

## Response by the Centre for Information Policy Leadership to the California Civil Rights Council’s Proposed Modifications to Employment Regulations Regarding Automated Decision Systems

The Centre for Information Policy Leadership (“CIPL”)<sup>1</sup> welcomes the opportunity to respond to the California Civil Rights Council (“CCRC”)’s [proposed modifications](#) to employment provisions of the Fair Employment and Housing Act regarding Automated Decision Systems.

CIPL has a long history of promoting responsible data practices through its efforts regarding organizational accountability. Indeed, CIPL’s Accountability Framework,<sup>2</sup> at its core, is a blueprint for responsible data practices. By encouraging organizations to implement and demonstrate accountability, CIPL has sought to ensure not only that organizations comply with applicable legal requirements and best practices but also that they earn societal trust in their commitment to legitimate and beneficial use of data. CIPL has also advocated for a principles-based approach to regulation of artificial intelligence (AI), automated decision-making, and accountable AI governance, including with respect to regulations in California.<sup>3</sup> CIPL has also underscored the importance of approaches to technology and data governance that prioritize the protection of civil rights,<sup>4</sup> including combating the potential for AI bias in employment contexts.

CIPL notes that the [Initial Statement of Reasons](#) accompanying the Proposed Rules did not discuss privacy or data protection. We encourage the CCRC to consider carefully the implications of any proposed changes to employment rules in these areas and to avoid contradicting or duplicating

---

<sup>1</sup> CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL’s mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL’s work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL’s website at <http://www.informationpolicycentre.com/>. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

<sup>2</sup> See CIPL resources and papers on organizational accountability: <https://www.informationpolicycentre.com/organizational-accountability.html>.

<sup>3</sup> See, for example: *Ten Recommendations for AI Regulation*, October, 2023, [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_ten\\_recommendations\\_global\\_ai\\_regulation\\_oct2023.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ten_recommendations_global_ai_regulation_oct2023.pdf), *Building Accountable AI Programs*, February 2024, [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_building\\_accountable\\_ai\\_programs\\_23\\_feb\\_2024.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_building_accountable_ai_programs_23_feb_2024.pdf) (informationpolicycentre.com), *Response by CIPL to the CPPA’s Invitation for Preliminary Comments on Proposed Rulemaking on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking*, March 2023, [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_response\\_to\\_cppa\\_invitation\\_for\\_preliminary\\_comments\\_on\\_proposed\\_rulemaking\\_on\\_cybersecurity\\_audits\\_risk\\_assessment\\_and\\_adm\\_march\\_27\\_2023.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_cppa_invitation_for_preliminary_comments_on_proposed_rulemaking_on_cybersecurity_audits_risk_assessment_and_adm_march_27_2023.pdf), and *Automated Decisionmaking and Profiling (ADM) Requirements in U.S. State Privacy Laws, and Current State of Play in State AI Regulations*, May 2024, [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/adm\\_profiling\\_requirements\\_us\\_privacy\\_law\\_cipl\\_may24.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/adm_profiling_requirements_us_privacy_law_cipl_may24.pdf).

<sup>4</sup> *CIPL Response to NTIA Privacy, Equity, and Civil Rights Request for Comment*, March 6, 2023, [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_response\\_to\\_ntia\\_privacy\\_equity\\_and\\_civil\\_rights\\_request\\_for\\_comment\\_6\\_march\\_2023.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_ntia_privacy_equity_and_civil_rights_request_for_comment_6_march_2023.pdf).

existing legislation. The CCRC should document the reasoning behind these proposed changes in the record and demonstrate how the proposed changes are consistent with applicable privacy regulations.

In addition, we outline several particular points of concern below.

1. **The CCRC’s draft rules implicate privacy and data protection.** The draft rules regulate “automated decision system data,” defined as “any data used in the process of developing and/or applying machine learning, algorithms, and/or artificial intelligence that is utilized as part of an automated decision system.”<sup>5</sup> This includes, but is not limited to, personal information provided by applicants or employees, or information about individual applicants or employees. Careful consideration of privacy principles and intersections of the proposed rules with existing privacy regulations is critical given how central the processing of personal data is in many automated systems.
  
2. **The CCRC’s draft rules intersect with existing privacy law and potential forthcoming regulations from the California Privacy Protection Agency (“CPPA”).**<sup>6</sup> The California Consumer Protection Act (“CCPA”), as amended by the California Privacy Rights Act (“CPRA”), regulates employment data (unlike many other U.S. state privacy laws). Additionally, the CPPA is in the process of preparing regulations on Automated Decision-Making Technology (“ADMT”).<sup>7</sup> Both existing and potential forthcoming regulations intersect with the CCRC’s proposed modifications addressing the use of automated decision systems in employment contexts. The CCRC should consider the intersections between the civil rights it seeks to protect and the privacy and data security rights the CPPA seeks to protect carefully to ensure a coherent, consistent and workable regulatory framework. Areas for which coordination is especially important include:
  - a. **Data Retention.** Under [CCPA](#), a business’s retention of personal information, including employment-related information, must be “*reasonably necessary and proportionate*” to achieve the purpose for which it was collected and processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.<sup>8</sup> By allowing for shorter (or longer) retention periods and a contextual assessment that considers privacy and security risks, the CCPA’s approach could be interpreted as a more flexible and privacy protective retention standard than the CCRC’s proposed recordkeeping requirements, which prescribe that all “relevant records,” including “automated decision system data”

---

<sup>5</sup> Section 11008.1(d) of the Proposed Modifications to Employment Regulations Regarding Automated-Decision System, available [here](#).

