FYI®
For Your Information®

Colorado enacts law regulating use of AI in employment

Volume 47

Issue 18

June 12, 2024

Authors
Nancy Vary, JD
Abe Dubin, JD

Signed into law on May 17, Senate Bill 24-205 imposes stringent requirements on employers using AI to prevent algorithmic discrimination. Slated to take effect on February 1, 2026, the new law will require employers using "high-risk" AI systems to implement risk management policies and programs, conduct impact assessments, and provide certain notices and disclosures.

Background

On May 17, 2024, Colorado Governor Jared Polis signed into law Senate Bill 24-205 ("SB205"), "Concerning Consumer Protections in Interactions with Artificial Intelligence Systems," making Colorado the first state in the U.S. to enact a broad-based regulatory framework for the development and use of artificial intelligence (AI) systems. The new law, which will take effect on February 1, 2026, seeks to regulate the growing use of AI and algorithmic decision tools (such as resume and job candidate screening software) to prevent automated discrimination in employment-related and other matters.

New obligations for developers and users of AI

SB205 generally requires developers of "high-risk" AI systems and the businesses that use them ("deployers") to take extensive measures to avoid algorithmic discrimination — a use of AI that results in "unlawful differential treatment or impact" based on a protected classification such as age, race, sex or religion. AI systems subject to the new law include any machine-based system that infers from the inputs it receives how to generate outputs, including content, decisions, predictions, or recommendations. Any AI system that is a substantial factor in making consequential decisions (e.g., providing or denying employment or employment opportunities) when deployed qualifies as "high-risk."

The new law provides limited exceptions for small businesses and certain AI tools. Businesses that employ less than 50 full-time equivalent employees may qualify for an exemption from the new law's risk management and impact assessment requirements if they: (1) use the high-risk AI system for the intended uses; (2) make impact assessments available to Colorado residents; and (3) do not train AI using their own data. Additionally, some technologies that utilize AI — including technologies used in cybersecurity, identity management, and daily business operations — may be excluded from being classified as high-risk under certain conditions.

While the developers of high-risk AI systems and the employers that use them each have a duty to avoid algorithmic discrimination, the new law imposes differing compliance obligations which are summarized below.

Requirements for developers

Developers of high-risk AI systems will have to use "reasonable care" to protect against known or reasonably foreseeable risks of algorithmic discrimination arising from the intended and contracted uses of the system. There is a rebuttable presumption that a developer used reasonable care if it complies with the following risk documentation, impact assessment and disclosure requirements and any additional rules promulgated by the state Attorney General.

Risk documentation

Developers of high-risk AI systems will be required to make available to deployers or other developers the reasonably foreseeable uses and known harmful or inappropriate uses of the system and documentation disclosing:

- High-level summaries of the type of training data, system's purpose and uses, limitations, and intended benefits, and any other information needed by the deployer to comply with the new law's requirement.

- Performance evaluations and mitigation of discrimination for the system completed prior to its release, training data, how examinations were conducted for data suitability, possible bias and mitigation, intended system outputs, steps taken to mitigate risks of algorithmic discrimination, how the system should or should not be used, and how it should be monitored.

- Additional documents reasonably necessary for the deployer to understand the system's output and monitor for risk of algorithmic discrimination.

Impact assessment information

Developers will be required to make available to a deployer or other developer documentation and information necessary to complete impact assessments of the system (such as model or dataset cards) and to post certain information to their website or in a public use case inventory including:

- Types of high-risk AI systems it has developed or intentionally and substantially modified, and currently makes available to deployers or other developers.

- Management of potential algorithmic discrimination risks from the development or intentional and substantial modification of the types of high-risk AI systems the developer posts to their website.

Risk disclosure
Developers of a high-risk AI system will be required to disclose to all known deployers or other developers and to the state Attorney General any known or reasonably foreseeable risks of algorithmic discrimination resulting from the intended uses of the system. Additional disclosures must be made no later than 90 days after: (1) the developer's ongoing testing uncovers that the high-risk AI system has been deployed and has caused or is reasonably likely to have caused algorithmic discrimination; or (2) the developer receives a credible report from a deployer that the high-risk AI system has been deployed and has caused algorithmic discrimination.

