

The Global AI Regulation Patchwork

The Global AI Regulation Patchwork: A Comparative Regulatory Landscape Report

Executive Summary

The global AI regulatory landscape as of mid-2026 is defined by six simultaneous dynamics that collectively determine the compliance environment for any organization developing, deploying, or integrating AI products across borders.

First, a small number of jurisdictions have enacted comprehensive, cross-sector, binding AI-specific statutes. The European Union's AI Act (Regulation (EU) 2024/1689) and South Korea's AI Basic Act—together with its Enforcement Decree, both effective 22 January 2026 [\[6-7\]](#)—are the only two omnibus AI laws in force globally [\[1-1\]\[1-2\]](#). China has assembled a functionally equivalent layered regime through binding, activity-specific administrative measures covering generative AI, deep synthesis, algorithmic recommendation, and content labeling [\[1-4\]\[1-5\]\[1-6\]\[1-7\]](#).

Second, the United States remains a fragmented dual-layer system comprising a state legislative patchwork—with 1,561 AI-related bills introduced across 45 states by March 2026 and no comprehensive federal AI statute [\[1-17\]\[1-18\]](#)—and a federal enforcement layer in which the FTC, EEOC, and California's CPPA are actively using existing consumer-protection, anti-discrimination, and privacy authorities to create binding AI-related obligations [\[4-1\]\[4-2\]\[4-6\]](#). A critical development in 2026 is the substantial revision of Colorado's AI regime: the original SB 24-205 was repealed and reenacted by SB26-189, which narrowed deployer obligations, removed the original duty-of-care and impact-assessment requirements, and delayed developer obligations to 1 January 2027 [\[6-1\]\[6-2\]\[6-3\]](#). The practical U.S. compliance burden remains substantially higher than an enacted-law inventory alone would suggest, but the highest-burden U.S. deployer regime is now California's CPPA ADMT regulations rather than Colorado. Separately, two states enacted frontier-model *developer* laws in 2025–2026—California's Transparency in Frontier Artificial Intelligence Act (SB 53, signed 29 September 2025) and New York's RAISE Act (signed 19 December 2025, effective 1 January 2027)—a provider/developer-facing state layer distinct from the CPPA's deployer-facing ADMT rules [\[1-48\]\[1-47\]](#).

Third, the EU has gone further than any other jurisdiction in building a proceduralized enforcement and implementation architecture. This includes a central AI Office, national market surveillance authorities coordinated through the European AI Board, a Scientific Panel, an Advisory Forum, a GPAI Code of Practice, a mandatory training-data transparency template, the AI Pact voluntary pre-compliance initiative, and a harmonised-standards pathway through CEN-CENELEC [\[2-1\]](#)[\[2-2\]](#)[\[2-3\]](#)[\[2-4\]](#)[\[2-6\]](#)[\[2-8\]](#)[\[2-9\]](#)[\[3-5\]](#)[\[3-6\]](#). However, this architecture has not been free of friction: the Commission missed deadlines for guidance on high-risk systems [\[6-15\]](#), industry stakeholders have publicly described the GPAI Code of Practice as imposing a "disproportionate burden" with key guidance still missing [\[6-12\]](#)[\[6-13\]](#), and the GPAI Code creates a two-track compliance environment in which signatories benefit from a presumption of compliance while non-signatories must demonstrate conformity through other means [\[6-14\]](#). The EU's implementation machinery is the most developed globally, but it is being experienced by affected providers as a source of both structure and uncertainty.

Fourth, a parallel layer of non-binding but operationally consequential governance infrastructure is emerging alongside formal legislation. International standards (ISO/IEC 42001), incident-reporting frameworks (OECD), technical guidance (NIST AI 600-1), privacy-regulator technical studies (Brazil's ANPD), and national AI charters (UAE, Saudi Arabia) are creating a form of convergence that transcends the divergence in formal law [\[3-1\]](#)[\[3-2\]](#)[\[3-4\]](#)[\[3-7\]](#)[\[3-8\]](#)[\[3-9\]](#).

Fifth, a transnational governance superstructure has materialized above domestic law, with three distinct functions. The Council of Europe's Framework Convention on Artificial Intelligence—the first-ever binding international AI treaty, opened for signature on 5 September 2024 and negotiated with participation from non-European states including the United States, Canada, Japan, and others [\[5-1\]](#)[\[5-2\]](#)—provides a treaty-level human-rights baseline that will require States Parties to adopt domestic measures consistent with its standards [\[5-1\]](#)[\[5-3\]](#). The G7 Hiroshima AI Process (HAIP) provides a voluntary but structured transparency and governance mechanism aimed especially at advanced AI organizations, now operationalized through a Reporting Framework that produced 25 reports in its first cycle [\[5-4\]](#)[\[5-7\]](#)[\[5-8\]](#). UNESCO's Readiness Assessment Methodology (RAM) provides a state-readiness and governance-capacity tool being used in concrete country-level assessment exercises [\[5-11\]](#)[\[5-12\]](#)[\[5-13\]](#).

Sixth, several jurisdictions previously characterized as static are in fact evolving faster than earlier assessments suggested. South Korea's Enforcement Decree is already in effect, with provisions on domestic-agent obligations and specific transparency methods for foreign providers [\[6-7\]](#)[\[6-8\]](#). Brazil's PL 2338/2023 has

passed the Senate and is now being processed by the Chamber of Deputies [\[6-10\]](#)[\[6-11\]](#). The UK Parliament is actively debating whether cross-sector AI legislation is needed [\[6-9\]](#). These developments narrow the gap between the "binding-law" jurisdictions and the "soft-law" jurisdictions.

A critical finding for Espadon's planning: the provider/deployer compliance split is now structurally embedded in the two most consequential regimes, but the specific allocation of burden has shifted in important ways. In the EU, GPAI model providers face centralized AI Office oversight, Scientific Panel scrutiny, and dedicated implementation tools, while deployers face nationally distributed market surveillance [\[2-1\]](#)[\[2-2\]](#)[\[2-4\]](#)[\[2-8\]](#)[\[2-9\]](#). In the United States, the FTC targets providers directly through AI-capability-claims enforcement [\[4-1\]](#)[\[4-3\]](#)[\[4-4\]](#), while employment and privacy rules place the direct legal obligation on deployers with indirect pressure on vendors [\[4-6\]](#)[\[4-11\]](#)[\[4-12\]](#). Colorado's revised SB26-189 retains a developer-to-deployer documentation transfer mechanism but has removed the deployer-side impact-assessment and risk-management program requirements that previously made it the closest U.S. analogue to the EU's high-risk deployer regime [\[6-1\]](#)[\[6-2\]](#)[\[6-3\]](#). California's CPPA ADMT regulations are now the most operationally significant U.S. deployer-facing AI-adjacent regime, though they are narrower than an AI statute and apply only where technology replaces or substantially replaces human decision-making in "significant decision" contexts [\[6-4\]](#)[\[6-5\]](#)[\[6-6\]](#).

For global AI product companies, the "patchwork" is not only a patchwork of laws; it is increasingly a patchwork of interoperable compliance artifacts spanning three layers: (1) binding domestic law, (2) governance infrastructure (standards, frameworks, technical guidance), and (3) transnational instruments (treaty commitments, voluntary codes, readiness assessments). The governance infrastructure and transnational layers provide the most promising basis for building a single global control environment that can be adapted to multiple jurisdictions.

1. The Transnational Governance Superstructure

Before examining individual jurisdictions, it is necessary to describe the transnational layer that now sits above domestic AI law. This layer has emerged rapidly since 2023 and shapes how states and firms operationalize AI governance across borders.

1.1 The Council of Europe Framework Convention on Artificial Intelligence

The Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law is the first-ever international legally binding treaty in the AI field [\[5-1\]](#). It was opened for signature on 5 September 2024 [\[5-1\]\[5-2\]](#).

The Convention was drafted by the Council's 46 member states with the participation of observer states including Canada, Japan, Mexico, the Holy See, and the United States, as well as the European Union and additional non-member states including Australia, Argentina, Costa Rica, Israel, Peru, and Uruguay [\[5-1\]](#). This broad participation means AI governance is now being shaped through a multilateral treaty venue that extends well beyond Europe.

The Convention is a **framework treaty**, not a directly self-executing AI rulebook. It requires parties to adopt or maintain legislative, administrative, or other measures to give effect to its standards [\[5-1\]\[5-3\]](#). Its practical focus is on ensuring that activities within the lifecycle of AI systems are consistent with human rights, democracy, and the rule of law [\[5-1\]](#). Implementation measures are to be graduated and differentiated according to the severity and probability of adverse impacts—a risk-based logic that converges with the EU AI Act's approach, even though the Convention is structured as public international law rather than product regulation [\[5-1\]\[5-3\]](#).

The Convention's significance for comparative analysis is that it creates an additional route for convergence outside the EU model. Because the treaty is open beyond Europe and focuses on lifecycle safeguards and human-rights-consistent governance, it can influence domestic AI governance even in countries that do not adopt the EU AI Act structure [\[5-1\]\[5-2\]\[5-3\]](#). For firms, the Convention does not directly impose provider or deployer duties, but it will shape the domestic legal environments of its States Parties over time.

1.2 The G7 Hiroshima AI Process (HAIP)

The Hiroshima AI Process was launched in May 2023 following the G7 Hiroshima Summit. The Hiroshima AI Process Comprehensive Policy Framework was agreed in December 2023 and endorsed by G7 leaders the same month [\[5-4\]](#). The framework includes guiding principles and an international code of conduct aimed at promoting safe, secure, and trustworthy advanced AI systems [\[5-4\]](#).

The **Hiroshima Code of Conduct** is targeted specifically at organizations developing advanced AI systems, including advanced foundation models and generative AI systems [\[5-5\]](#). It calls for actions across the lifecycle—design, development, deployment, and use—including identifying, evaluating, and mitigating risks; publishing transparency reports; keeping documentation up to date; reporting evaluations of safety, security, and societal risks; documenting capabilities and limitations; discussing risks such as bias, discrimination, privacy, and fairness; and disclosing governance and risk-management policies [\[5-5\]\[5-6\]](#). These topics overlap strongly with obligations appearing in binding regimes: the EU AI Act's GPAI documentation requirements, Colorado's developer documentation rules, China's security assessment and filing requirements, and NIST's generative AI guidance [\[5-5\]\[5-6\]](#).

In February 2025, HAIP added a **Reporting Framework** that turns the Code into a repeatable disclosure mechanism [\[5-7\]](#). The OECD states that the Reporting Framework provides a standardised structure for organizations to report on their alignment with the Code of Conduct [\[5-8\]](#). The Framework is open across the AI value chain, including developers, deployers, and providers of advanced AI systems [\[5-8\]](#). The first reporting cycle produced 25 reports, and the OECD's September 2025 publication *How are AI developers managing risks?* presents preliminary insights from submissions by 20 organisations across diverse sectors and countries [\[5-8\]\[5-9\]\[5-10\]](#). Submitted reports are published on the OECD AI Policy Observatory [\[5-8\]](#).

Participants reported internal benefits from engaging in the reporting process, including value as a transparency tool and as a mechanism for internal capacity-building and coordination [\[5-7\]](#). The HAIP transparency topics map closely onto the compliance artifacts firms are already being asked to produce in stricter jurisdictions [\[5-6\]\[5-9\]](#), making the Reporting Framework a practical tool for organizations building global compliance architectures.

1.3 UNESCO Readiness Assessment Methodology (RAM)

UNESCO's Recommendation on the Ethics of AI is a global normative framework, and UNESCO's Readiness Assessment Methodology (RAM) is directly linked to that Recommendation [\[5-11\]\[5-12\]](#). RAM evaluates a country's AI ecosystem across multiple dimensions including legal and regulatory, social and cultural, economic, scientific and educational, and technological and infrastructural dimensions [\[5-12\]\[5-13\]](#). UNDP and UNESCO offer RAM and UNDP's AI Landscape Assessment together as complementary support for governments [\[5-12\]](#).

RAM is being used in concrete country processes in 2025–2026, with consultations or reports in the Philippines, Trinidad and Tobago, and Lao PDR [\[5-11\]](#)[\[5-13\]](#)[\[5-14\]](#). This demonstrates that UNESCO's AI governance influence is being operationalized through country-level assessment exercises, creating a practical channel through which international organizations shape how national governments diagnose regulatory gaps and prioritize future AI policy actions [\[5-12\]](#)[\[5-13\]](#)[\[5-14\]](#).

