GOODWIN

JUNE 10, 2026

Colorado Enacts Law Repealing and Replacing Landmark Colorado AI Act

Bethany P. Withers, Gabe Maldoff, Omer Tene, Daniel Berrick

On May 14, 2026, Colorado Gov. Jared Polis signed into law SB26-189 (the Colorado ADMT Act), repealing and replacing the landmark 2024 Colorado AI Act, which, when passed, was billed as the first "comprehensive AI law" in the country. The new law followed mounting concerns over the potential overregulation of AI. These concerns — reflected in the Trump administration's efforts to preempt state AI laws, the May 2026 political agreement by EU bodies to delay implementation of the EU's AI Act, and other actions — prompted the creation of a bipartisan legislative committee in Colorado. The committee's report recommended the changes now embodied in the Colorado ADMT Act.

The Colorado ADMT Act shifts the law's focus from "artificial intelligence" to "automated decision-making technology" (ADMT) and eliminates many of the original law's procedural obligations, including requirements to conduct impact assessments and maintain a risk management framework. Nevertheless, far from gutting the protections intended by the prior law, key changes to the Act's scope and liability provisions may ultimately motivate parties to employ the very governance measures that have been stripped from the law's explicit requirements.

Specifically, the Colorado ADMT Act expands the law's application to financial services and healthcare organizations, among other regulated sectors, while clarifying that developers and deployers of regulated AI systems cannot shift responsibility for discrimination claims by contract. The Colorado ADMT Act also replaces internal governance requirements with a transparency and consumer rights regime echoing the 1970 Fair Credit Reporting Act (FCRA). To comply with these requirements — including by providing satisfactory explanations to consumers of AI-assisted decisions — and to manage legal risks, businesses will likely look to AI governance frameworks and standards to demonstrate reasonable care.

Most of the law's provisions take effect on January 1, 2027, giving companies more time to comply than the original 2024 Act, which had an implementation date of June 2026. Companies should now assess how these changes affect their obligations to ensure compliance with the new law.

Background

Stakeholders heralded the Colorado AI Act as the first comprehensive AI regulation when the state's legislature enacted it in 2024. Modeled on the EU's risk-graded AI framework (albeit with a narrower

conception of risks), the Colorado AI Act regulated “high-risk artificial intelligence systems” that serve as a “substantial factor” in “consequential decisions” affecting access to financial services, medical care, housing, jobs, and other listed services.

The law imposed different requirements on “developers,” who develop or substantially modify AI systems, than on “deployers,” who make use of such systems for consequential decisions. The law required developers to maintain, and make available to deployers, technical documentation regarding the intended uses, testing, data governance procedures, and risks associated with use of the AI system. Deployers had to notify consumers of consequential decisions, provide consumers with avenues to challenge such decisions, and maintain “reasonable care” in using such systems, which they could demonstrate by maintaining a risk management program consistent with the National Institute of Standards and Technology (NIST) AI Risk Management Framework.

The Colorado AI Act has since been joined by other state laws regulating the use of AI in important decisions — most notably, ADMT regulations under the California Consumer Privacy Act — as well as law regulating various facets of generative AI, chatbots and AI companions, deployment of AI in regulated sectors such as healthcare, and use of AI to provide therapy services, among others.

The flurry of state AI lawmaking prompted pushback from the Trump administration, which issued an executive order intended to limit state regulation of AI in order to promote AI innovation and US technological “supremacy.”

While the Trump administration’s efforts have not slowed the rate of state lawmaking on AI, the reformulation of the old Colorado AI Act as the new Colorado ADMT Act is part of a shift in the regulatory climate around AI — both within and outside the United States — toward tightly focused regulation targeting specific identified AI harms and away from more sprawling “comprehensive” frameworks. At the same time, the Colorado ADMT Act is far from a deregulatory measure. By clarifying its focus on key industries in which AI-assisted decisions pose the greatest risk, and by imposing transparency and individual rights requirements upon a wider range of actors and activities in those industries, the new law is likely to have a direct and visible impact for both AI developers and deployers across the country.