Requirements for deployers

Like developers, deployers of a high-risk AI system must also use "reasonable care" to protect against known or reasonably foreseeable risks of algorithmic discrimination. There is a rebuttable presumption that a deployer used reasonable care if it complies with the following risk management, impact assessment, notice and disclosure requirements, and any additional rules promulgated by the state Attorney General.

Risk management
Deployers of high-risk AI systems will be required to implement a risk management policy and program that includes the principles, processes and personnel used to document and mitigate the known and foreseeable risks of algorithmic discrimination. The policy and program, which must be regularly reviewed and updated, must be reasonable in light of the following:

- The latest AI Risk Management Framework (RMF) guidance from the National Institute of Standards and Technology (NIST), or RMF designated by the state Attorney General.
- The deployer's size and complexity.
- The nature and scope of the high-risk AI systems deployed and their intended uses.
- The sensitivity and volume of data processed in connection with those systems.

Impact assessments
Deployers of high-risk AI systems, or their third-party contractors, will be required to complete an impact assessment at least annually to ensure the deployed systems are not causing algorithmic discrimination. Impact assessments must include the following:

- Purpose, intended uses, deployment context and benefits of the system;

- Known or reasonably foreseeable risks of algorithmic discrimination posed by the system's deployment, along with mitigating steps taken;
- Categories of data processed as inputs, as well as the outputs;
- Whether the deployer used data to customize the system, and the categories of data used;
- Performance evaluation metrics and known limitations of the system;
- Transparency measures taken, including disclosures to Colorado residents when the system is in use; and
- Post-deployment monitoring and user safeguards, including the deployer's system oversight, use and learning process.

Additional assessments will be required within 90 days after any intentional and substantial system changes that lead to new risks of algorithmic discrimination. Deployers will have to maintain their most recently completed impact assessment, all records for each impact assessment and all prior impact assessments for at least three years after the final deployment of the high-risk AI system.

Notices

When a high-risk AI system makes, or is a substantial factor in making a consequential employment decision, deployers will have to notify employees and applicants of:

- The deployment of a high-risk AI system to make, or to be a substantial factor in making, a consequential decision before the decision is made.
- The purpose of the high-risk AI system, nature of the consequential decision, deployer's contact information, a description of the high-risk AI system and instructions for accessing more information on the deployer's website.
- The right to opt out of the processing of certain personal data.

In the event of an adverse decision, the deployer will have to: (1) notify the employee or applicant of the principal reason(s) for the decision, (2) allow them to correct any incorrect personal data the system processed in making the decision, and (3) provide an opportunity to challenge the decision and, if technically feasible, seek human review.

Additionally, deployers will have to publish summary information on their websites on the types of high-risk AI systems they deploy, how they manage associated known or reasonably foreseeable risks of algorithmic discrimination, and the nature, source and extent of the information they collect and use.

Additional disclosures
A deployer of a high-risk AI system will be required to report to the state Attorney General any algorithmic discrimination it discovers within 90 days. The Attorney General may also request deployers or their third-party contractor to disclose their risk management policy, completed impact assessment or required records for impact assessments within 90 days.

Enforcement
Violations of the new law's requirements will be enforced by Colorado's Attorney General as unfair and deceptive trade practices. While the new law imposes significant compliance burdens, it also provides an affirmative defense to developers and deployers that: (1) find and cure violations using feedback from deployers or users, adversarial testing or red teaming, or an internal review process; and (2) are in compliance with the latest NIST AI RMF, another substantially equivalent nationally recognized RMF, or an RMF designated by the state Attorney General.

In closing

Colorado employers that use — or are considering using — AI should begin to consider what, if any, steps they will have to take to ensure that the necessary AI governance programs and risk management policies and processes are in place when the new law takes effect in 2026.

Produced by the Compliance Consulting Practice

The Compliance Consulting Practice is responsible for national multi-practice compliance consulting, analysis and publications, government relations, research, training, and knowledge management. For more information, please contact your account executive.