1.4 The Three-Function Transnational Architecture

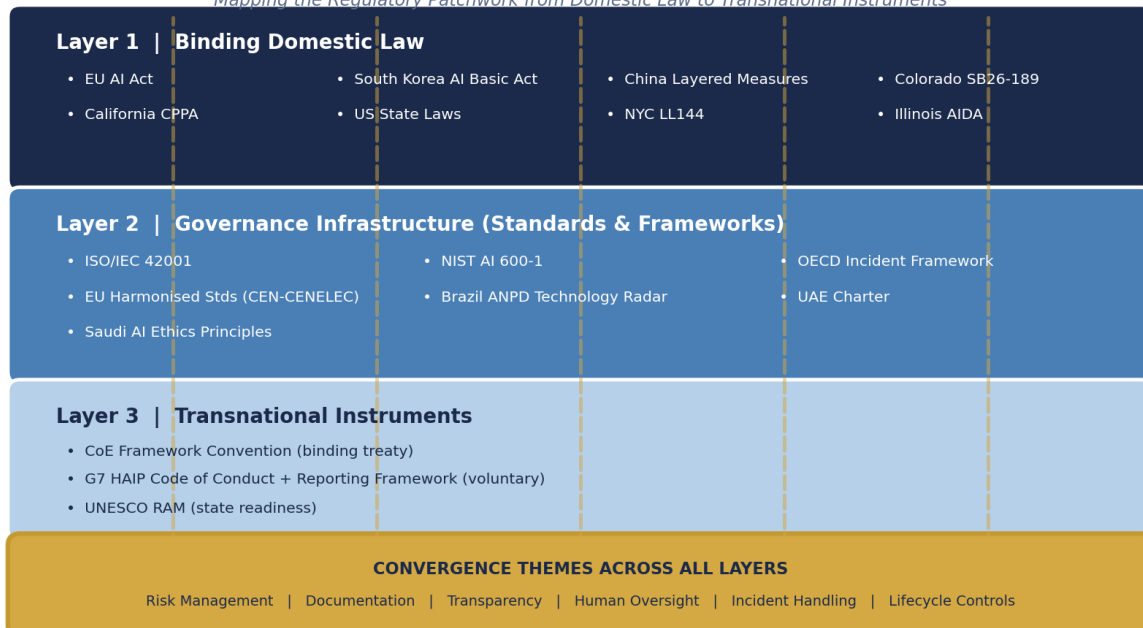
The transnational layer now performs three distinct functions:

1. **Binding international baseline:** The Council of Europe Convention provides a treaty-level human-rights standard that will require domestic implementation by its States Parties [\[5-1\]](#)[\[5-2\]](#)[\[5-3\]](#).
2. **Voluntary structured transparency:** The G7 HAIP provides a repeatable disclosure and governance mechanism aimed at advanced AI organizations across the value chain [\[5-4\]](#)[\[5-5\]](#)[\[5-7\]](#)[\[5-8\]](#).
3. **State-readiness and capacity-building:** UNESCO RAM provides a diagnostic tool that influences how governments prepare for AI regulation [\[5-11\]](#)[\[5-12\]](#)[\[5-13\]](#).

These mechanisms do not impose the same kind of direct firm-level liability as the EU AI Act or China's administrative rules, but they are now concrete parts of the global AI governance architecture. They help explain why compliance concepts—risk management, documentation, transparency, human oversight, incident handling—are converging internationally even while legal obligations remain fragmented across jurisdictions [\[5-1\]](#)[\[5-8\]](#)[\[5-12\]](#).

Global AI Governance: Three-Layer Architecture

Mapping the Regulatory Patchwork from Domestic Law to Transnational Instruments



2. European Union

2.1 Legal Status and Scope

The EU AI Act, Regulation (EU) 2024/1689, is a binding cross-sector regulation that entered into force on 1 August 2024 [\[1-1\]](#). It covers providers, deployers, importers, distributors, product manufacturers, and providers of general-purpose AI (GPAI) models, with extraterritorial reach where AI system outputs are used in the EU market [\[1-1\]](#).

2.2 Risk Model

The Act employs a four-tier risk classification:

- **Prohibited practices** (Article 5): Unacceptable-risk AI applications are banned outright.
- **High-risk AI systems** (Articles 6 and Annex III): Systems deployed in listed sectors or use cases face the most extensive compliance obligations.
- **Transparency obligations** (Article 50): Certain AI systems—such as chatbots and emotion-recognition systems—must meet specified disclosure requirements.

- **GPAI models** (Articles 51, 53, 55): General-purpose AI models, including those with systemic risk, face dedicated obligations [\[1-1\]](#).

2.3 Obligations: Developers/Providers

Providers of high-risk AI systems must implement risk management systems, data governance controls, technical documentation, logging capabilities, transparency and instructions for use, human-oversight design features, accuracy/robustness/cybersecurity safeguards, quality management systems, conformity assessments, registration where applicable, post-market monitoring, and serious incident reporting [\[1-1\]](#).

Providers of GPAI models must prepare technical documentation, furnish information and documentation to downstream providers, comply with EU copyright law, and publish a sufficiently detailed summary about training content [\[1-1\]](#). Where a GPAI model presents systemic risk, additional obligations include model evaluation, systemic-risk assessment and mitigation, adversarial testing, incident reporting, and cybersecurity protections [\[1-1\]](#).

These GPAI provider obligations have been operationalized through dedicated implementation instruments. The Commission finalized a **mandatory training-data transparency template** on 24 July 2025, prescribing the specific format GPAI providers must use to summarize data used for model training [\[2-9\]](#). The **GPAI Code of Practice**, submitted by independent experts, provides a voluntary compliance tool covering transparency, copyright, and safety and security obligations [\[2-6\]](#)[\[2-8\]](#). The Code directly targets model-provider obligations rather than deployer obligations [\[2-8\]](#).

2.4 Obligations: Deployers/Users/Integrators

Deployers of high-risk AI systems must use systems according to provider instructions, ensure human oversight, monitor operations, maintain logs, and report serious incidents. Certain public-sector or listed use cases trigger mandatory fundamental-rights impact assessments [\[1-1\]](#). Deployers are primarily subject to enforcement through national market surveillance authorities rather than the central AI Office [\[2-2\]](#).

2.5 Enforcement Architecture

The EU AI Act has generated the most developed enforcement and implementation machinery of any AI regime globally. This architecture operates across multiple

institutional layers:

- **The AI Office** is the central EU-level body responsible for implementing the AI Act, with particular authority over GPAI rules. Its tasks include enforcing and supervising GPAI obligations, contributing to the consistent application of the Act across Member States, and promoting implementation tools such as codes of practice and innovation measures [\[2-1\]](#).
- **National market surveillance authorities** are jointly responsible with the AI Office for implementing, supervising, and enforcing the AI Act. Each Member State must designate market surveillance authority capacity, and where multiple authorities exist, one single point of contact must be designated [\[2-2\]](#). These authorities have affirmative investigative and reporting powers and must report annually to the Commission and relevant national authorities [\[2-2\]](#).
- **The European AI Board** is the coordination mechanism through which national market surveillance authorities cooperate, exchange expertise, and facilitate effective enforcement [\[2-2\]](#).
- **The Advisory Forum** (Article 67) provides technical expertise and advice on a broad range of AI Act matters, including standardization and implementation challenges [\[2-3\]](#).
- **The Scientific Panel** (Article 68, Implementing Regulation (EU) 2025/454) advises the AI Office and national authorities on the impacts and risks of GPAI models. Its core tasks include alerting the AI Office to systemic risks, advising on GPAI classification and evaluation methodologies, and supporting market-surveillance activities [\[2-4\]](#).
- **The AI Pact** is a voluntary pre-compliance initiative that has attracted over 100 company signatories as of 2024 [\[2-5\]](#)[\[2-7\]](#). The pledges include organizational AI governance strategies designed to foster AI uptake and work toward future compliance with the AI Act [\[2-7\]](#).

2.6 The Standardisation Layer

The EU is building a separate compliance layer through **harmonised standards**. The European Commission's AI Act standardisation page states that harmonised standards will offer legal certainty under the AI Act, and that once standards are published by CEN and CENELEC, the Commission will assess them and reference them in the Official Journal of the EU [\[3-5\]](#). CEN-CENELEC's JTC 21 states that its purpose is to develop European standards providing manufacturers with a **presumption of conformity** with the AI Act [\[3-6\]](#).

On 19 November 2025, the Digital Omnibus proposed linking the application of rules for high-risk AI systems to the availability of support tools, including standards [\[3-5\]](#). Because providers of high-risk systems need to demonstrate compliance and deployers often depend on provider documentation, the standards infrastructure will also affect the information packages, instructions, and conformity artifacts that downstream users receive [\[3-5\]](#)[\[3-6\]](#).

2.7 Implementation Friction and the GPAI Two-Track Problem

The EU's implementation machinery is real and institutionally advanced, but it has not been frictionless. The European Commission missed deadlines for guidance on high-risk AI systems [\[6-15\]](#), and there was visible mid-2025 uncertainty around possible AI Act timing relief, with strong industry calls for delay [\[6-16\]](#). CCIA Europe stated in July 2025 that the final GPAI Code of Practice still imposed a "disproportionate burden" and that key AI Office guidance was still missing [\[6-12\]](#). ITI likewise reacted publicly to the Code's publication [\[6-13\]](#).

The GPAI Code of Practice creates a functionally important **two-track compliance environment**. Providers who sign the Code benefit from a presumption of compliance with the AI Act's GPAI obligations. Providers who choose not to sign the Code must still meet the Act's legal requirements, but without the benefit of that presumption [\[6-14\]](#). This means the Code is not binding law in the traditional sense, yet it functionally pressures GPAI providers to participate or face a higher evidentiary burden when demonstrating compliance through alternative means [\[6-14\]](#). For global model developers, this two-track structure is a material compliance design choice: signing the Code provides legal certainty but commits the organization to its specific requirements; declining creates a bespoke-compliance pathway with more uncertainty.

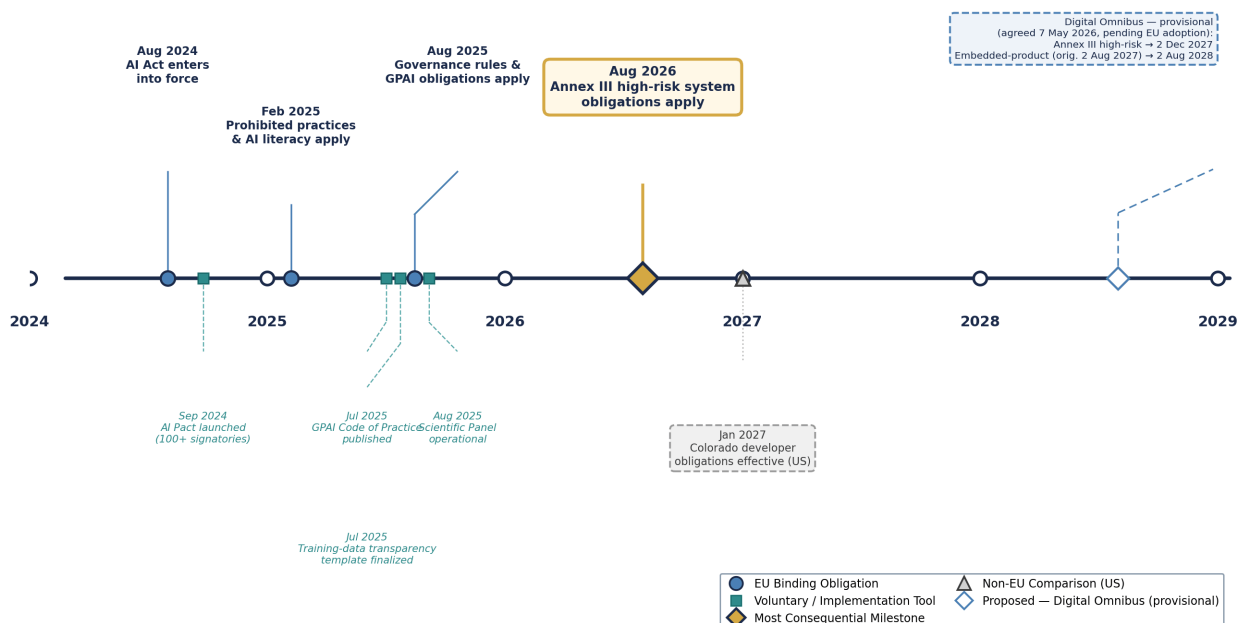
2.8 Enforcement Timeline

- **2 February 2025:** Prohibited AI practices and AI literacy obligations began applying [\[1-1\]](#).
- **2 August 2025:** Governance rules and GPAI obligations began applying [\[1-1\]](#).
- **2 August 2026:** Most stand-alone Annex III high-risk system obligations apply under the original statutory timeline [\[1-1\]](#).
- **2 August 2027:** High-risk AI systems that are safety components of products already covered by EU harmonisation legislation (Annex I — e.g. medical devices, machinery, radio equipment) become subject to high-risk obligations under the original statutory timeline [\[1-1\]](#).

- **"Digital Omnibus" deferrals (provisional — not yet adopted):** On 7 May 2026 the Council and the European Parliament reached a provisional political agreement on the Commission's "Digital Omnibus" simplification package, which links the application of high-risk rules to the availability of supporting standards and tools and defers, as a backstop, the application of high-risk obligations [2-6]. Under that agreement, **stand-alone Annex III high-risk obligations are deferred from 2 August 2026 to no later than 2 December 2027 (≤ 16 months), and embedded-product (Annex I) high-risk obligations from 2 August 2027 to 2 August 2028 (≤ 12 months);** GPAI obligations and the core governance provisions keep their existing dates [2-6]. These deferred dates take legal effect only upon formal adoption and publication in the Official Journal (expected before 2 August 2026); until then the original statutory dates above remain the legally binding timeline.

EU AI Act — Phased Implementation Timeline (2024–2028)

Key binding obligations, voluntary tools, and international comparison milestones



2.9 Penalties

Administrative fines reach up to EUR 35 million or 7% of worldwide annual turnover for prohibited-practice breaches; up to EUR 15 million or 3% for certain other violations; and up to EUR 7.5 million or 1.5% for supplying incorrect information, with lower caps for SMEs and startups in some cases [1-1].