Who and What Is in Scope

The Colorado ADMT Act applies to “covered ADMT” that is used to “materially influence” certain “consequential decisions” affecting educational enrollment or opportunity, employment, residential real estate, financial or lending services, insurance, healthcare, or essential government services and public benefits.

The original law included exemptions for certain federally regulated sectors, such as financial services and healthcare. These exemptions had created significant ambiguity, and the amended law removes them. While the Colorado AI Act focused on consequential decisions such as AI-assisted decisions affecting access to financial or healthcare services, it also exempted many of the entities that use AI technologies to make decisions in those environments, deferring to sector-specific federal legislation such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, and the FCRA.

The amendments address these contradictions by striking exemptions for banks, credit unions, and entities developing or deploying systems in compliance with federal agency standards, as well as by narrowing exemptions for healthcare organizations regulated by HIPAA.

The amended law also shifts the focus from "AI systems" to "ADMT," broadening the law's reach to encompass a wider range of digital technologies, including systems that may be less sophisticated than modern AI. Other notable changes to the scope of regulated systems include:

- The amended law clarifies, and may even lower, the threshold for an ADMT's involvement in a "consequential decision" to trigger regulation. Specifically, under the amended law, ADMT is regulated where it is used to "materially influence" a consequential decision, where "materially influence" is defined as an output that is "a *non-de minimis factor* that is used in making a consequential decision" (emphasis added). This non-de minimis standard replaces the previous "substantial factor" standard, which likely set a higher bar.
- The amended law defines the concept of a "consequential decision" as a decision that " *relates to* (i) the provision of or a consumer's access to, eligibility for, selection for, or compensation for a covered domain; or (ii) a decision, determination, or action about a consumer that relates to a differentiated price, cost sharing, compensation, or other material terms in a manner that is reasonably likely to materially limit, delay, effectively deny, or otherwise fundamentally alter the consumer's access, eligibility, or opportunity for a covered domain" (emphasis added). The phrase "relates to" replaces the previous requirement that the decision have a "material legal or similarly significant effect" on access, eligibility, or opportunity for a covered domain. Notably, the amended law also excludes "legal services" from the list of covered domains and limits the kinds of housing decisions it addresses to those concerning "the lease or purchase of residential real estate in Colorado." This amendment too will likely lower the threshold for regulatory oversight.
- The amended law expands exemptions for certain AI technologies that have become ubiquitous. For example, it clearly exempts AI-assisted decisions concerning advertising and marketing, summarization and translation tools that "present information for human review or administrative processing," and consumer-facing chatbots, subject to an "acceptable use policy that prohibits generated content to be used in a consequential decision." The exemptions add to the list of technologies that were exempt from the previous law, including antivirus, anti-spam, and other cybersecurity tools, as well as hosting, web caching, data storage, and simple spreadsheets.

A New Focus on External Notice and Consumer Rights

The Colorado ADMT Act retains the previous law's distinction between "developers," who develop, offer, sell, license, or otherwise make commercially available a covered ADMT, and "deployers," who "deploy" a covered ADMT.

The most significant change in the amended law is a shift away from internal governance requirements toward a regulatory model focused on consumer notice and rights. While implementing these external-facing requirements will require businesses to develop appropriate internal policies and procedures, the removal of explicit governance mandates gives them greater flexibility in how they address the law's requirements.

The Colorado ADMT Act imposes streamlined obligations on developers, focused on transparency and documentation for compliance purposes. Neither developers nor deployers are subject to an explicit duty of care, and they are not required to publish a public website statement or report discovered discrimination to the attorney general. The Colorado ADMT Act also relieves deployers of their requirements regarding risk management policies and programs, AI interaction disclosures, and impact assessments.

Key Requirements for "Developers"

Under the amended law, developers must:

- Provide certain disclosures to deployers concerning the covered ADMT. This needs to be a "general statement" that describes the intended uses of the system and any known harmful or inappropriate uses. The disclosures must also describe the categories of data used to train the system, any known limitations or risks of the system, and instructions for appropriate use (including human review, where applicable).
- Provide deployers with information necessary for the deployer to comply with its disclosure obligations, which may include information about how the developer assists the deployer with facilitating consumer rights.
- Provide separate notices to deployers, within a reasonable amount of time, for material updates, intentional and substantial modifications, and changes to the intended use of, limitations for, or risk mitigation for the covered ADMT.
- Adhere to recordkeeping requirements for at least three years in order to demonstrate compliance with the law.

