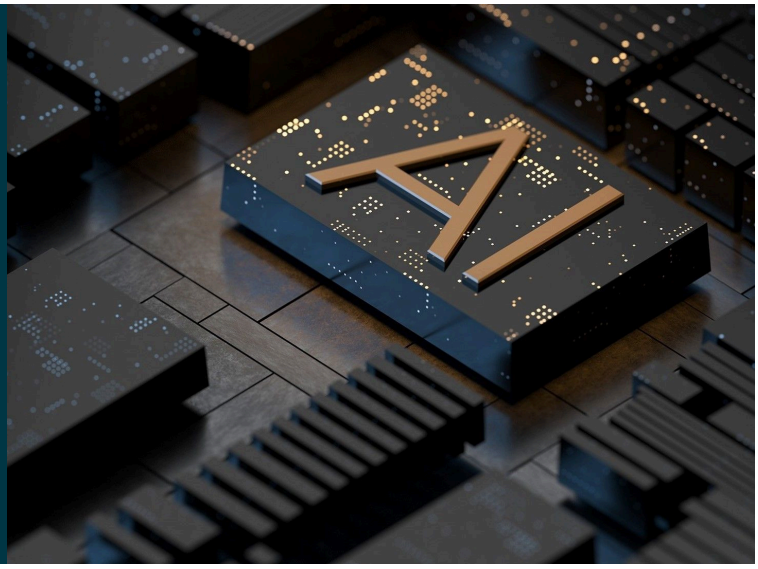
WILSON SONSINI

Colorado Legislature Repeals and Replaces Colorado AI Act: What SB 189 Means for Your Business



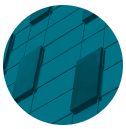
CONTRIBUTORS


Maneesha Mithal


Tracy Shapiro


Hale Melnick


Doo Lee


Kimia Favagehi

ALERTS

May 19, 2026

On May 14, 2026, Colorado Governor Jared Polis signed SB 189 into law, which repeals and replaces the Colorado Artificial Intelligence Act (CAIA). SB 189 goes into effect on January 1, 2027.

Key Takeaways

- SB 189 pivots away from the CAIA's focus on artificial intelligence (AI) governance and algorithmic discrimination and instead provides for a transparency-based framework focused on developer and deployer disclosures and documentation.
- SB 189 applies to covered automated decision-making technology (ADMT) that is used to make or materially influence consequential decisions.
- The bill applies to developers and deployers that do business in Colorado, with some exceptions.
- Similar to the CAIA, SB 189 does not provide a private right of action but grants the Colorado Attorney General (AG) with enforcement and rulemaking authority.
- Consumers are granted the rights to access, correction, and meaningful human review and reconsideration of adverse outcomes resulting from consequential decisions materially influenced by ADMT.
- Consumers are not provided a right to opt out of the use of ADMT.

Background

Two years ago, on May 17, 2024, Governor Polis signed the CAIA into law. The CAIA regulated the development, deployment, and use of AI systems and imposed significant obligations on developers and deployers of high-risk AI systems used in making consequential decisions, including duty of care, risk and impact assessments, and AG notices, among other obligations.

Shortly after it was signed into law, however, the CAIA received criticism both from local business groups and consumer watchdog advocates. As a result, Governor Polis convened the Colorado AI Policy Work Group (AI Work Group) to assess policy-based solutions to criticism that the law was overly broad and stifled innovation, on the one hand, while weakening protections, on the other. The CAIA was also the subject of litigation in which the U.S. Department of Justice intervened, alleging that it violated the Equal Protection Clause of the Fourteenth Amendment. The Work Group ultimately released a new framework on March 17, 2026, and the Colorado legislature introduced SB 189 shortly thereafter, closely mirroring the efforts of Governor Polis' AI Work Group.

On May 14, 2026, the Governor signed SB 189 into law, which now repeals and replaces the CAIA with a narrower framework focused on covered ADMT that makes or materially influences consequential decisions.

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.

Key Differences between the CAIA and SB 189

Whereas the CAIA would have required developers and deployers of high-risk AI systems to conduct risk and impact assessments, annual reviews, and discrimination reporting to regulators, SB 189 shifts to more transparency- and disclosure-based requirements for ADMTs that make or materially influence consequential decisions.

More specifically, the CAIA imposed on developers various disclosure obligations, both to deployers and to the AG. Under SB 189, however, developers are only required to provide notice about covered ADMTs to deployers. Deployers continue to bear most of the obligations under SB 189, but a few things have changed. For example, deployers are no longer required to conduct annual impact assessments and they are no longer required to implement risk management programs. SB 189 also introduces some new requirements for both developers and deployers (described in more detail below), such as a three-year recordkeeping obligation for certain documentation.