2.10 Compliance Burden Assessment

The EU regime imposes the highest combined compliance burden globally for both model developers/providers and deployers. The burden on GPAI/model providers is increasing through proceduralized implementation detail: providers now face the central AI Office's enforcement authority, Scientific Panel scrutiny pathways, the GPAI Code of Practice (with its two-track presumption structure [\[6-14\]](#)), a mandatory training-data summary template [\[2-9\]](#), and the emerging harmonised-standards pathway [\[3-5\]](#)[\[3-6\]](#). The implementation friction documented through missed guidance deadlines [\[6-15\]](#) and industry contestation [\[6-12\]](#)[\[6-13\]](#) does not reduce the legal obligations themselves but does create near-term compliance uncertainty about the precise operational standards expected. Deployers face a substantial but differently structured burden through national market surveillance channels, fundamental-rights impact assessments, human-oversight duties, and logging requirements [\[1-1\]](#)[\[2-2\]](#).

The net effect is that the EU's compliance ecosystem now comprises three interlocking layers: (1) the statute itself, (2) institutional enforcement machinery (AI Office, national MSAs, AI Board, Scientific Panel, Advisory Forum), and (3) technical standardisation and voluntary governance tools (harmonised standards, GPAI Code of Practice, training-data template, AI Pact). This three-layer structure has no equivalent in any other jurisdiction.

3. United States: The 50-State Patchwork and Federal Enforcement Layer

3.1 National Structure: A Dual-Layer System

The United States lacks a single federal AI law. The U.S. regulatory environment is best understood as a **dual-layer system**: a state legislative patchwork and a federal enforcement layer that operates through existing consumer-protection, anti-discrimination, and privacy authorities.

The state legislative layer is a composite of enacted AI-specific state laws, comprehensive privacy laws with automated-decision-making (ADMT) provisions, biometric and deepfake statutes, employment-specific AI rules, executive orders, state agency guidance, and a large volume of pending legislation [\[1-3\]](#)[\[1-17\]](#)[\[1-18\]](#). By March 2026, 1,561 AI-related bills had been introduced across 45 states, and 99 AI-related bills were enacted in 2024 [\[1-17\]](#)[\[1-18\]](#). Unlike the EU, which manages internal national

variation through the European AI Board and single points of contact [\[2-2\]](#), the U.S. state patchwork has no formal coordination mechanism.

The federal enforcement layer creates binding AI-related obligations without a dedicated AI statute. The FTC has built a dedicated AI enforcement and policy hub under its existing consumer-protection authority [\[4-1\]](#), and the EEOC has created an AI and algorithmic fairness initiative for employment discrimination enforcement [\[4-2\]](#). These agencies are actively bringing enforcement actions and issuing guidance that shapes AI compliance obligations for both providers and deployers. Narrow AI-specific federal statutes have also begun to appear—most notably the TAKE IT DOWN Act (Public Law 119-12, signed 19 May 2025), which criminalizes non-consensual intimate imagery including AI-generated deepfakes and requires covered platforms to operate a notice-and-removal process—though there is still no comprehensive federal AI statute [\[1-49\]](#).

Additionally, the United States possesses a detailed federal **voluntary** governance layer. NIST's *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile* (NIST AI 600-1) is an official cross-sectoral publication intended to help organizations apply the AI RMF to generative AI contexts [\[3-4\]](#). The Profile recommends lifecycle controls that closely resemble obligations found in binding laws elsewhere: acceptable-use policies, assumptions and limitations of use, disclosure information or notices, incident response plans, data provenance information, human-oversight roles and responsibilities, underlying foundation-model versions and access modes, and updated hierarchies of identified risks [\[3-4\]](#).

3.2 Federal Enforcement: The FTC and AI Providers

The FTC's enforcement activity represents the highest immediate federal compliance risk for AI model developers and providers. In September 2024, the FTC announced "Operation AI Comply," describing five enforcement actions targeting companies that allegedly used AI claims or AI-enabled tools in deceptive or unfair ways [\[4-3\]](#). The actions focused on false or misleading claims that products were "AI-powered" or could reliably deliver specified outcomes, building on earlier cases involving online storefront schemes, AI moderation claims, AI facial recognition, and AI-related accuracy claims [\[4-3\]](#).

A concrete 2025 example is the FTC's finalized order against DoNotPay over claims that its service was "the world's first robot lawyer." The FTC stated the company had not tested whether its AI-generated legal documents could substitute for a human lawyer's

expertise, and the order prohibits deceptive AI-lawyer claims, imposes monetary relief, and requires notice to past subscribers [\[4-4\]](#)[\[4-5\]](#).

The practical U.S. burden for providers therefore includes **substantiating capability claims and avoiding "AI-washing"**: companies face enforcement if they market tools as AI-powered or outcome-capable without adequate support [\[4-1\]](#)[\[4-3\]](#)[\[4-4\]](#).

3.3 Federal Enforcement: The EEOC and Employment AI

The EEOC has made clear that employer use of AI and algorithmic tools is already subject to Title VII disparate-impact analysis [\[4-2\]](#). The EEOC's public explainer lists recruiting, screening, hiring, monitoring employees, assessing productivity, setting wages, and deciding whom to promote or fire as areas where AI use may violate employment discrimination laws [\[4-11\]](#).

The EEOC's Title VII technical-assistance document explains that if a tool has an adverse impact on a protected group, its use violates Title VII unless the employer can show the use is job-related and consistent with business necessity [\[4-12\]](#). The document also states that employers considering whether to rely on a vendor may want to ask specifically whether the vendor assessed adverse impact using measures such as the four-fifths rule of thumb [\[4-12\]](#). This creates a **concrete vendor-management obligation** that makes employment-AI vendors part of the compliance chain even when the legal duty remains on the employer [\[4-11\]](#)[\[4-12\]](#).

3.4 California CPPA: The Most Operationally Significant U.S. Deployer-Facing AI-Adjacent Regime

California's privacy rulemaking has matured into the most operationally significant U.S. deployer-facing AI-adjacent regime. In September 2025, the CPPA announced that the Office of Administrative Law approved regulations covering automated decisionmaking technology (ADMT), risk assessments, and cybersecurity audits [\[6-4\]](#). The compliance timeline is more staggered than broad summaries suggest:

- Businesses subject to **risk-assessment** requirements must begin compliance by **1 January 2026** [\[6-4\]](#).
- Businesses using ADMT to make **significant decisions** must comply with the ADMT-specific requirements beginning **1 January 2027** [\[6-5\]](#)[\[6-6\]](#).
- For risk assessments conducted in 2026 and 2027, businesses must submit information regarding the assessment to the CPPA by **1 April 2028** (for larger

businesses) [\[6-5\]](#).

The final rules are **narrower than earlier drafts and narrower than many broad "AI law" descriptions imply**. They apply when technology **replaces or substantially replaces human decision-making** in certain "significant decision" contexts, and explicit references to artificial intelligence were removed from the final text compared with earlier drafts [\[6-6\]](#). The regulations require businesses to provide notice, opt-out rights in covered cases, and related information/access mechanisms [\[4-7\]\[4-8\]](#).

California's CPPA rules functionally push the state toward the EU/Colorado pattern on impact assessment and significant-decision controls, but the legal vehicle is CCPA rulemaking rather than an AI act, and the scope is limited to a privacy-law definition of automated decisionmaking rather than a general AI-system definition [\[6-4\]\[6-6\]](#).

3.5 Colorado: A Substantially Revised Regime

Colorado's AI regulatory story has undergone a fundamental change. The original SB 24-205, signed on 17 May 2024, was the first broad state high-risk AI law and was widely described as imposing EU-like developer and deployer obligations for high-risk AI systems used in consequential decisions [\[1-19\]\[1-20\]](#). However, **SB26-189 repealed and reenacted those provisions** with a materially different compliance architecture [\[6-1\]](#).

The revised Colorado regime:

- **Removes** the original duty of care, the deployer risk-management program requirement, the deployer impact-assessment requirement, and certain attorney general reporting duties [\[6-2\]\[6-3\]](#).
- **Retains** a developer-to-deployer documentation transfer mechanism: developers of covered ADMT must provide deployers with technical documentation on intended uses, categories of training data, known limitations, and instructions for appropriate use and human review [\[6-1\]](#).
- **Retains** consumer-notice, adverse-decision explanation, and human review-related rights for deployers [\[6-1\]\[6-2\]\[6-3\]](#).
- **Delays** developer obligations to **1 January 2027** [\[6-1\]](#), superseding the prior SB 24-205 schedule (obligations originally set for 1 February 2026, later delayed to 30 June 2026).

The practical effect is that Colorado's regime is now centered on **documentation transfer and consumer-facing transparency** rather than the ex ante risk-management

and impact-assessment architecture that made it the closest U.S. analogue to the EU's high-risk deployer framework. Colorado remains significant as the first U.S. state to create a comprehensive developer-to-deployer information-transfer obligation for AI systems used in consequential decisions, but the deployer-side burden is substantially lighter than the original law would have imposed [\[6-1\]](#)[\[6-2\]](#)[\[6-3\]](#).

3.6 Other High-Impact Enacted State Regimes

Utah enacted its AI disclosure law on 13 March 2024, effective 1 May 2024. It requires consumer disclosures when individuals interact with generative AI in covered contexts and established the Office of Artificial Intelligence Policy and an AI Learning Laboratory Program [\[1-21\]](#)[\[1-22\]](#). The law was updated in 2025, with reports noting the state "scaled back" its reach [\[1-21\]](#).

Texas enacted the Responsible Artificial Intelligence Governance Act (TRAIGA) on 22 June 2025. Public analyses describe it as imposing prohibited-practice rules and public-sector notice duties while removing many of the broader private-sector developer/deployer obligations from earlier drafts [\[1-23\]](#)[\[1-24\]](#). The final enacted version is narrower in scope than the EU model or even the revised Colorado law, but it takes effect on **1 January 2026** and reaches both developers and deployers through its prohibited-use and disclosure provisions [\[1-23\]](#).

Frontier-model developer laws (California and New York). Two states have enacted laws aimed specifically at developers of frontier/foundation models—a category distinct from the deployer-facing and employment-AI rules above. California's **Transparency in Frontier Artificial Intelligence Act (SB 53 / TFAIA)**, signed on 29 September 2025, requires frontier developers (with heightened duties for "large frontier developers") to publish a safety/governance framework and model transparency reports, report critical safety incidents, and extends whistleblower protections; it takes effect 1 January 2026 [\[1-48\]](#). New York's **RAISE Act**, signed on 19 December 2025 (Chapter 699) and effective 1 January 2027, imposes safety-framework, disclosure, and incident-reporting duties on large frontier-model developers [\[1-47\]](#). These are provider/developer-facing regimes, in contrast to California's CCPA ADMT rules (Section 3.4), which are deployer-facing.

New York City Local Law 144 requires annual independent bias audits for automated employment decision tools (AEDTs) used in hiring or promotion, public posting of audit summaries, and at least 10 business days' advance notice to applicants and employees, including information about the tool and alternative assessment requests [\[1-25\]](#).

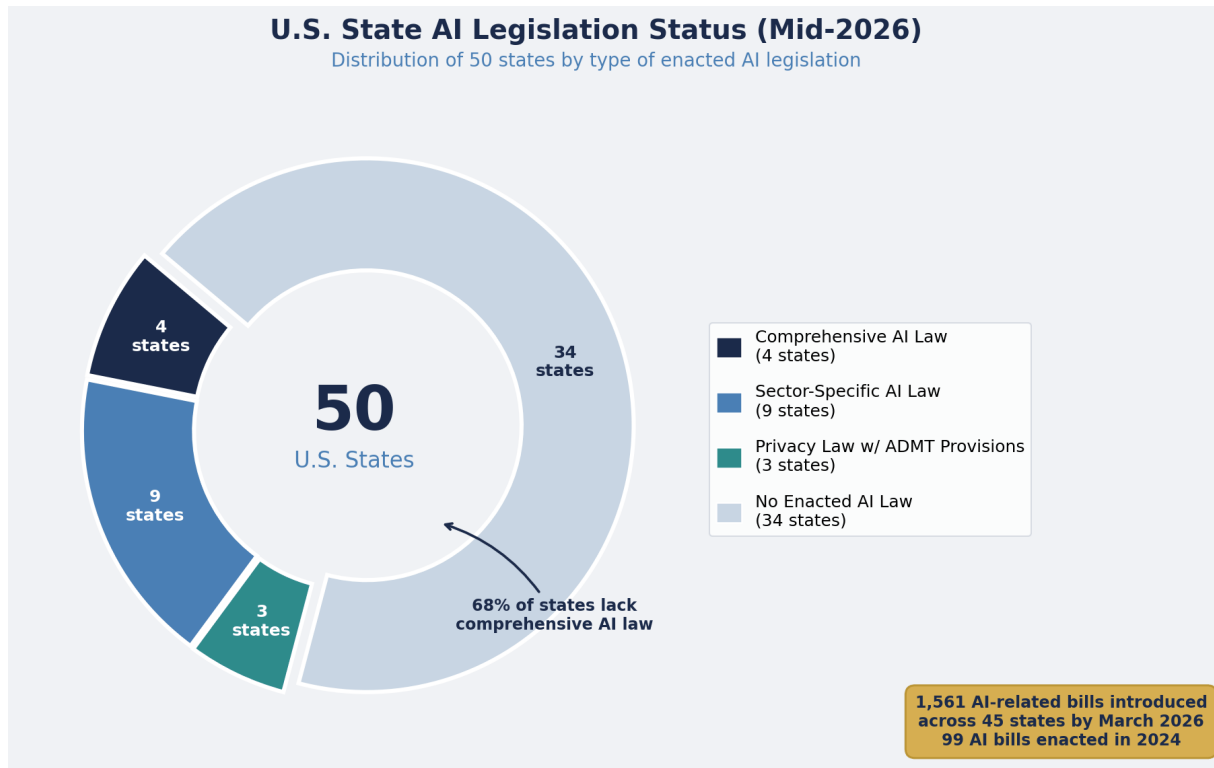
Illinois has two notable enacted measures. The Artificial Intelligence Video Interview Act requires employers using AI to analyze recorded applicant videos to notify applicants, explain how the AI works and what characteristics it evaluates, obtain consent, limit sharing, and comply with destruction/deletion rules [\[1-26\]](#). The Biometric Information Privacy Act (BIPA) remains a major enforcement law for AI systems using faceprints, voiceprints, or other biometric identifiers [\[1-26\]](#).