The amended law removes express internal procedural requirements, which will give developers flexibility in how they implement programs to review, test, and document the limitations and risks inherent in covered ADMT in order to support these disclosures.

Key Requirements for "Deployers"

Under the new law, deployers must engage in record retention for compliance and provide a pre-deployment use statement, an explanation of consumer rights, and an adverse decision notice. Specifically, they must:

- Provide consumers a notice indicating the use of covered ADMT and how consumers can acquire more information about it, although the amount of information that must be disclosed is less than what the Colorado AI Act required.
- Provide consumers an adverse decision notice if the deployer uses a covered ADMT to materially influence a consequential decision that has this outcome. The notice must contain certain details, such as a description of the decision, the ADMT's role in reaching it, and instructions on how to request more information about the system and its inputs.
- Provide consumers with an explanation of their rights in the event of an adverse decision and details on how to exercise them. The law empowers the state attorney general to promulgate regulations that further specify the content of adverse decision notices.
- Retain records containing certain information for at least three years for compliance demonstration

purposes.

While the amended law removes the previous requirement on deployers to conduct a risk assessment, such an assessment may be required by other laws – such as the Colorado Privacy Act, where applicable – and some deployers may find such an assessment to be necessary to confirm that the covered ADMT does not introduce unreasonable risks of error, discrimination, or bias.

Spreading Responsibility for Discrimination Claims

The Colorado ADMT Act is enforced primarily by the state attorney general, and the law does not provide a private right of action. In place of the affirmative defenses available under the old law, developers and deployers now have a 60-day cure period after the attorney general notifies them of a violation. However, the attorney general may seek penalties or other relief without providing this notice if they demonstrate that a developer or deployer knowingly or repeatedly violated the law. Courts may consider successful cures as a mitigating factor when determining civil penalties or other monetary relief.

Most significantly, while the law does not create an independent basis for private claims, it allocates liability between developers and deployers for claims under anti-discrimination laws based on relative fault. Developers are liable if the ADMT was used as intended and materially influenced the consequential decision giving rise to the discrimination claim. Deployers are responsible for their ADMT-influenced consequential decisions, as well as for decisions derived from unintended uses of the ADMT. The law rules out joint and several liability and voids indemnification clauses as against public policy.

By prohibiting contractual risk shifting, the Colorado ADMT Act may motivate both developers and deployers to undertake testing of their ADMT systems and develop internal governance processes — indeed, the very same measures that were removed from the language of the Colorado AI Act — to prove that they have taken reasonable care to avoid discrimination. This change will also encourage developers to clearly define the intended uses of covered ADMT within customer contracts to reduce potential exposure for discrimination resulting from deployers' use of such systems in ways the developer had not intended or tested.

Conclusion

The Colorado ADMT Act comes at a time when US states have been focused on regulating various kinds of AI technologies, including chatbots and data-driven pricing algorithms. Colorado's amendments draw attention to a law that was once seen as a prototype for comprehensive AI legislation in other states. More than a regulatory rollback, the Colorado ADMT Act represents a pivot from an accountability-centered framework to one grounded in transparency and individual rights. Because the Colorado ADMT Act covers numerous domains and retains its developer/deployer framework, it will continue to have more industry-wide implications than more targeted legislation in other states (e.g., the amendment to the Illinois Human Rights Act, which prohibits the use of AI in employment contexts when it results in illegal discrimination).

Most of the Colorado ADMT Act's provisions take effect on January 1, 2027. Organizations that offer or use these AI technologies should evaluate how the Colorado ADMT Act affects their compliance obligations and how it fits within the broader landscape of similar laws, such as California's ADMT regulations.

CONTACTS

Bethany P. Withers
Partner
Technology
bwithers@goodwinlaw.com

Gabe Maldoff
Partner
Data, Privacy & Cybersecurity
gmaldoff@goodwinlaw.com

Omer Tene
Partner
Technology
otene@goodwinlaw.com

Daniel Berrick
Associate
Data, Privacy & Cybersecurity