Scope

To Whom Does SB 189 Apply?

SB 189 applies to developers and deployers of "covered ADMT," defined as "**automated decision-making technology** that is used to **materially influence** a **consequential decision**" about a Colorado consumer. Determining whether an entity has developed or deployed a "covered ADMT" is one of the more challenging aspects of the law.

- "**Automated Decision-making technology**" is defined to mean "a technology that processes personal data and uses computation to generate output, including predictions, recommendations, classifications, rankings, scores, or other information that is used to make, guide, or assist a decision, judgment, or determination concerning an individual." It specifically excludes certain technologies, such as anti-malware and calculators.
- "**Materially influence**" is defined vaguely to mean: "(I) An ADMT Output is a non-de minimis factor that is used in making a consequential decision; and (II) An ADMT output affects the outcome of a consequential decision, including by constraining, ranking, scoring, recommending, classifying, or otherwise meaningfully altering how a consequential decision is made." On first impression, "materially influence" appears to be a limiting factor, but then is defined so broadly that this qualifier could potentially be rendered functionally meaningless. We may receive additional guidance before the law takes effect, as the bill permits (although does not require) the AG to issue a rule to "clarify the application" of the term, "including presumptions, illustrative examples, and objective indicators."
- "**Consequential decision**" is defined to mean any decision about a consumer relating to access, eligibility, or compensation in one of the following covered domains: 1) education; 2) employment; 3) real estate; 4) financial and lending services; 5) insurance; 6) healthcare; and 7) essential government services and public benefits. Also covered is a decision that relates to differentiated pricing that materially limits or delays a consumer's access to such covered domains. Certain activities are explicitly carved out of the definition, such as low-stakes or routine business processes for customer service triage and workflow management, just to name a few.

SB 189 defines "consumer" based on the definition found in the Colorado Privacy Act, but goes one step further and extends the definition to also include employees and job applicants who are Colorado residents and any individual whose access to, eligibility for, or opportunity in Colorado is evaluated in a consequential decision by a person doing business in Colorado.

An entity's obligations with regard to a covered ADMT will vary depending on whether it is a "developer" or "deployer" of the ADMT.

- A "developer" is "a person doing business in Colorado that develops, offers, sells, leases, licenses, or otherwise makes commercially available a covered ADMT; develops a component that is designed, marketed, intended, documented, advertised, configured, or contracted to be used as part of a covered ADMT; or intentionally and substantially modifies[1] an ADMT such that it becomes a covered ADMT (subject to certain exceptions).
- A "deployer" is defined, in a circular fashion, as "a person doing business in Colorado that deploys a covered ADMT." SB 189 does not define "deploy," but the CAIA defined it to mean "to use a high-risk AI system." (Note that the CAIA generally regulated "high-risk AI systems," whereas SB 189 regulates "covered ADMTs.") SB 189's use of the term "deploy" suggests that it is similarly intended to mean a person that "uses" a covered ADMT.

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.

Developer Obligations under SB 189

Developers must provide deployers with the following disclosures when the developer creates a covered ADMT that is marketed, advertised, configured, or contracted to be used to make consequential decisions *or* when the developer becomes aware that the covered ADMT is being used to make consequential decisions in a manner consistent with the intended and contracted uses.

- a general statement describing the intended uses and known harmful or inappropriate uses of the covered ADMT;
- a description of the categories of data, including personal data, used to train the covered ADMT, to the extent known;
- the known limitations of the covered ADMT, including known risks and circumstances in which the ADMT should not be used;
- instructions for the deployer's appropriate use, monitoring, and meaningful human review; and
- information reasonably necessary for the deployer to comply with its obligations, including notifying the deployer if any information is withheld.

Additionally, developers are required to provide, within a reasonable time, notice to deployers of any material updates, intentional and substantial modifications, and changes to the intended use of, limitations for, or risk mitigation for the covered ADMT.

Deployer Obligations under SB 189

Deployers have the following obligations under SB 189:

Pre-Use Notice. Prior to using an ADMT to materially influence a consequential decision, deployers must provide a clear and conspicuous notice that the deployer will use an ADMT in a consequential decision affecting them, along with instructions for obtaining additional information. Deployers may comply with the notice requirement by maintaining a prominent, reasonably accessible public notice at points of consumer interaction, such as a link or posting close to the interaction where a consequential decision may occur.

Adverse Outcome Notice. If a deployer's covered ADMT materially influences a consequential decision that results in an adverse outcome for the consumer, the deployer must, within 30 days, provide a plain-language explanation of the decision and the ADMT's role, instructions for requesting additional information about the covered ADMT and its inputs, and an explanation of the consumer's related rights.