3.7 Privacy-Law Automated Decision-Making Provisions

Multiple states regulate AI indirectly through comprehensive privacy laws with profiling opt-outs, automated-decision-making rights, and data-protection assessment requirements:

- **Connecticut:** Requires opt-outs for profiling in decisions producing legal or similarly significant effects; 2025 amendments added explicit impact assessment requirements for such profiling and additional AI/LLM training disclosures effective 2026 [\[1-28\]](#)[\[1-29\]](#).
- **Virginia:** The Consumer Data Protection Act gives consumers the right to opt out of profiling producing legal or similarly significant effects and requires data processing assessments for specified risky processing [\[1-30\]](#)[\[1-31\]](#).
- **Alabama:** An enacted privacy law includes an opt-out right for solely automated significant decisions, effective 1 May 2027 [\[1-3\]](#).
- **California:** High legislative activity with enacted 2024–2025 AI laws covering generative AI transparency, training-data disclosures, election/deepfake measures, health and chatbot/frontier-model provisions; multiple additional proposals remain pending or have evolved [\[1-32\]](#)[\[1-33\]](#). The CPPA's ADMT regulations add a further compliance layer as described in Section 3.4 above. California also enacted the Transparency in Frontier Artificial Intelligence Act (SB 53, signed 29 September 2025), a frontier-model *developer* regime distinct from the deployer-facing ADMT rules [\[1-48\]](#).

3.8 All 50 States: Structured Status Snapshot



State	Status
Alabama	Enacted privacy law with automated-decision opt-out (effective 2027) [1-3]
Alaska	No major enacted cross-sector AI law identified; general laws and pending activity [1-3] [1-17]
Arizona	No major enacted cross-sector AI law identified; pending/tracked [1-3] [1-17]
Arkansas	Enacted AI-related transparency legislation (2025 generative AI transparency) [1-32]
California	Multiple enacted AI laws (generative AI transparency, training-data, deepfake, health, chatbot) + CCPA ADMT regulations (phased: risk assessments Jan 2026, ADMT Jan 2027, reporting Apr 2028); additional proposals pending [1-32] [1-33] [6-4] [6-5] [6-6]
Colorado	SB 24-205 repealed and reenacted by SB26-189; narrowed to documentation transfer, consumer notice, and human-review rights; developer obligations effective 1 January 2027 [6-1] [6-2] [6-3]

State	Status
Connecticut	Privacy/profiling regime with 2025 impact-assessment amendments [1-28] [1-29]
Delaware	AI innovation/task-force activity [1-17] [1-32]
Florida	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Georgia	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Hawaii	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Idaho	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Illinois	AI Video Interview Act; BIPA; employment/health updates [1-26] [1-32]
Indiana	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Iowa	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Kansas	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Kentucky	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Louisiana	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Maine	Enacted 2025 chatbot law [1-32]
Maryland	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]

State	Status
Massachusetts	Active proposals; no enacted comprehensive AI law identified [1-17] [1-27]
Michigan	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Minnesota	Privacy/AI related activity [1-32]
Mississippi	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Missouri	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Montana	No comprehensive enacted cross-sector AI law identified [1-17] [1-18]
Nebraska	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Nevada	Health-related AI law enacted (2025) [1-32]
New Hampshire	Enacted 2025 chatbot law [1-32]
New Jersey	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
New Mexico	Proposal activity; no enacted comprehensive AI law identified [1-17] [1-27]
New York	NYC Local Law 144 (employment AEDT); RAISE Act enacted 19 Dec 2025 (Chapter 699), effective 1 Jan 2027, regulating frontier-model developers [1-25] [1-47]

State	Status
North Carolina	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
North Dakota	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Ohio	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Oklahoma	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Oregon	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Pennsylvania	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Rhode Island	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
South Carolina	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
South Dakota	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Tennessee	Enacted 2024 IP/digital replica law [1-32]
Texas	Enacted TRAIGA (signed 22 June 2025; effective 1 Jan 2026) [1-23] [1-24]
Utah	Enacted AI disclosure law (1 May 2024); updated 2025 [1-21] [1-32]

State	Status
Vermont	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Virginia	Privacy/profiling regime; 2024 AI-specific bills failed [1-17] [1-30] [1-31]
Washington	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
West Virginia	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Wisconsin	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]
Wyoming	No comprehensive enacted cross-sector AI law identified [1-3] [1-17]

3.9 The Provider/Deployer Split in the U.S. System

The U.S. patchwork has a clearer provider/deployer compliance split than an enacted-law inventory alone would suggest:

For providers/developers: - FTC consumer-protection enforcement targets developers, providers, and marketers making AI capability claims or enabling deceptive uses [\[4-1\]](#)[\[4-3\]](#)[\[4-4\]](#). - Colorado's revised SB26-189 retains developer documentation obligations (intended uses, training-data categories, known limitations, instructions for use and human review) effective 1 January 2027 [\[6-1\]](#). - California's enacted transparency and training-data disclosure laws create additional provider-facing obligations [\[1-32\]](#)[\[1-33\]](#).

For deployers/users/integrators: - California's CPPA ADMT regulations create notice, opt-out, risk-assessment, and reporting obligations, phased from January 2026 through April 2028 [\[6-4\]](#)[\[6-5\]](#)[\[6-6\]](#). - Colorado's revised regime retains consumer-notice, adverse-decision explanation, and human review-related rights, but no longer requires deployer impact assessments or risk-management programs [\[6-1\]](#)[\[6-2\]](#)[\[6-3\]](#). - EEOC-driven employment testing and vendor-management expectations push employers to obtain adverse-impact evidence from vendors [\[4-11\]](#)[\[4-12\]](#). - State privacy-law profiling

and ADMT provisions in Connecticut, Virginia, Alabama, and others impose opt-out rights and assessment duties [\[1-28\]\[1-30\]\[1-3\]](#). - NYC and Illinois employment rules impose sector-specific deployer obligations [\[1-25\]\[1-26\]](#).

3.10 Compliance Burden Assessment

The U.S. patchwork creates a high operational burden through volume, fragmentation, and the combination of state legislation with federal enforcement. The burden is being created through: (a) FTC substantiation-of-AI-claims enforcement, (b) consumer-protection enforcement against AI-enabled conduct, (c) EEOC anti-discrimination testing expectations in employment, and (d) CPPA privacy-rule-based notice, opt-out, and risk-assessment duties for automated decisionmaking [\[4-1\]\[4-3\]\[4-4\]\[6-4\]\[4-11\]\[4-12\]](#).

The revision of Colorado's regime [\[6-1\]\[6-2\]\[6-3\]](#) means that the highest deployer-side burden in the U.S. has shifted from Colorado to California's CPPA ADMT regulations. However, California's rules are narrower than an AI statute: they apply only where technology replaces or substantially replaces human decision-making in significant-decision contexts [\[6-6\]](#). The U.S. therefore lacks any state-level deployer regime that matches the breadth of the EU's high-risk system obligations.

Compared with the EU, the U.S. model remains less centralized and less ex ante, but it is not light-touch in operational terms. The NIST Generative AI Profile [\[3-4\]](#) partially mitigates fragmentation for organizations that adopt it as an internal governance framework, and the HAIP Reporting Framework [\[5-7\]\[5-8\]](#) provides an additional international transparency structure. However, neither creates a legal safe harbor.

4. China

4.1 Legal Status and Scope

China's AI regulatory regime is layered and activity-specific rather than omnibus. It consists of binding administrative measures for public-facing generative AI services, deep synthesis internet information services, algorithmic recommendation services, and AI-generated/synthetic content labeling, all overlaid by the Cybersecurity Law, Data Security Law, and Personal Information Protection Law (PIPL) [\[1-4\]\[1-5\]\[1-6\]\[1-7\]](#).

The Interim Measures for the Management of Generative Artificial Intelligence Services apply to entities using generative AI to provide services to the public in mainland China for generating text, images, audio, video, or other content [\[1-4\]](#).

4.2 Risk and Regulatory Model

China's structure is not an EU-style single risk-tier law. It is activity- and content-based, with strong emphasis on public-facing services, content control, security assessment, algorithm filing, data/personal-information compliance, and state oversight [\[1-4\]](#)[\[1-5\]](#)[\[1-6\]](#).

4.3 Obligations: Developers/Providers

- **Generative AI service providers** must uphold content-law requirements, adopt measures for data and model security, protect personal information, label or handle illegal content, and for some services complete security assessments and algorithm filing procedures [\[1-4\]](#).
- **Deep synthesis providers** must not produce or disseminate prohibited information, must implement identity/authenticity-related measures, and must apply labeling obligations in specified contexts [\[1-5\]](#).
- **Algorithm recommendation service providers** must establish management systems, protect users, provide options to turn off recommendation services in some contexts, and undergo filing/security oversight where required [\[1-6\]](#).
- On 14 March 2025, the CAC and three other agencies released final Measures for Labeling Artificial Intelligence-Generated and Synthetic Content and the national standard GB 45438-2025, imposing explicit and implicit labeling duties and traceability-related duties for providers [\[1-7\]](#).

4.4 Enforcement and Penalties

Violations of the algorithm recommendation provisions may trigger warnings, criticism notices, orders to rectify, suspension of information updates, and fines of RMB 10,000 to RMB 100,000 where no other law provides otherwise; other violations are handled under other applicable laws and regulations [\[1-6\]](#). The Cybersecurity Law, Data Security Law, and PIPL serve as enforcement overlays [\[1-4\]](#)[\[1-5\]](#)[\[1-6\]](#).

4.5 Compliance Burden Assessment

China's regime imposes the highest compliance burden on providers of public-facing AI services operating in mainland China. The combination of content-control obligations, security assessments, algorithm filing, labeling duties (explicit and implicit), and data/personal-information compliance creates a dense regulatory layer. The content-control dimension—requiring alignment with state content standards—is a fundamental point of divergence from all other jurisdictions covered in this report and represents a potentially irreconcilable compliance asymmetry for global model developers [\[1-4\]](#)[\[1-5\]](#).

China's regime stands apart from the transnational governance layer. The Council of Europe Convention's human-rights framing [\[5-1\]](#)[\[5-3\]](#) and the HAIP Code of Conduct's transparency and documentation topics [\[5-5\]](#)[\[5-6\]](#) do not map onto China's content-control and state-oversight requirements. Organizations operating in both China and Western markets face fundamentally incompatible compliance architectures for the content and values dimensions of AI governance.

5. United Kingdom

5.1 Legal Status and Structure

The UK has not enacted a single comprehensive AI law equivalent to the EU AI Act. The current model relies on existing regulators and laws, supplemented by AI-specific guidance and public-policy programs [\[1-8\]](#)[\[1-9\]](#). However, the question of cross-sector AI legislation is not dormant: a 2026 House of Lords Library briefing states the UK government's approach remains based on the 2023 white paper's sector-led framework but discusses active debate on whether cross-sector AI legislation is needed [\[6-9\]](#). This indicates that binding AI legislation remains a live possibility in the UK, even if no specific timeline has been announced.

5.2 Institutional and Policy Direction

The UK government published the AI Opportunities Action Plan and issued a formal government response in January 2025. The Plan states the UK should invest in compute, data infrastructure, talent, and regulation, and that regulation, safety, and assurance can support AI adoption and growth [\[1-8\]](#)[\[1-34\]](#).

5.3 Obligations

For both model developers/providers and deployers, binding duties arise primarily through existing laws: UK GDPR/data protection, consumer protection, equality law, product-safety rules, online safety/content rules, procurement, and sectoral supervision [\[1-9\]](#). The ICO's guidance on AI and data protection addresses lawfulness, fairness, transparency, governance, accuracy, security, and individual rights for AI processing personal data [\[1-9\]](#).

5.4 Compliance Burden Assessment

The UK's compliance burden is moderate and distributed across multiple existing legal frameworks rather than concentrated in a single AI statute. The absence of a dedicated AI act means there are no AI-specific conformity assessments, model documentation mandates, or risk-tier classifications. However, the cumulative weight of UK GDPR, consumer protection, equality, and sectoral rules creates meaningful obligations, particularly for deployers processing personal data.

The UK's position is influenced by the transnational layer. The UK participated in negotiating the Council of Europe Convention and is among its signatories [\[5-1\]](#); if the UK ratifies the treaty, it will be required to adopt or maintain domestic measures consistent with the Convention's human-rights, democracy, and rule-of-law standards [\[5-3\]](#)—potentially catalyzing the binding AI legislation currently under parliamentary debate [\[6-9\]](#).

6. Japan

6.1 Legal Status

Japan enacted its first AI-specific statute in 2025, but its substantive approach remains light-touch. The **AI Promotion Act** (Act on the Promotion of Research and Development and Utilization of AI-Related Technologies) was passed by the Diet on 28 May 2025, promulgated on 4 June 2025, and came into full effect in September 2025 [\[1-46\]](#). It is a framework ("basic") law: it sets national policy direction, establishes an AI Strategy Headquarters and an AI Basic Plan, and frames private-sector responsibilities as best-effort cooperation rather than enforceable mandates—it imposes no AI-specific penalties [\[1-46\]](#). Japan's operative cross-sector expectations therefore continue to flow from soft-law guidance: METI and MIC published the AI Guidelines for Business Version

1.0 in April 2024 and Version 1.1 on 28 March 2025 [\[1-10\]](#), with binding obligations arising only through data-protection, copyright, and sectoral law.

