HOGAN LOVELLS
CADWALADER

Insights and Analysis

U.S. State AI laws v. EU AI Act: key differences and implications for AI agreements

03 August 2026

Businesses are navigating a rapidly evolving, increasingly complex regulatory landscape that should be considered when providing or using artificial intelligence (AI) technologies in the United States and abroad.

In the European Union (EU), the EU AI Act serves as a uniform regulatory framework governing the provision and use of "AI systems" (meaning, for purposes of the EU AI Act, machine-based systems that infer how to generate outputs from received inputs) – and, in certain circumstances, outputs generated by those systems – in the EU. By contrast, the United States has no comparable federal AI framework, leaving businesses providing or using AI systems in the United States to contend with a patchwork of state-level AI laws that impose differing obligations depending on where and how an AI system is provided or used.

This article (i) highlights key differences between the EU AI Act and the emerging landscape of U.S. state-level AI laws concerning AI systems (and, in some cases, the outputs generated by those systems) and (ii) discusses how those structural differences directly influence how businesses should

consider negotiating agreements for the provision and use of AI systems and outputs, including with respect to allocation of compliance responsibilities and regulatory risk. For the sake of providing clear comparisons, this article does not discuss the EU AI Act's requirements for general-purpose AI models (i.e., general foundational models that perform a wide range of distinct tasks and can be integrated into downstream systems), which are regulated separately from AI systems under the EU AI Act.

Certain Key Differences between U.S. State AI Laws and the EU AI Act

This section provides a non-exhaustive summary of key differences between U.S. state AI laws and the EU AI Act that are particularly relevant when negotiating agreements for the provision and use of AI systems.

1. EU AI Act

The EU AI Act establishes a single EU-wide regulatory framework governing the provision and use of AI systems – and, in certain circumstances, outputs generated by those systems – in the EU. A defining feature of the EU AI Act is its risk-based structure, which categorizes AI systems into one of four tiers (prohibited, high-risk, limited-risk, or minimal-risk) and imposes obligations tied to the corresponding risk level. High-risk AI systems, such as those intended for use in employment, education, or critical infrastructure contexts, are subject to extensive requirements relating to risk management, data governance, technical documentation, recordkeeping, and human oversight.

The EU AI Act also establishes a standardized allocation of compliance responsibilities corresponding to four categories of regulated actors:

i. “providers” (defined as entities that develop AI systems and provide them to others or, subject to certain exceptions, use them internally in the EU, regardless of whether the entity is located inside or outside the EU);

ii. “deployers” (defined as entities that use AI systems, other than for “personal, non-professional activities”);

iii. “importers” (defined as entities established or located in the EU that provide AI systems branded under the name of a non-EU provider); and

iv. “distributors” (defined as entities that provide AI systems in the EU, other than providers or importers).

The EU AI Act also applies to providers and deployers located outside the EU when outputs generated by their AI systems are used in the EU. The EU AI Act assigns a distinct set of compliance obligations to each of these four roles, with the scope of those obligations determined by the AI system’s risk classification. For example, for high-risk AI systems: (i) “providers” are required to implement and maintain an AI risk-management system, maintain technical documentation demonstrating compliance with the EU AI Act, and apply appropriate data governance practices with respect to training data; and (ii) “deployers” (i.e., users) are required to conduct human oversight of AI use, maintain logs of AI system operations, and monitor AI system performance.

2. U.S. State Laws

By contrast, U.S. state AI laws generally take a narrower, harm-based approach by regulating discrete AI use cases – such as automated employment-related decision-making, consumer profiling, or biometric data collection – rather than establishing a single, comprehensive framework applicable to all AI systems based on tier-based risk profiles.