The bill defines "adverse outcome" to mean either: "(a) a decision that denies, terminates, revokes, or materially reduces or restricts a consumer's access to, eligibility for, selection for, compensation for, or the provision of an opportunity or service; or (b) a decision that results in materially less favorable differentiated price, cost, compensation, or other material terms that are reasonably likely to materially limit, delay, or effectively deny, or otherwise fundamentally alter, a consumer's access to, eligibility for, selection for, compensation for, or the provision of an opportunity or service compared to terms offered to similarly situated consumers." The bill explains that "if a decision outcome imposes materially less favorable differentiated pricing or terms, the decision outcome materially influences price, cost sharing, compensation, or material terms."

Consumer Rights

Similar to the California Consumer Privacy Act's ADMT regulations, SB 189 requires deployers to provide a set of consumer rights focused on consequential decisions and adverse outcomes, and authorizes the AG to adopt necessary rules clarifying the requirements. When a consequential decision that is materially influenced by ADMT results in an adverse outcome for a consumer, the consumer may request and the deployer must provide 1) instructions for requesting personal data and correcting factually or materially inaccurate personal data used in a consequential decision; and 2) a commercially reasonable opportunity for "meaningful human review"[2] and reconsideration.

Recordkeeping Requirements

SB 189 introduces recordkeeping obligations, and requires both developers and deployers to retain records and documentation demonstrating compliance for at least three years. For example, SB 189 explains developers and deployers must retain ADMT version identifiers, changelogs, and documentation of material updates as part of its recordkeeping compliance requirement.

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.

Exemptions and Compliance with Other Laws

Certain entities that are subject to the obligations of other laws, such as some HIPAA-covered entities, Colorado insurers, some FDA-regulated entities, creditors, and schools are exempt from the requirements of SB 189 to the extent the entities comply with their other legal obligations.

Rulemaking

SB 189 directs the AG to adopt, by January 1, 2027, rules clarifying the requirements for post-adverse outcome notices—which may include clarification around content, sector-specific guidance, consumer-friendly explanations, and interactions with other laws—to ensure consumers receive meaningful information about adverse outcomes. The AG may also adopt other rules as necessary, such as to clarify the definition of "materially influence" (including presumptions, illustrative examples, and objective indicators), but in so doing, the AG must utilize a process that meaningfully engages with interested stakeholders. With a compliance deadline of January 1, 2027, companies may find themselves with very little time to address compliance with the rules.

Enforcement

The AG is authorized to enforce SB 189 through the Colorado Consumer Protection Act, and any violation is deemed to be a deceptive trade practice. Prior to initiating an action, the AG must provide a 60-day notice and opportunity to cure if a cure is possible, except for knowing or repeated violations. There is no private right of action. SB 189 allocates liability between developers and deployers in civil discrimination actions based on relative fault. Developers are liable only to the extent that the ADMT was used as intended, documented, marketed, advertised, configured, or contracted for by the developer and the ADMT materially influenced the consequential decision that gave rise to the violation of law.

Deployers are responsible for their own independent decisions, including using AI in ways the developer did not intend or authorize. SB 189 states there is no joint and several liability unless permitted by existing law, and liability-shifting clauses are void as against public policy, with exceptions.

Looking Ahead

SB 189 goes into effect on January 1, 2027.

Interestingly enough, Colorado is not alone in undergoing changes to AI regulations. We recently reported in another client alert that, on May 7, 2026, EU legislators reached a political agreement to amend the EU Artificial Intelligence Act with significant implications for AI companies operating in the EU.

Wilson Sonsini routinely helps companies navigate complex privacy and data security issues and monitors AG guidance, enforcement, and litigation involving AI legislation to stay current on compliance issues. For more information or advice concerning your AI compliance efforts, please contact Maneesha Mithal, Tracy Shapiro, Hale Melnick, Doo Lee, Kimia Favagehi or any member of the firm's Data, Privacy, and Cybersecurity practice.

---

[1]"Intentional and substantial modification" means "a deliberate change made to an ADMT that results in a material change to the system's intended, documented, advertised, configured, or contracted use."

[2]"Meaningful human review" means "review by a[n] individual designated by the deployer who has authority to approve, modify, or override a consequential decision and who: a) considers relevant, available primary evidence; b) is trained to conduct the review; c) does not default to the system output; and d) has access to sufficient information to understand: (i) the output's: a) intended use; b) material limitations; and c) categories of inputs; and (ii) the principal factors used to generate the output, without requiring disclosure of proprietary source code, model weights, or other trade secrets."

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.