6.2 Scope and Actor Categories

The guidelines distinguish AI business actors, including developers, providers, and business users, and organize expected actions by role [\[1-10\]](#).

6.3 Obligations and Themes

The guidelines address governance, safety, transparency, security, privacy, human rights/fairness, and role-based responsibilities rather than statutory fines [\[1-10\]](#). The Japan AI Safety Institute (J-AISI) describes the updated guideline version as part of Japan's safety infrastructure [\[1-35\]](#).

6.4 Copyright/Training-Data Overlay

Japan's Agency for Cultural Affairs published "General Understanding on AI and Copyright in Japan," clarifying copyright issues around AI training and outputs [\[1-36\]](#).

6.5 Japan's Role in the Transnational Layer

Japan's significance in the global AI governance landscape extends beyond its domestic soft-law approach. Japan hosted the G7 Hiroshima Summit that launched the HAIP in May 2023 [\[5-4\]](#) and continues to operate the official HAIP Reporting Framework page [\[5-7\]](#). Japan also participated in negotiating the Council of Europe Convention as an observer state [\[5-1\]](#). This means Japan is simultaneously maintaining a light-touch domestic regime and playing a leading role in building the transnational governance infrastructure that shapes global AI compliance expectations.

6.6 Compliance Burden Assessment

Japan's compliance burden is low relative to the EU, China, or the U.S., given the non-binding nature of the guidelines. Binding obligations arise primarily through Japan's data protection and sectoral laws. The guidelines' role-based structure mirrors actor-category distinctions appearing in binding regimes elsewhere, facilitating governance mapping across jurisdictions.

7. South Korea

7.1 Legal Status and Timeline

South Korea adopted the Framework Act on Artificial Intelligence Development and Establishment of a Foundation for Trustworthiness in January 2025. Both the Act and its **Enforcement Decree took effect on 22 January 2026** [6-7]. This makes South Korea, alongside the EU, one of only two jurisdictions with a comprehensive enacted AI-specific statute, and the existence of an effective Enforcement Decree means South Korea has moved beyond statute-only status into operational implementation. That said, MSIT is operating a grace period of at least one year in 2026, during which fact-finding investigations and administrative fines are generally deferred except in cases of serious social harm, so near-term enforcement risk is lower than the in-force date alone suggests [6-7].

7.2 Scope, Reach, and Domestic-Agent Requirements

The Act applies to AI development business operators and AI utilization business operators and has extraterritorial application for certain businesses offering products or services in Korea [1-2]. The Enforcement Decree includes provisions on methods for implementing transparency obligations for generative and high-impact AI business operators, criteria for defining high-performance AI, standards for determining high-impact AI, and the scope of operators required to designate a **domestic agent** [6-8]. This domestic-agent requirement is particularly significant for foreign model developers and AI service providers, as it creates a concrete in-country compliance presence obligation analogous to GDPR representative requirements.

7.3 Risk Model

The Act distinguishes "generative AI" and "high-impact AI." High-impact AI is defined as AI significantly affecting human life, physical safety, or fundamental rights [1-2].

7.4 Obligations: Developers/Providers

Businesses providing generative AI or high-impact AI have transparency duties, including requirements to notify users when operations use generative or high-impact AI and to label outputs produced by generative AI, including deepfakes [1-2][1-38].

High-impact AI operators face obligations concerning safety and reliability [\[1-38\]](#). The Enforcement Decree specifies the methods for implementing these transparency obligations [\[6-8\]](#).

7.5 Penalties

Public analyses describe lower financial penalties than the EU model. The U.S. Department of Commerce trade note identifies the Act as a comprehensive framework creating new compliance requirements [\[1-2\]](#)[\[1-37\]](#).

7.6 Compliance Burden Assessment

South Korea's regime is binding, comprehensive, and now operationally implemented through the Enforcement Decree [\[6-7\]](#)[\[6-8\]](#). The compliance burden is moderate: lower than the EU AI Act in terms of financial penalties and the absence of comparable three-layer implementation machinery, but higher than previously assessed given the Enforcement Decree's specific transparency methods, high-impact AI determination criteria, and domestic-agent requirements for foreign operators [\[6-8\]](#). The extraterritorial reach means that foreign model developers and deployers offering products or services in Korea face a concrete and enforceable compliance obligation.

8. Brazil

8.1 Legal Status

Brazil's principal AI framework remains proposed rather than enacted. PL 2338/2023 has **passed the Senate and is now being processed by the Chamber of Deputies (House of Representatives)** [\[6-10\]](#)[\[6-11\]](#). This represents meaningful legislative progress: the bill is no longer an undifferentiated congressional proposal but has cleared one chamber and is in the final legislative stage before potential enactment.

8.2 Core Bill Structure

Available summaries describe a risk-based bill establishing general standards for development, implementation, and responsible use of AI systems, with governance duties and impact assessments for high-risk systems [\[1-11\]](#)[\[1-39\]](#).

8.3 Current Binding Overlays and Emerging Regulatory Activity

Until any AI bill is enacted, Brazil's binding controls relevant to AI come primarily from the LGPD data protection law and sectoral/consumer frameworks [\[1-11\]](#). However, the Brazilian national data protection authority (ANPD) is already building a technical interpretation layer for generative AI under existing LGPD-based oversight. The ANPD released an English-language version of its *Technology Radar – Generative Artificial Intelligence* in December 2024, addressing topics such as data scraping/web scraping and synthetic content generation, both of which may involve personal data processing [\[3-7\]](#). This means Brazil's immediate AI compliance burden is being shaped not only by the pending AI bill and LGPD enforcement generally, but by regulator-authored technical framing of generative AI issues under existing law [\[3-7\]](#).

8.4 Compliance Burden Assessment

The current compliance burden is limited to LGPD and consumer-law obligations, but the ANPD's Technology Radar work signals that regulator expectations around AI-related data processing are becoming more specific. The bill's passage through the Senate [\[6-10\]](#)[\[6-11\]](#) increases the probability of enactment in the near term. If PL 2338/2023 is enacted in a form resembling current summaries, Brazil would join the EU and South Korea in the category of jurisdictions with comprehensive, risk-based AI statutes.

9. India

9.1 Legal Status and Scope

India does not have a dedicated enacted cross-sector AI statute. The current framework is based on the Digital Personal Data Protection Act (DPDP Act) 2023, the IT Act, the Intermediary Guidelines and Digital Media Ethics Code Rules 2021 (as amended), cyber advisories, and MeitY advisories [\[1-12\]](#)[\[1-13\]](#).

9.2 MeitY Advisory and Platform Obligations

MeitY's 2024 advisory instructed intermediaries and platforms to ensure that AI/LLM/generative AI software or algorithms do not permit users to host, display,

upload, modify, publish, transmit, store, update, or share unlawful content under the IT Rules framework [\[1-12\]](#).

9.3 Data Protection Overlay

The DPDP Act 2023 applies extraterritorially where processing outside India is connected with offering goods or services to individuals in India [\[1-13\]](#).

9.4 Deepfakes and Online Harms

A 2025 government statement to Parliament identifies the IT Act 2000 and the IT Rules 2021 as the core legal framework used to address deepfakes and related cyber harms, including sections on identity theft, impersonation, privacy violations, obscene/sexually explicit content, blocking orders, and intermediary notice/removal powers [\[1-40\]](#).

9.5 Compliance Burden Assessment

India's current AI compliance burden is moderate and arises primarily from the DPDP Act's extraterritorial reach and the IT intermediary framework. The absence of a dedicated AI statute means no AI-specific conformity assessments, risk tiers, or model documentation requirements exist.

10. Gulf Region (GCC)

10.1 Regional Overview

No GCC-wide binding AI law was identified. The landscape is composed of national strategies, data protection laws, cybersecurity rules, sector guidance, and selective AI-specific governance measures [\[1-14\]](#)[\[1-16\]](#)[\[1-41\]](#). No evidence was found of a binding UAE federal omnibus AI law despite some public claims online; credible regulatory trackers confirm the UAE does not have a specific standalone AI law and instead relies on strategies, ethical frameworks, data-protection laws, and free-zone regimes [\[6-17\]](#)[\[6-18\]](#).

10.2 United Arab Emirates

There is no dedicated federal AI law in force in the UAE [\[6-17\]](#)[\[6-18\]](#). The applicable framework is built from personal-data and sector rules plus strategy/policy documents [\[1-15\]](#).

DIFC Regulation 10, enacted 1 September 2023, specifically regulates processing personal data through autonomous and semi-autonomous systems, including AI. DIFC describes Regulation 10 as a risk- and outcomes-based framework and provides an accreditation/certification architecture [\[1-15\]](#). Abu Dhabi created the Artificial Intelligence and Advanced Technology Council under Law No. 3 of 2024 [\[1-14\]](#).

The UAE has adopted the **UAE Charter for the Development and Use of Artificial Intelligence**, a policy instrument published on the official legislation portal that aims to achieve the strategic goals of the UAE AI Strategy [\[3-8\]](#). While not a standalone AI statute, the Charter provides a formal national governance reference point that applies conceptually across sectors [\[3-8\]](#).

10.3 Saudi Arabia

Saudi Arabia's binding baseline is the Personal Data Protection Law (PDPL) and related data/cyber rules [\[1-16\]](#)[\[1-42\]](#). SDAIA's Generative Artificial Intelligence Guidelines for Government require alignment with personal data protection, cybersecurity standards, data-classification rules, and AI Ethics Principles [\[1-42\]](#).

Saudi Arabia's AI Ethics Principles are more structured than a generic principles statement. SDAIA's official document sets out **lifecycle-oriented controls** covering planning and design, input data preparation, building and validation, and deployment and monitoring [\[3-9\]](#). The substantive principles include fairness, privacy and security, humanity, social and environmental benefits, reliability and safety, transparency and explainability, and accountability and responsibility [\[3-9\]](#). The framework incorporates **risk categorization** and defined **organizational roles and responsibilities** for adopting entities [\[3-10\]](#)[\[3-11\]](#). While not statutory mandates, these indicate that Saudi Arabia's guidance is moving beyond abstract ethics into implementable governance design resembling the management-system controls found in ISO/IEC 42001 and the NIST AI RMF.

10.4 Qatar

Qatar has a National Artificial Intelligence Strategy and a federal data protection law, Law No. 13 of 2016 [\[1-44\]](#)[\[1-45\]](#). The national AI strategy includes an "AI Ethics and

Governance" pillar and states that explainability guidelines are needed for different types of AI decisions [\[1-44\]](#).

10.5 Bahrain, Kuwait, and Oman

Bahrain is characterized as active on digital policy and data protection, but no enacted cross-sector AI law was identified [\[1-14\]](#)[\[1-41\]](#). Kuwait is in early stages of developing an AI regulatory framework aligned with Vision 2035 [\[1-41\]](#). Oman has a draft National Artificial Intelligence Policy defining governance for data management and development/use of AI systems [\[1-41\]](#).

10.6 Compliance Burden Assessment

The GCC region presents a relatively low AI-specific compliance burden compared to the EU, China, or the U.S. The DIFC's Regulation 10 is the most developed AI-specific binding regime in the region, but it applies only within the DIFC free zone. Government-sector AI users in Saudi Arabia face additional guidance-based obligations through SDAIA's guidelines and ethics framework. The UAE Charter and Saudi AI Ethics Principles add governance expectations that, while not legally binding in the manner of the EU AI Act, are increasingly structured enough to influence procurement decisions, public-sector requirements, and organizational governance practices.

11. The Global Governance Infrastructure Layer

11.1 A Second Layer Beyond Formal Law

By mid-2026, a parallel layer of non-binding but operationally consequential governance infrastructure has emerged alongside formal legislation. This layer includes international standards, incident-reporting frameworks, technical guidance, privacy-regulator technical studies, and national AI charters [\[3-1\]](#)[\[3-2\]](#)[\[3-4\]](#)[\[3-5\]](#)[\[3-7\]](#)[\[3-8\]](#)[\[3-9\]](#).

11.2 ISO/IEC 42001: The Global Management-System Baseline

ISO/IEC 42001:2023 is the world's first AI management system standard. It specifies requirements for establishing, implementing, maintaining, and continually improving an AI management system (AIMS) within organizations [\[3-1\]](#). The standard is designed for

entities **providing or utilizing AI-based products or services**, mapping directly onto the developer/provider versus deployer/user split [\[3-1\]](#). It is process-focused rather than model- or sector-specific, offering a management-system structure rather than prescribing prohibited practices or high-risk categories [\[3-1\]](#).

11.3 NIST Generative AI Profile

NIST AI 600-1 provides detailed voluntary risk-management guidance for generative AI contexts [\[3-4\]](#). Its recommended lifecycle controls—acceptable-use policies, data provenance information, human-oversight roles, incident response plans, disclosure notices, and risk hierarchies—converge operationally with concepts embedded in the EU AI Act, Colorado's revised developer documentation requirements, and South Korea's AI Basic Act [\[3-4\]](#).

11.4 OECD Incident-Reporting Framework

The OECD's 2025 paper *Towards a common reporting framework for AI incidents* contains 29 criteria intended to help policymakers understand AI incidents across diverse contexts [\[3-2\]](#). The OECD's AI Incidents and Hazards Monitor is developing definitions and monitoring through a common reporting framework, supported by an Expert Group on AI Incidents [\[3-3\]](#). The framework distinguishes between AI incidents and AI hazards, includes fields for quantifying harm, and is actor- and sector-neutral [\[3-2\]](#)[\[3-3\]](#).

