

Response by the Centre for Information Policy Leadership to the Colorado Department of Law Pre-Rulemaking Request for Comments under the Automated Decision-Making Technology Act

Submitted July 13, 2026

The Centre for Information Policy Leadership (CIPL) welcomes the opportunity to respond to the Colorado Department of Law's request for input regarding its upcoming rulemaking under the Automated Decision-Making Technology Act. CIPL commends this effort to promote consumer rights, clarify ambiguities, and facilitate efficient, interoperable compliance while supporting beneficial innovation. The Automated Decision-Making Technology Act (ADMT Act) and the related rulemaking represent significant steps toward strengthening privacy protections for Colorado residents while signalling the state's efforts to shape a modern, risk-focused data governance framework.

CIPL acknowledges that the irresponsible use and application of automated decision-making technology (ADMT) can directly result in unfair discrimination, financial loss, reputational damage, and other legal and societal consequences for individuals. At the same time, ADMT facilitates great benefits for individuals, society, and businesses as digital services take on a more central role in both public and private sectors, including healthcare, education, banking, insurance and marketing. Thus, by implementing ADMT responsibly, organizations can ensure effective and appropriate protection for individuals while enabling society, individuals and businesses to reap the benefits of machine learning and other relevant technologies. Overregulating low-risk automated processing can also inadvertently cancel out the benefits of deploying ADMT and hinder innovation in Colorado by overburdening regulated organizations with compliance requirements that do not meaningfully protect consumers.

Key Recommendations:

- Align ADMT Act and related rulemaking terminology with existing Colorado law in the Colorado Privacy Act (CPA) and the CPA Rules.
- Clarify "materially influence" to mean "Solely Automated Processing" or "Human Reviewed Automated Processing", as defined in the CPA Rules.
- Clarify ambiguities related to consumer rights to promote effective compliance.

I. Adopt ADMT Act rules that align with existing Colorado law

Colorado should adopt a consistent data governance framework that does not introduce overlapping and potentially contradictory terms and definitions for data processing activities. Existing law and regulations outline useful terms and definitions that should be considered in the rulemaking process for the ADMT Act. For example, the Colorado Privacy Act (CPA) includes and defines a key concept in data protection, "Decisions that produce legal or similarly significant effects concerning a consumer" (Section 6-1-1303(10)). Additionally, the CPA Rules regulate automated decision-making involving personal data and define key terms, distinguishing between "Human Involved Automated Processing", "Human Reviewed Automated Processing", "Profiling", and "Solely Automated Processing".

Under the CPA, consumers have the right to opt-out of profiling activities that produce legal or similarly significant effects. The CPA Rules clarify that this opt-out right applies to decisions that produce legal or similarly significant effects when they are based on Solely Automated Processing or Human Reviewed Automated Processing. Further, the CPA Rules clarify that data protection assessments are mandatory for profiling based on Human Involved-, Human Reviewed-, and Solely Automated Processing. The Department should keep these obligations in mind when considering rules clarifying the ADMT Act.

II. Definitions of “materially influence” and other terms

Organizations cannot effectively implement compliance programs without clear thresholds for when obligations apply. The definition of “materially influence” in the ADMT Act is central to determining the scope of the Act. However, as currently drafted, it creates significant ambiguity and overbreadth, potentially applying to all automated processing in covered domains. The Act defines “materially influence” to include situations where an ADMT output is a “non-de minimis factor” of a consequential decision, including by constraining, ranking, scoring, recommending, or classifying how a consequential decision is made.

To ensure that the law achieves its objectives, rulemaking should clarify and narrow the “materially influence” standard by:

- Establishing objective indicators of applicability;
- Excluding any processing activities involved in consequential decisions where a human retains full decision authority; and
- Aligning with risk-based, interoperable regulatory approaches.

