT/ADS and AI in the employment lifecycle. (We offer clients an online stakeholder survey tool, which is a good place to start). Clarify whether any processing activities fall within the new definitions and decision thresholds, or otherwise implicate labor and employment and human rights law prohibitions on bias and discrimination.

2. **Inventory and protect HR data and technologies** – Map all HR data and data processing, especially algorithmic and data-enhanced tools used for workforce management, including those provided by third-party vendors. Implement management and data security policies and procedures. Learn the requirements for a successful cybersecurity audit and become audit ready.

3. **Prioritize data processing impact risk assessments** – Identify tools likely to meet the "significant decision" test and begin developing data protection impact assessments (DPIAs), especially for systems with direct employment consequences, as well as for other high-risk processing activities, such as processing of sensitive personal information, creating HR inferences through systematic observation, or training of ADMT for significant decision-making. Document and retain at least what is called for in assessment summary reports. Reassess when there are changes to the activity.

4. **Revisit internal policies** – Update employee privacy notices, human resources information system (HRIS) documentation and internal compliance playbooks to reflect the new requirements and evolving use of technology.

For more information, contact the authors.

Contacts

Michael W. Kelly
Partner, San Francisco, Palo Alto, Los Angeles
T +1 415 954 0375, +1 650 856 6500, +1 213 689 5175
E michael.kelly@squirepb.com

Lydia de la Torre
Of Counsel, Palo Alto
T +1 650 843 3227
E lydia.delatorre@squirepb.com

Alan L. Friel
Partner, Los Angeles
T +1 213 689 6518
E alan.friel@squirepb.com

The opinions expressed in this update are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.