11.5 EU Harmonised Standards

Within the EU specifically, harmonised standards published by CEN and CENELEC, once referenced in the Official Journal, will provide a **presumption of conformity** with the AI Act [\[3-5\]](#)[\[3-6\]](#). The Digital Omnibus proposal of 19 November 2025 explicitly proposed linking the application of rules for high-risk AI systems to the availability of support tools, including standards [\[3-5\]](#).

11.6 Convergence Through Infrastructure

Across ISO/IEC 42001, the NIST Generative AI Profile, the OECD incident framework, EU standardization, Brazil's ANPD Technology Radar, the UAE Charter, Saudi AI Ethics Principles, and the HAIP Reporting Framework, recurring themes include governance systems, documentation, data provenance, monitoring, human oversight, incident

handling, transparency, and lifecycle controls [\[3-1\]](#)[\[3-2\]](#)[\[3-4\]](#)[\[3-5\]](#)[\[3-7\]](#)[\[3-8\]](#)[\[3-9\]](#)[\[5-5\]](#)[\[5-6\]](#)[\[5-8\]](#). This convergence is distinct from convergence in formal law: jurisdictions remain divergent on penalties, enforcement powers, and prohibited practices, but they are increasingly similar in the kinds of internal controls they expect organizations to build.

12. Cross-Jurisdictional Convergence and Divergence

12.1 Areas of Convergence

Several regulatory concepts are converging across jurisdictions, reinforced by formal law, governance infrastructure, and the transnational layer:

- **Transparency and disclosure:** EU Article 50 disclosures and mandatory training-data summary template [\[1-1\]](#)[\[2-9\]](#), Utah consumer disclosures [\[1-21\]](#), South Korea generative-AI notices/labeling with Enforcement Decree-specified methods [\[1-2\]](#)[\[1-38\]](#)[\[6-8\]](#), China mandatory explicit/implicit labeling [\[1-7\]](#), NYC applicant notice [\[1-25\]](#), Illinois candidate notice [\[1-26\]](#), HAIP Code of Conduct transparency reports [\[5-5\]](#)[\[5-6\]](#), FTC enforcement against unsubstantiated AI claims [\[4-3\]](#)[\[4-4\]](#), Qatar strategy references to explainability [\[1-44\]](#), Saudi/UAE guidance [\[1-42\]](#)[\[3-8\]](#).
- **Risk and impact assessments:** EU conformity/risk management and deployer FRIAs [\[1-1\]](#), California CPPA ADMT risk assessments (phased from Jan 2026) [\[6-4\]](#)[\[6-5\]](#), privacy-law assessments in Virginia and Connecticut [\[1-28\]](#)[\[1-30\]](#), DIFC Regulation 10 [\[1-15\]](#), Saudi risk categorization [\[3-10\]](#)[\[3-11\]](#), Council of Europe Convention's graduated-and-differentiated approach [\[5-3\]](#). Colorado's deployer impact-assessment requirement has been removed by SB26-189 [\[6-2\]](#)[\[6-3\]](#), narrowing the U.S. convergence with EU-style deployer assessments.
- **Human oversight and contestability:** EU high-risk rules [\[1-1\]](#), UK data protection guidance [\[1-9\]](#), Colorado's revised human review-related rights [\[6-1\]](#)[\[6-2\]](#), U.S. privacy/employment frameworks [\[1-25\]](#), NIST Profile recommendations [\[3-4\]](#), HAIP Code of Conduct [\[5-5\]](#).
- **Data governance, privacy, and security:** Central in EU [\[1-1\]](#), China [\[1-4\]](#), UK ICO guidance [\[1-9\]](#), India DPDP [\[1-13\]](#), UAE/DIFC [\[1-15\]](#), Saudi PDPL/SDAIA [\[1-42\]](#), Brazil ANPD [\[3-7\]](#), California CPPA [\[6-4\]](#).
- **Documentation and model information:** EU GPAI and high-risk providers (with prescribed template [\[2-9\]](#)), Colorado developers (documentation transfer retained under SB26-189 [\[6-1\]](#)), China filing/security processes [\[1-4\]](#), HAIP Code of

Conduct documentation requirements [\[5-5\]](#)[\[5-6\]](#), NIST Profile model versioning [\[3-4\]](#).

- **Content labeling and synthetic media controls:** Strong in China [\[1-7\]](#), present in South Korea [\[1-38\]](#) and several U.S. states [\[1-32\]](#).
- **Internal governance systems:** EU AI Pact governance pledges [\[2-7\]](#), EU GPAI Code of Practice [\[2-8\]](#), ISO/IEC 42001 management-system structure [\[3-1\]](#), NIST lifecycle controls [\[3-4\]](#), Saudi lifecycle-oriented ethics framework [\[3-9\]](#), HAIP Reporting Framework organizational governance disclosures [\[5-7\]](#)[\[5-8\]](#).
- **Incident handling and post-deployment monitoring:** EU serious incident reporting [\[1-1\]](#), OECD 29-criterion incident framework [\[3-2\]](#)[\[3-3\]](#), NIST incident response plans [\[3-4\]](#), China security assessment/oversight [\[1-4\]](#).
- **Vendor-documentation transmission:** EU provider-to-deployer documentation [\[1-1\]](#), Colorado developer-to-deployer packages (retained under SB26-189 [\[6-1\]](#)), EEOC vendor-management expectations [\[4-12\]](#).
- **Lifecycle-oriented governance:** Council of Europe Convention lifecycle approach [\[5-1\]](#), HAIP lifecycle actions [\[5-5\]](#), ISO/IEC 42001 lifecycle management [\[3-1\]](#), Saudi AI Ethics Principles lifecycle controls [\[3-9\]](#), NIST lifecycle framework [\[3-4\]](#).

12.2 Areas of Material Divergence

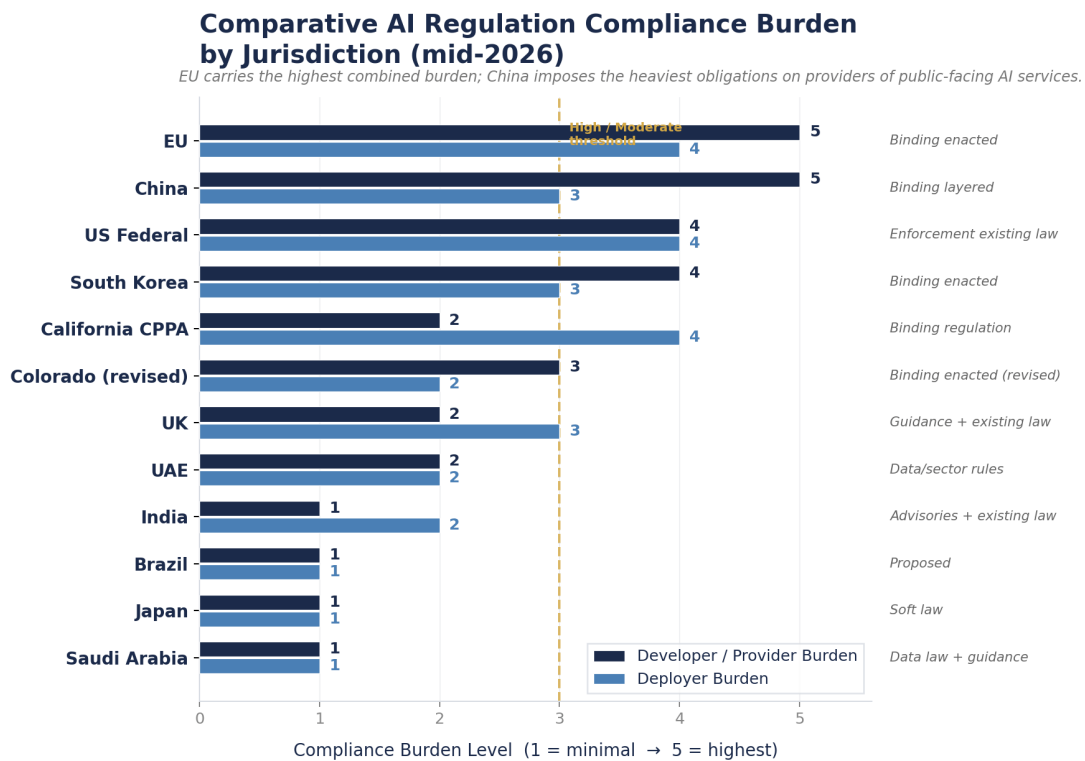
Several points of divergence are potentially irreconcilable for global AI products:

1. **Content control:** China's content-control obligations have no equivalent in any other jurisdiction and create a fundamental compliance asymmetry for global model developers [\[1-4\]](#)[\[1-5\]](#). The Council of Europe Convention's human-rights framing [\[5-1\]](#) and the HAIP Code of Conduct's transparency approach [\[5-5\]](#) are structurally incompatible with China's content-alignment requirements.
2. **Regulatory architecture:** The EU's single omnibus risk-tier statute with three-layer compliance ecosystem versus China's layered activity-specific measures versus the U.S. dual-layer system versus the UK's regulator-led approach creates structurally incompatible frameworks. The EU's formal coordination through the European AI Board [\[2-2\]](#) and harmonised-standards pathway [\[3-5\]](#)[\[3-6\]](#) contrasts with the entirely uncoordinated U.S. state landscape.
3. **Penalty scale and enforcement mechanism:** The EU's fines of up to EUR 35 million or 7% of worldwide annual turnover dwarf other jurisdictions [\[1-1\]](#). China's RMB 10,000–100,000 fines under algorithmic recommendation rules are modest [\[1-6\]](#), and South Korea's penalties are described as lower than the EU model [\[1-2\]](#). In

the U.S., the FTC operates through consent orders and monetary relief rather than a statutory fine schedule [\[4-4\]](#)[\[4-5\]](#).

4. **Developer versus deployer allocation:** The EU places substantial obligations on both [\[1-1\]](#). China focuses primarily on public-facing service providers [\[1-4\]](#). Colorado's revised regime retains developer documentation duties but has scaled back deployer obligations [\[6-1\]](#)[\[6-2\]](#)[\[6-3\]](#). Many U.S. states regulate only deployers in specific contexts [\[1-25\]](#)[\[1-26\]](#). California's CPPA rules focus on deployers using ADMT for significant decisions [\[6-4\]](#)[\[6-6\]](#).
5. **Extraterritorial reach:** The EU AI Act, South Korea's AI Basic Act (with domestic-agent requirements [\[6-8\]](#)), India's DPDP Act, and the Council of Europe Convention (through state implementation obligations) all assert cross-border application through different mechanisms [\[1-1\]](#)[\[1-2\]](#)[\[1-13\]](#)[\[5-1\]](#)[\[5-3\]](#).
6. **Implementation depth:** The EU's proceduralized implementation—templates, codes, expert panels, pre-compliance initiatives, harmonised-standards pathways—is unmatched [\[2-1\]](#)[\[2-8\]](#)[\[2-9\]](#)[\[3-5\]](#)[\[3-6\]](#), though it has been accompanied by missed guidance deadlines and industry contestation [\[6-12\]](#)[\[6-13\]](#)[\[6-15\]](#).
7. **Binding versus non-binding status:** The same organizational control—a documented risk management system or incident response plan—may be legally required in one jurisdiction (EU), effectively required through enforcement risk in another (U.S. FTC/EEOC), expected under a treaty obligation that awaits domestic implementation (Council of Europe Convention Parties), voluntarily disclosed through a reporting framework (HAIP), and merely recommended in a third (Japan, UK, Gulf).

