KPMG

Regulatory Alert

Regulatory Insights

June 2024

AI Regulation: Colorado Artificial Intelligence Act (CAIA)

KPMG Insights:

- ***Consumer Protection Focus:*** *The Colorado AI law imposes obligations on both developers and deployers of "high-risk AI systems" to mitigate the risk of "algorithmic discrimination" and consumer harm across numerous sectors, including financial services, insurance, and healthcare.*
- ***Core AI Principles:*** *The new law follows core principles from the NIST AI Risk Management Framework, including guidance and standards related to design, development, deployment, and testing, and also aligns with the EU AI Act's focus on "high-risk AI systems" and their relationship to "consequential decisions".*
- ***Near-term Implementation:*** *Compliance for developers and deployers is required beginning February 1, 2026, providing only eighteen-months to implement operational, risk management, and compliance changes.*
- ***More State AI Regulation:*** *Colorado has actively pursued AI-related legislation/regulation (see Colorado Division of Insurance regulation here). Expect continued (but likely differing/nuanced) AI-related legislative and regulatory activity across many states.*

The State of Colorado recently enacted S.B. 24-205, commonly referred to as the Colorado Artificial Intelligence Act (CAIA). This new law, which takes effect February 1, 2026, is directed to persons conducting business in Colorado as "developers" or "deployers" of "high-risk artificial intelligence systems" (all as defined in the law) in such areas as employment, housing, financial services, insurance and healthcare. "Developers" and "deployers" must meet certain obligations, including disclosures, risk management practices, and consumer protections.

Key provisions of the CAIA include:

1. Applicability
2. Obligations for Developers
3. Obligations for Deployers

1. Applicability

The CAIA is intended to protect consumers (defined as Colorado residents) from potential discrimination from the use of a "high-risk artificial intelligence system", defined as an AI system that makes, or is a substantial factor in making, a "consequential decision" concerning a consumer.

A "consequential decision" is defined as a "decision that has a material legal or similar significant effect on the provision or denial to any consumer of, or the cost of terms of":

- Education enrollment or an education opportunity.
- Employment or an employment opportunity.
- Financial or lending service.
- An essential government service.
- Health Care services.
- Housing.
- Insurance.
- Legal service.

The CAIA is directed toward persons doing business in Colorado as "developers" (defined as persons that develop or intentionally and substantially modify an AI system) and "deployers" (defined as persons that

deploy a high-risk AI system). Compliance is required beginning February 1, 2026.

2. Obligations for Developers

Developers of "high-risk artificial intelligence systems" are required to:

- Use "reasonable care" to protect consumers from "known or reasonably foreseeable" risks of "algorithmic discrimination" stemming from the intended and contracted uses of high-risk AI systems.
  - "Algorithmic discrimination" means any condition in which the use of an AI system results in an unlawful differential treatment or impact that disfavors an individual or group on the basis of their actual or perceived age, color, disability, ethnicity, genetic information, limited proficiency in the English Language, national origin, race, religion, reproductive health, sex, veteran status, or other classification protected under the laws of the state or federal law.
- Make available to deployers or other developers of the high-risk AI system:
  - A general statement describing foreseeable uses or known harmful uses of the system.
  - Documentation disclosing information including the purpose and uses of the high-risk AI system, training data/data governance, limitations, and discrimination risk mitigation.
- Make available on the developer's website or in a public use case inventory, a clear and readily available statement summarizing:
  - The type(s) of high-risk AI systems the developer has developed or intentionally and substantially modified.
  - How the developer manages known or reasonably foreseeable risks of algorithmic discrimination.
- Disclose to the Attorney General, and to all known deployers or other developers, any "known or reasonably foreseeable" risks of algorithmic discrimination arising from the intended use of the high-risk AI system discovered through the developer's ongoing testing or through a "credible report" from a deployer.

3. Obligations for Deployers

Similar to the obligations of developers, deployers of "high-risk artificial intelligence systems" are required to use "reasonable care" to protect consumers from any "known or reasonably foreseeable" risks of algorithmic discrimination. The CAIA further requires deployers to:

- Implement a risk management policy and program to govern the deployment of the high-risk artificial intelligence system.
  - The law states the policy and program must be "reasonable" considering the guidance and standards in the "Artificial Intelligence Risk Management Framework" published by the National Institute of Standards and Technology (NIST) or another nationally or internationally recognized risk management framework for AI systems.
- Complete and update, at least annually, and within 90 days of any intentional and substantial modification, an impact assessment that includes the: purpose; intended use cases; known or foreseeable risks; known limitations; data inputs and outputs; performance metrics; and transparency measures.
  - Maintain records of impact assessments for at least three years following the final deployment of the high-risk AI system.
  - Conduct annual reviews of each deployed high-risk AI system "to ensure that the high-risk artificial intelligence system is not causing algorithmic discrimination."
- Provide notifications to consumers, including:
  - The deployment of a high-risk AI system to make "consequential decisions" regarding the consumer before the decision is made.
  - The purpose of the "high-risk artificial intelligence system" and the nature of the "consequential decision".
  - Certain opt-out rights.
  - In the event of an adverse decision, a statement of the reasons for the adverse decision; an opportunity to correct any incorrect personal data that the high-risk artificial intelligence system processed to make, or was a substantial factor in making, the "consequential decision"; and an opportunity to appeal.
  - Disclose to the Attorney General, the discovery of algorithmic discrimination within 90 days of discovery, as well as the implemented risk management policy.

Exemptions. Certain exemptions are provided for deployers that employ fewer than 50 full-time equivalent employees and i) do not employ their own data to train the system (and the system continues to learn from sources other than the deployers' data), ii) use the

system as intended by the developer, and iii) make available any impact assessment provided by the developer. Additional exemptions are provided for certain insurers and banks and credit unions.

Enforcement. A violation of the CAIA constitutes an unfair or deceptive trade practice under Colorado law and is enforceable by the Colorado Attorney General.

See Related KPMG Thought Leadership

- AI Regulations: Present and Future
- The Empowerment of State Law and Regulation

For more information, please contact Amy Matsuo or Bryan McGowan .

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com