Colorado’s recent legislative shift underscores the harm-based approach preferred by U.S. states. In May 2026, Colorado repealed its earlier, more comprehensive 2024 Colorado AI Act (SB 24-205), which had included a risk-based classification system comparable to the EU AI Act, and replaced it with SB 26-189, a narrower AI law focused on automated decision-making technologies used to

"materially influence a consequential decision" relating to a Colorado consumer (e.g., decisions relating to a consumer's ability to access education, employment, real estate, financial services, etc.). Other states have taken similarly targeted approaches, including:

- **Illinois** (regulates use of AI in employment decisions),
- **Texas** (prohibits specified uses of AI systems, including certain uses related to child exploitation, and requires disclosures to consumers interacting with AI systems),
- **Utah** (requires disclosures by certain "regulated occupations," such as health care providers, to consumers interacting with generative AI),
- **New York** (imposes transparency, safety, and disclosure requirements on "large developers" of "frontier" AI models), and
- **California** (imposes disclosure and transparency requirements relating to certain AI-generated content and training data).

As a result, a company providing or using the same AI system nationwide may face differing compliance obligations across various states. For example, a company seeking to use an AI hiring tool nationwide may be required, under the applicable state laws, to (i) provide clear and conspicuous notice to Colorado interviewees if the tool will "materially influence" hiring decisions, (ii) obtain consent from Illinois interviewees before using AI to analyze video-based interviews or otherwise evaluate candidates as part of the hiring process, and (iii) conduct an AI risk assessment under California law.

Certain Key Considerations in Negotiating U.S. AI Agreements

This section provides a non-exhaustive summary of certain key considerations relevant to negotiating agreements for the provision or use of AI systems in the United States, based on the current landscape of U.S. state AI laws.

1. Use Restrictions and Tailored Compliance Commitments

Because U.S. state AI laws impose different obligations depending on the jurisdiction and the specific use case, providers and users of AI systems in the United States may wish to seek contractual guardrails that define where and how an AI system may be provided and used, as well as compliance commitments tailored to those locations and use cases.

- For providers, this may include (i) imposing targeted use restrictions and limitations that prohibit or restrict use in higher-risk contexts or jurisdictions (e.g., prescribing specific geographic locations where users may be located or specific activities that users are prohibited from conducting using the AI system), (ii) requiring users to certify intended use cases or refrain from using the AI system in regulated contexts without prior approval, and (iii) disclaiming or narrowing legal compliance warranties to reflect the fragmented regulatory landscape (e.g., tying provider compliance commitments to desirable jurisdictions, intended uses, or documented system capabilities, rather than "all applicable laws").

- For users, this may include seeking (i) warranties or other commitments that the provider and the AI system are and will remain fully compliant under the laws of each of the jurisdictions in which the user intends to use the AI system and (ii) provider obligations to notify the user of changes in law that could affect the user's use of the AI system.

2. Indemnification and Limitations of Liability

Providers and users of AI systems may also wish to allocate risk via AI-tailored indemnification and limitation of liability provisions. Providers may wish to (i) limit their obligations to indemnify users for compliance with law issues to violations of law directly caused by the provider's conduct, as opposed to those arising from the AI system itself or user-specific use of that system, and (ii) impose a damages cap on any provider indemnity relating to compliance with AI laws. Users, on the other hand, may wish to seek (i) broad provider indemnification obligations covering all compliance with law issues arising from authorized use of an AI system and (ii) uncapped (or heightened) provider liability for compliance with law issues.

3. Ongoing Operational Governance

Providers and users of AI systems may also wish to address ongoing operational governance rights and obligations (e.g., provisions addressing audit rights, cooperation, maintenance of technical documentation, and AI system monitoring and data governance practices), particularly where applicable laws impose bias testing, impact assessment, transparency, or other continuing obligations on AI providers or users. In the absence of a unified U.S. regulatory framework, these types of provisions can help ensure that ongoing compliance responsibilities are clearly allocated and operationalized between the parties.

Contacts

David A. Toy

Partner

Denver

Email me

Thomas J. Petrie

Senior Associate

Denver

Email me

Colin Harris

Associate

Denver

Email me