13. Comparative Classification Matrix



EU — Binding enacted law + harmonised standards pathway

- **Risk model:** 4-tier risk + GPAI
- **Developer/provider burden:** Very high
- **Deployer/user burden:** High
- **Enforcement:** AI Office + national MSAs + AI Board + Scientific Panel + Advisory Forum + CEN-CENELEC [\[2-1\]](#)[\[2-2\]](#)[\[2-3\]](#)[\[2-4\]](#)[\[3-5\]](#)[\[3-6\]](#)
- **Penalty ceiling:** EUR 35M / 7% turnover [\[1-1\]](#)
- **Key dates:** Phased (statutory): Feb 2025–Aug 2026, embedded-product Aug 2027; Digital Omnibus (provisional, pending adoption) would defer Annex III to Dec 2027 and embedded-product to Aug 2028 [\[1-1\]](#)[\[2-6\]](#)

U.S. (federal enforcement) — Enforcement through existing law

- **Risk model:** No AI-specific tiers
- **Developer/provider burden:** High (AI-washing/claims) [\[4-3\]](#)[\[4-4\]](#)
- **Deployer/user burden:** High (employment/privacy) [\[6-4\]](#)[\[4-11\]](#)[\[4-12\]](#)
- **Enforcement:** FTC + EEOC + CPPA (uncoordinated) [\[4-1\]](#)[\[4-2\]](#)[\[6-4\]](#)
- **Penalty ceiling:** Varies by agency/case
- **Key dates:** Ongoing

Colorado (revised) — Binding enacted law (repealed and reenacted by SB26-189)

- **Risk model:** Consequential-decision ADMT

- **Developer/provider burden:** Moderate (documentation transfer) [\[6-1\]](#)
- **Deployer/user burden:** Low–moderate (consumer notice, human review rights; no impact assessment) [\[6-1\]](#)[\[6-2\]](#)[\[6-3\]](#)
- **Enforcement:** AG enforcement
- **Penalty ceiling:** AG enforcement
- **Key dates:** Developer obligations: 1 Jan 2027 [\[6-1\]](#)

California (CPPA) — Binding regulation under privacy law

- **Risk model:** Significant-decision ADMT (narrower than AI statute) [\[6-6\]](#)
- **Developer/provider burden:** Low–moderate
- **Deployer/user burden:** High [\[6-4\]](#)[\[6-5\]](#)
- **Enforcement:** CPPA [\[6-4\]](#)
- **Penalty ceiling:** CCPA penalties
- **Key dates:** Risk assessments: Jan 2026; ADMT: Jan 2027; reporting: Apr 2028 [\[6-4\]](#)[\[6-5\]](#)

South Korea — Binding enacted law + Enforcement Decree

- **Risk model:** Generative AI + high-impact AI
- **Developer/provider burden:** Moderate–high (with domestic-agent requirement for foreign operators) [\[6-7\]](#)[\[6-8\]](#)
- **Deployer/user burden:** Moderate
- **Enforcement:** Government authorities [\[1-2\]](#)
- **Penalty ceiling:** Lower than EU [\[1-2\]](#)
- **Key dates:** 22 Jan 2026 (Act + Decree) [\[6-7\]](#)

China — Binding administrative measures (layered)

- **Risk model:** Activity/content-based
- **Developer/provider burden:** Very high (public-facing)
- **Deployer/user burden:** Moderate
- **Enforcement:** CAC + multi-agency [\[1-4\]](#)[\[1-6\]](#)
- **Penalty ceiling:** RMB 10K–100K + overlay laws [\[1-6\]](#)
- **Key dates:** Various (2022–2025)

UK — Regulator guidance + existing law (cross-sector legislation under active parliamentary debate [\[6-9\]](#))

- **Risk model:** No AI-specific tiers
- **Developer/provider burden:** Low (AI-specific)
- **Deployer/user burden:** Moderate (existing law)

- **Enforcement:** Existing sectoral regulators + ICO [\[1-9\]](#)
- **Penalty ceiling:** Varies by underlying law
- **Key dates:** Ongoing

Japan — Basic law (AI Promotion Act, 2025; non-binding) + soft-law guidance

- **Risk model:** No binding tiers
- **Developer/provider burden:** Low
- **Deployer/user burden:** Low
- **Enforcement:** AI Strategy HQ (policy) + sectoral regulators
- **Penalty ceiling:** None (AI-specific; no penalties)
- **Key dates:** AI Promotion Act in force Sep 2025; Guidelines v1.1 Mar 2025 [\[1-46\]](#)[\[1-10\]](#)

Brazil — Proposed bill (passed Senate, in Chamber of Deputies [\[6-10\]](#)[\[6-11\]](#)) + existing law + ANPD analysis

- **Risk model:** Risk-based (proposed)
- **Developer/provider burden:** Low (current)
- **Deployer/user burden:** Low (current)
- **Enforcement:** ANPD + LGPD + sectoral [\[1-11\]](#)[\[3-7\]](#)
- **Penalty ceiling:** LGPD/consumer law
- **Key dates:** Pending

India — Advisories + existing law

- **Risk model:** No AI-specific tiers
- **Developer/provider burden:** Low
- **Deployer/user burden:** Low–moderate
- **Enforcement:** MeitY + sectoral [\[1-12\]](#)[\[1-13\]](#)
- **Penalty ceiling:** DPDP/IT Act
- **Key dates:** Ongoing

UAE — Data/sector rules + free-zone regulation + charter; no federal AI law [\[6-17\]](#)[\[6-18\]](#)

- **Risk model:** DIFC risk-based (limited scope)
- **Developer/provider burden:** Low–moderate
- **Deployer/user burden:** Low–moderate
- **Enforcement:** Data commissioners + free-zone authorities [\[1-15\]](#)[\[3-8\]](#)
- **Penalty ceiling:** Data law penalties
- **Key dates:** DIFC Reg 10: Sep 2023 [\[1-15\]](#)

Saudi Arabia — Data law + structured ethics/guidance

- **Risk model:** Risk categorization in guidance [\[3-10\]](#)[\[3-11\]](#)
- **Developer/provider burden:** Low
- **Deployer/user burden:** Low
- **Enforcement:** SDAIA + PDPL authority [\[1-16\]](#)[\[1-42\]](#)
- **Penalty ceiling:** PDPL penalties
- **Key dates:** Ongoing

Qatar — Strategy + data law

- **Risk model:** No binding AI tiers
- **Developer/provider burden:** Low
- **Deployer/user burden:** Low
- **Enforcement:** Data protection authority [\[1-44\]](#)[\[1-45\]](#)
- **Penalty ceiling:** Data law penalties
- **Key dates:** Ongoing

Council of Europe Convention — Binding international treaty (framework)

- **Risk model:** Risk-based, lifecycle [\[5-1\]](#)[\[5-3\]](#)
- **Developer/provider burden:** Indirect (through state implementation)
- **Deployer/user burden:** Indirect (through state implementation)
- **Enforcement:** State parties' domestic measures [\[5-3\]](#)
- **Penalty ceiling:** Determined by domestic law
- **Key dates:** Opened for signature Sep 2024 [\[5-2\]](#)

G7 HAIP — Voluntary code + reporting framework

- **Risk model:** Lifecycle-based [\[5-5\]](#)
- **Developer/provider burden:** Moderate (governance expectations) [\[5-5\]](#)[\[5-8\]](#)
- **Deployer/user burden:** Moderate (now open to deployers) [\[5-8\]](#)
- **Enforcement:** Voluntary / OECD publication [\[5-8\]](#)
- **Penalty ceiling:** None
- **Key dates:** Code: Dec 2023; Reporting: Feb 2025 [\[5-4\]](#)[\[5-7\]](#)

Global non-binding layer — ISO/IEC 42001, NIST AI 600-1, OECD incident framework

- **Risk model:** Process/lifecycle-based
- **Developer/provider burden:** Moderate (governance expectations)
- **Deployer/user burden:** Moderate (governance expectations)
- **Enforcement:** Voluntary / procurement-driven [\[3-1\]](#)[\[3-2\]](#)[\[3-4\]](#)

- **Penalty ceiling:** None
- **Key dates:** Active (2023–2026)

14. Operational Burden: Developers versus Deployers

The following section details the compliance burden ranking for both model developers/providers and deployers/users across jurisdictions. See Figure 4 above for a visual comparison.

14.1 Highest Burden for Model Developers/Providers

1. **EU:** GPAI providers face the AI Office's centralized enforcement, Scientific Panel scrutiny, the GPAI Code of Practice's two-track presumption structure [\[6-14\]](#), a mandatory training-data transparency template [\[2-9\]](#), and the emerging harmonised-standards pathway [\[3-5\]](#)[\[3-6\]](#). High-risk system providers face conformity assessments, technical documentation, post-market monitoring, and incident reporting [\[1-1\]](#). The EU's burden on model developers is the highest globally. The implementation friction documented through missed guidance deadlines [\[6-15\]](#) and industry contestation [\[6-12\]](#)[\[6-13\]](#) adds near-term uncertainty to the compliance experience without reducing the underlying legal obligations.
2. **China:** Public-facing service providers face content-control, security assessment, algorithm filing, labeling, and data/personal-information compliance [\[1-4\]](#)[\[1-5\]](#)[\[1-6\]](#)[\[1-7\]](#). The content-control dimension adds a compliance burden with no equivalent elsewhere.
3. **United States (federal enforcement layer):** The FTC's enforcement of AI capability claims and "AI-washing" creates a substantiation burden that directly affects model vendors and AI application developers [\[4-1\]](#)[\[4-3\]](#)[\[4-4\]](#).
4. **Colorado (revised):** Developers of covered ADMT must provide deployers with technical documentation on intended uses, training-data categories, known limitations, and instructions for appropriate use and human review, effective 1 January 2027 [\[6-1\]](#). The original duty-of-care requirement has been removed [\[6-2\]](#)[\[6-3\]](#), reducing the developer burden from the original SB 24-205 level.

5. **South Korea:** AI development operators face transparency and safety/reliability obligations for generative and high-impact AI, with Enforcement Decree-specified methods and domestic-agent requirements for foreign operators [\[1-2\]](#)[\[1-38\]](#)[\[6-7\]](#)[\[6-8\]](#).

14.2 Highest Burden for Deployers/Users/Integrators

1. **EU:** Deployers of high-risk systems face human-oversight, monitoring, logging, incident-reporting, and fundamental-rights impact assessment duties [\[1-1\]](#). Enforcement flows through national market surveillance authorities [\[2-2\]](#).
2. **California (CPPA):** Businesses using ADMT for significant decisions face notice, opt-out, risk-assessment, and reporting obligations, phased from January 2026 through April 2028 [\[6-4\]](#)[\[6-5\]](#)[\[6-6\]](#). The rules are narrower than an AI statute—applying only where technology replaces or substantially replaces human decision-making [\[6-6\]](#)—but they represent the most operationally significant U.S. deployer-facing AI-adjacent regime.
3. **U.S. employment context (EEOC + state rules):** Employers face Title VII disparate-impact liability [\[4-12\]](#), with vendor-management obligations to obtain adverse-impact testing evidence [\[4-12\]](#). NYC's Local Law 144 requires annual bias audits, public posting, and applicant notice [\[1-25\]](#). Illinois's AI Video Interview Act requires notification, explanation, consent, and data-handling controls [\[1-26\]](#).
4. **Colorado (revised):** Deployers retain consumer-notice, adverse-decision explanation, and human review-related rights obligations, but the original impact-assessment and risk-management program requirements have been removed [\[6-1\]](#)[\[6-2\]](#)[\[6-3\]](#). Colorado's deployer burden is now substantially lighter than the EU's or California's CPPA regime.
5. **U.S. privacy-law states:** Connecticut, Virginia, Alabama, and others impose profiling opt-outs, impact assessments, and automated-decision-making rights [\[1-28\]](#)[\[1-30\]](#)[\[1-3\]](#).
6. **UK:** Deployers face existing-law compliance across data protection, consumer protection, equality, and sectoral supervision [\[1-9\]](#).

14.3 The Provider/Deployer Split: A Structural Feature

The EU and the United States have each institutionalized the distinction between developer/provider and deployer compliance, but through fundamentally different mechanisms:

In the EU, the split is built into the enforcement architecture itself. GPAI model providers are subject to the AI Office's centralized oversight and dedicated implementation tools [\[2-1\]\[2-4\]\[2-8\]\[2-9\]](#). Deployers are primarily subject to national market surveillance authorities [\[2-2\]](#).

In the United States, the split emerges from the fragmented enforcement landscape. The FTC targets providers [\[4-1\]\[4-3\]\[4-4\]](#). Employment and privacy rules target deployers with indirect vendor pressure [\[6-4\]\[4-11\]\[4-12\]](#). Colorado's revised SB26-189 retains the developer-to-deployer documentation transmission mechanism but has removed the deployer-side impact assessment and risk-management program [\[6-1\]\[6-2\]\[6-3\]](#), making the U.S. developer/deployer split less symmetrical than the EU's.

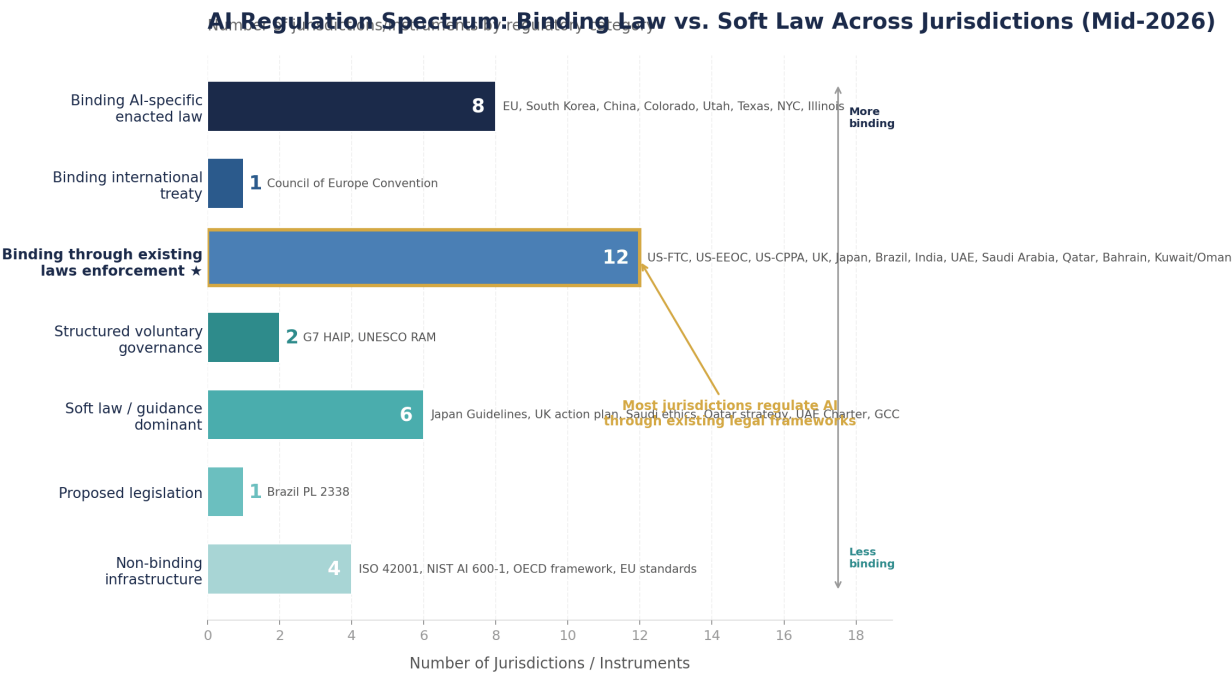
At the transnational level, the HAIP Reporting Framework has expanded from its original developer focus to include deployers and providers across the AI value chain [\[5-8\]](#), reflecting recognition that governance transparency obligations must span the entire supply chain.