As drafted, it is not clear how to determine when an ADMT output constitutes a “non-de minimis factor” of a consequential decision. Thus, the definition of “materially influence” may capture routine and low-risk advisory outputs or recommendations that remain subject to meaningful human judgment. The definition of “materially influence” should be clarified to exclude consequential decisions made via “human decision-making” or “meaningful human review.” This would create operational clarity between automated decision-making that results in consequential decisions and human decision-making that is assisted by various, low-risk computational processes. This can be achieved by clarifying that “materially influence” means “Solely Automated Processing” or “Human Reviewed Automated Processing”, as defined by the CPA Rules. This clarification would establish a functional applicability threshold, namely by targeting technology that processes personal data and uses computation to replace human judgment when executing consequential decisions.

A definition that fails to distinguish between fully automated systems and those that merely inform human judgment risks obscuring the true nature of the decision and overextending regulatory requirements. Where human oversight is meaningful—such that individuals can review, challenge, or alter outcomes—the risks associated with automation may be significantly mitigated. The Department should therefore ensure that the “materially influence” concept is clearly delineated and applies only where the outputs of a system constitute a decisive or determinative factor in a consequential decision.

To the extent possible, we recommend that the Department clarify that the requirements of the ADMT Act apply to automated decisions that *produce legal or similarly significant effects concerning a consumer*. By adding “produces legal or similarly significant effects” to the definition of covered ADMT, the Department can apply the CPA’s general requirements to low-impact or low-risk ADMT

and profiling activities, but impose and enforce heightened regulatory obligations on processing activities that pose the most significant risks or harms to consumers. As written, the ADMT Act will inadvertently capture many low-risk processing activities and overburden both businesses and the Department.

Finally, the Department should provide a non-exhaustive list of examples across industries and use cases to encourage effective compliance.

III. Consumer rights, notice, and post-adverse outcome disclosure requirements

Timelines for consumer rights requests: The Department should establish timelines for consumer access, correction, and human review requests. A forty-five-day timeline for response with a forty-five day extension when reasonably necessary, as established by the CPA for consumer requests, would be appropriate.

Human review of adverse decisions: The Department should provide guidance as to what constitutes “commercially reasonable” for human review of adverse decisions, including a list of non-exhaustive examples across various industries and use cases. The Department should also consider a list of non-exhaustive factors that could influence the commercial reasonability threshold, such as the size of an organization and the volume of decisions made.

Pre-use ADMT notice requirements: The Department should clarify how the notice requirements in Sections 6-1-1704(1)-(3) apply to deployers of ADMT that are business-to-business providers and do not have a direct relationship with consumers. Many organizations rely on third-party service providers for information that informs decision-making, and in some cases third-party service providers can rely on ADMT. The Department should clarify that the pre-use ADMT notice requirements apply to deployers with direct relationships with consumers and/or final decision-making authority.

Post-adverse outcome disclosure requirements: The post-adverse outcome disclosure requirement requiring disclosure of “types, categories, and sources of personal data used” (Section 6-1-1704(3)(b)), specifically the inclusion of “sources of personal data”, could be interpreted to require deployers to reveal information that could create security vulnerabilities or expose competitively sensitive and proprietary information. The Department should clarify that “sources” means categories of sources (e.g., “credit bureau data,” “employer-provided records,” “publicly available records”).

Applicability of disclosure requirements that interact with federal law: Under Section 6-1-1704(4)(b)(IV), the Department is authorized to adopt rules clarifying post-adverse outcome disclosure requirements and their interaction with federal law. Financial institutions are already subject to extensive federal privacy and consumer protection regulations under the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA) (e.g., under the GLBA Safeguards Rule). Parallel obligations under state law are overly burdensome on organizations and do not mitigate harm to consumers. As written, the Act only exempts creditors under the FCRA from deployer disclosure requirements in Section 6-1-1704(6)(a). The Department should clarify that all organizations subject to the GLBA and FCRA are exempt from deployer disclosure requirements.

Illustrative examples: The Department should consider providing non-exhaustive illustrative examples such as model consumer notices, sample disclosures, and safe harbor provisions that organizations may use to satisfy disclosure requirements.