<sup>6</sup> In addition, Bill [AB2930](#), which remains live in the current legislative session in California, seeks to restrict use of automated decision tools that could result in algorithmic discrimination and includes requirements for developers and deployers to conduct annual impact assessments.

<sup>7</sup> California Draft Regulations Regarding Risk Assessments and Automated Decision-making Technology (“ADMT”), March 2024, available [here](#).

<sup>8</sup> Section 1798.100(c) California Consumer Privacy Act of 2018.

created or received by an employer or other covered entity dealing with any employment practice, must be preserved for a period of four years from the date of the making of the record or the date of the personnel action involved, whichever occurs later.<sup>9</sup> Because the CCPA provides a general exemption for compliance with other legal obligations, in instances where the CCRC's rules would apply, CCRC's standard would prevail, arguably exposing that data to greater privacy and security risks through retention of data for a mandatory four-year period.<sup>10</sup>

- b. Deletion Requests.** Under the CCPA, California employees and job applicants can request the deletion of their personal information from employers.<sup>11</sup> An exemption is if the personal information is needed for a business to comply with another legal obligation.<sup>12</sup> Given the breadth of the CCRC's proposed data retention requirements, its rulemaking could limit the deletion rights granted to employees and job applicants under the CCPA, potentially increasing the privacy and data security risks with respect to personal data that would otherwise be subject to deletion.
- c. Definition of "Automated Decision-making Technology."** The CCRC's definition of "automated decision-making system" is different from the definition of "automated decision-making technology" proposed by the CPPA.<sup>13</sup> Whereas the CCRC's definition captures any software that "facilitates" a decision that "impacts" an employee or job applicant, the CPPA's draft regulations focus more narrowly on technology that substantially facilitates human decision-making, defined as using the output of the technology as a "key factor" in a human's decision-making.

---

<sup>9</sup> Section 11013 (Recordkeeping) of the Proposed Modifications to Employment Regulations Regarding Automated-Decision Systems, available [here](#).

<sup>10</sup> Section 1798.145 (Exemptions) (a)(1)(A) California Consumer Privacy Act of 2018.

<sup>11</sup> Section 1798.105 CCPA.

<sup>12</sup> Section 1798.105(d)(8) CCPA.

<sup>13</sup> The CCRC's Proposed Modifications define "automated decision system" as "*a computational process that screens, evaluates, categorizes, recommends, or otherwise makes a decision or facilitates human decision making that impacts applicants or employees. An Automated Decision System may be derived from and/or use machine-learning, algorithms, statistics, and/or other data processing or artificial intelligence techniques.*" See Section 11008.1(a) of the Proposed Modifications to Employment Regulations Regarding Automated Decision Systems. On the other hand, the Draft Risk Assessment and Automated Decision-making Technology (March 2024) Regulations define "automated decision-making technology" as "*any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decision-making.*" For the purposes of this definition, to "substantially facilitate human decision-making" means using the output of the technology as a key factor in a human's decision-making. While automated decision-making technology under this definition includes profiling, it excludes the following technologies, provided that the technologies do not execute a decision, replace human decision-making, or substantially facilitate human decision-making: web hosting, domain registration, networking, caching, website-loading, data storage, firewalls, anti-virus, anti-malware, spam- and robocall-filtering, spellchecking, calculators, databases, spreadsheets, or similar technologies. See Section 7001 of the Draft Risk Assessment and Automated Decision-making Technology Regulations (March 2024).

- d. **Allocation of Responsibilities Between Businesses and Service Providers.** The CCRC’s proposed data retention requirements make no distinction between “businesses,” who under the CCPA determine the purposes and means of the personal information being retained, and “service providers,” who receive and process personal information on behalf of another business. A service provider that qualifies as an “agent” or “employment agent” under the draft CCRC rules may be required to retain data on behalf of a business.<sup>14</sup> Under the CCRC’s proposed rules, a service provider may be required to actively identify California-based workers or job applicants to determine whether their personal information must be retained, thereby accessing and copying personal information they would otherwise not handle. This would increase the privacy and data security risks associated with that data.

CIPL encourages the CCRC to address these and other privacy and data protection concerns in close coordination with the CPPA and other agencies whose remit touches on data privacy and security, and to develop and publish explanations of its decisions in these areas. We appreciate this opportunity to share our perspectives and welcome any questions that you may have about them.

---

<sup>14</sup> Section 11008(b) and (h) in conjunction with Section 11013 of the Proposed Modifications to Employment Regulations Regarding Automated Decision Systems.