Organizations that are both providers and deployers face dual compliance tracks in both the EU and the U.S. The key difference is that the EU provides a more predictable, institutionally defined framework (despite implementation friction [\[6-12\]\[6-15\]](#)), while the U.S. requires navigating multiple uncoordinated enforcement channels.

14.4 The Role of Voluntary Governance Infrastructure in Burden Allocation

Even where there is no binding omnibus AI law, organizations face strong expectations to maintain governance systems, inventories, incident workflows, documentation, and risk-management processes [\[3-1\]\[3-4\]\[3-7\]\[3-9\]](#). ISO/IEC 42001 applies to both providers and users [\[3-1\]](#). The NIST Generative AI Profile recommends lifecycle controls for both model developers and downstream users [\[3-4\]](#). The OECD incident framework captures both developer-side and deployer-side failures [\[3-2\]](#). The HAIP Reporting Framework is open to developers, deployers, and providers [\[5-8\]](#). These instruments can influence procurement requirements, regulator dialogue, assurance programs, and readiness for future binding rules [\[3-1\]\[3-5\]\[3-8\]\[5-7\]](#).

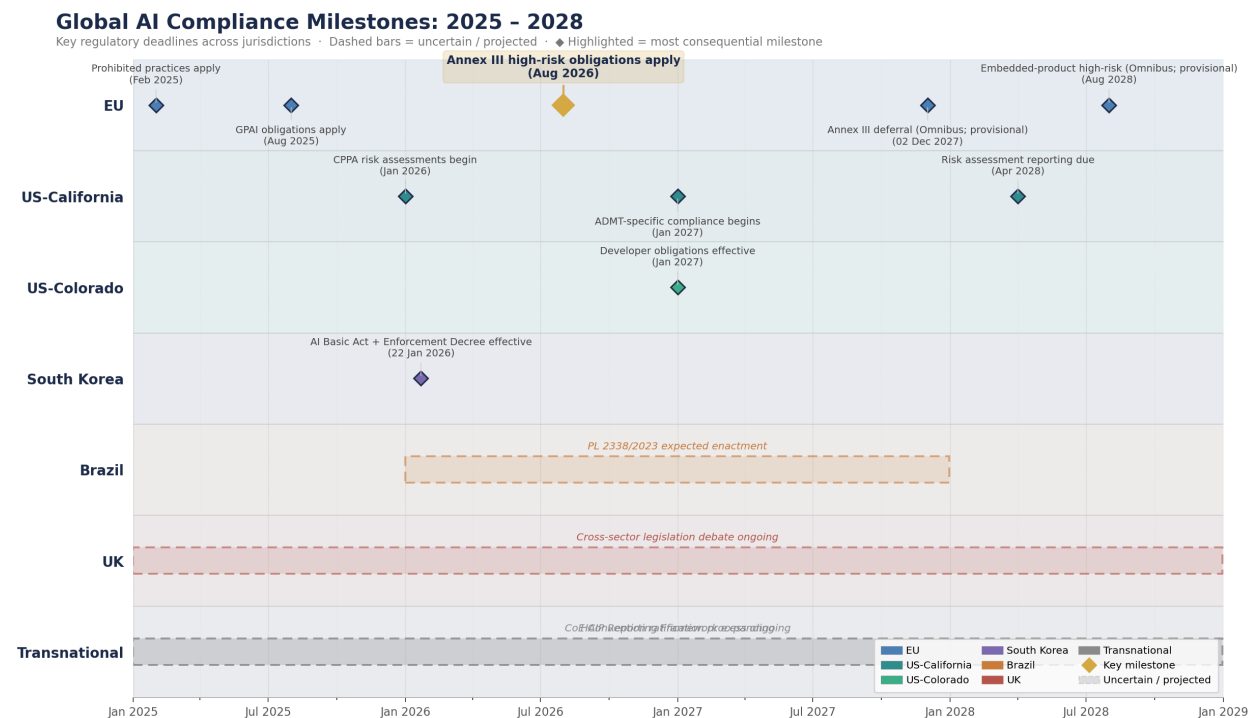
15. Binding-Law versus Guidance Snapshot



Category	Jurisdictions/Instruments
Binding AI-specific enacted law/regulation	EU, South Korea (Act + Enforcement Decree [6-7]), China (layered measures), Colorado (revised SB26-189 [6-1]), Utah, Texas, NYC (local), Illinois hiring law [1-1] [1-2] [1-4] [1-5] [1-6] [1-7] [1-21] [1-23] [1-25] [1-26]
Binding international treaty (framework)	Council of Europe Convention (open for signature; requires domestic implementation) [5-1] [5-2] [5-3]
Binding through enforcement of existing laws	U.S. (FTC, EEOC, CPPA [6-4]), UK, Japan, Brazil (currently), India, many U.S. states, UAE, Saudi Arabia, Qatar, Bahrain, Kuwait, Oman [4-1] [4-2] [1-9] [1-10] [1-11] [1-13] [1-15] [1-42] [1-45] [1-41]
Structured voluntary transnational governance	G7 HAIP Code of Conduct + Reporting Framework [5-4] [5-5] [5-7] [5-8] , UNESCO RAM [5-11] [5-12] [5-13]

Category	Jurisdictions/Instruments
Soft law/guidance/strategy dominant	Japan AI Guidelines, UK action-plan model (with active legislative debate [6-9]), Saudi ethics framework, Qatar strategy, UAE Charter, much of GCC [1-10] [1-8] [3-9] [1-44] [3-8] [1-41]
Proposed comprehensive AI legislation (advanced stage)	Brazil PL 2338/2023 (passed Senate, in Chamber [6-10] [6-11])
Non-binding global governance infrastructure	ISO/IEC 42001, NIST AI 600-1, OECD incident framework, EU harmonised standards (in development), Brazil ANPD Technology Radar [3-1] [3-4] [3-2] [3-5] [3-7]

16. Trajectory and Emerging Developments



- **August 2026** marks the full operationalization of the EU AI Act's Annex III high-risk obligations under the original statutory timeline—the single most consequential

compliance milestone globally [\[1-1\]](#). The provisional "Digital Omnibus" agreement (7 May 2026, pending adoption) would defer stand-alone Annex III high-risk obligations to **2 December 2027** and the transition for high-risk AI systems embedded into regulated products to **2 August 2028** [\[2-6\]](#). The harmonised-standards pathway through CEN-CENELEC JTC 21 [\[3-6\]](#) will add a further compliance dimension as standards are published. The GPAI Code of Practice's two-track presumption structure [\[6-14\]](#) will become increasingly important as providers decide whether to sign or pursue alternative compliance pathways.

- **1 January 2027** is the effective date for Colorado's revised SB26-189 developer obligations [\[6-1\]](#), creating the first U.S. state regime with a mandatory developer-to-deployer documentation transfer for ADMT used in consequential decisions—though without the original law's broader risk-management and impact-assessment architecture [\[6-2\]](#)[\[6-3\]](#).
- **California's CPPA ADMT regulations** require risk-assessment compliance beginning January 1, 2026; ADMT-specific compliance beginning January 1, 2027; and risk-assessment information submission to the CPPA by April 1, 2028 [\[6-4\]](#)[\[6-5\]](#)[\[6-6\]](#).
- **FTC enforcement** against AI-related deceptive claims will continue to create compliance pressure on providers [\[4-3\]](#)[\[4-4\]](#).
- The volume of U.S. state AI bills—1,561 introduced across 45 states by March 2026—indicates continued fragmentation and likely additional enacted laws in the near term [\[1-17\]](#)[\[1-18\]](#). Colorado's experience with SB26-189 [\[6-1\]](#)[\[6-2\]](#)[\[6-3\]](#) demonstrates that even enacted AI laws can be substantially revised before their original effective dates, creating compliance-planning uncertainty for organizations preparing for state-level obligations.
- **South Korea's Enforcement Decree** is already in effect [\[6-7\]](#), with provisions on transparency methods, high-impact AI criteria, and domestic-agent requirements [\[6-8\]](#) creating concrete operational obligations for foreign providers.
- **Brazil's PL 2338/2023** has passed the Senate and is in the Chamber of Deputies [\[6-10\]](#)[\[6-11\]](#), making enactment more likely than at any previous point.
- The **UK Parliament** is actively debating cross-sector AI legislation [\[6-9\]](#), and UK signature and ratification of the Council of Europe Convention [\[5-1\]](#) could catalyze future binding legislation.

- The **Council of Europe Convention** will gain additional signatories and ratifications, creating treaty-level obligations for domestic AI governance measures across its States Parties [\[5-1\]](#)[\[5-2\]](#)[\[5-3\]](#).
- The **HAIP Reporting Framework** will likely expand beyond its initial 25 reports [\[5-8\]](#), with OECD continuing to publish analytical insights [\[5-9\]](#)[\[5-10\]](#).
- **UNESCO RAM** assessments will continue in additional countries [\[5-11\]](#)[\[5-13\]](#)[\[5-14\]](#), influencing how governments in the developing world diagnose AI governance gaps.

17. Key Uncertainties and Alternative Scenarios

17.1 EU Implementation Intensity

Central scenario: The EU's proceduralized enforcement machinery will produce active, technically informed enforcement by 2027–2028, with the harmonised-standards pathway adding presumption-of-conformity mechanisms. The GPAI Code of Practice's two-track structure [\[6-14\]](#) will incentivize most major GPAI providers to sign, creating a de facto compliance standard.

Alternative scenario: Member State capacity constraints, political pressure, the targeted extension for embedded-product AI systems [\[2-6\]](#), missed guidance deadlines [\[6-15\]](#), and industry resistance to the GPAI Code's burden [\[6-12\]](#)[\[6-13\]](#) signal broader delayed or softened enforcement, with the implementation architecture producing more process than substance.

Assessment: The central scenario is more likely because: (a) the AI Office, Scientific Panel, and Advisory Forum are already operational [\[2-1\]](#)[\[2-3\]](#)[\[2-4\]](#); (b) the GPAI Code of Practice and training-data template have been published [\[2-8\]](#)[\[2-9\]](#); (c) over 100 companies have signed the AI Pact [\[2-7\]](#); (d) the omnibus extension is narrowly targeted [\[2-6\]](#); and (e) CEN-CENELEC JTC 21 work is actively underway [\[3-6\]](#). The implementation friction is real but reflects the normal challenges of operationalizing a complex new regulatory system, not a fundamental failure of the enforcement model. The industry contestation [\[6-12\]](#)[\[6-13\]](#) is itself evidence that the regime is being taken seriously by affected organizations. The alternative scenario would require a broader political decision to deprioritize enforcement, which is inconsistent with the institutional investments already made.

17.2 U.S. Federal Preemption

Central scenario: Continued state-level fragmentation with no federal AI law in the near term.

Alternative scenario: Congress enacts a federal AI statute that preempts or harmonizes state laws.

Assessment: The central scenario is more likely because: (a) no federal bill has advanced to enactment; (b) the sheer volume of state activity [\[1-17\]](#) indicates states are not waiting; (c) the FTC, EEOC, and CPPA are actively creating de facto obligations [\[4-1\]](#) [\[4-2\]](#) [\[6-4\]](#); and (d) Colorado's experience with SB26-189 [\[6-1\]](#) [\[6-2\]](#) [\[6-3\]](#) shows that even states with enacted laws are still iterating on their frameworks, suggesting the policy landscape is too fluid for federal consensus. However, a major AI incident or election-cycle pressure could shift the calculus rapidly.

17.3 Colorado's Revised Regime as a Model

Central scenario: Colorado's SB26-189 represents a durable political equilibrium in which the developer-to-deployer documentation transfer and consumer-facing transparency are preserved while the broader risk-management and impact-assessment architecture is abandoned. Other states considering comprehensive AI laws will follow this narrower model rather than the original SB 24-205 approach.

Alternative scenario: Colorado's revision was a temporary political concession, and the state or other states will re-expand deployer obligations toward the original SB 24-205 model once the documentation-transfer mechanism is established and operational.

Assessment: The central scenario is more likely because: (a) the revision was a deliberate legislative choice to remove specific obligations (duty of care, impact assessments, risk-management programs) [\[6-2\]](#) [\[6-3\]](#); (b) Texas's TRAIGA also adopted a narrower approach than earlier drafts [\[1-23\]](#) [\[1-24\]](#); (c) the pattern across multiple states suggests a political preference for disclosure-based rather than prescriptive-management-based AI regulation; and (d) the FTC and CPPA are already filling some of the deployer-side gap through enforcement and rulemaking [\[4-3\]](#) [\[6-4\]](#). The alternative scenario would require a significant shift in political dynamics or a high-profile AI harm that catalyzes demand for stronger deployer obligations.

17.4 Brazil's AI Bill

Central scenario: PL 2338/2023 is enacted by the Chamber of Deputies in late 2026 or 2027, creating a comprehensive risk-based AI statute. The bill's passage through the Senate [\[6-10\]](#)[\[6-11\]](#) and the ANPD's active technical work on generative AI [\[3-7\]](#) indicate sufficient institutional momentum.

Alternative scenario: The bill stalls in the Chamber, and Brazil continues to rely on LGPD and consumer-law enforcement for AI governance.

Assessment: The central scenario is more likely because: (a) the bill has cleared the Senate [\[6-10\]](#)[\[6-11\]](#); (b) the ANPD is building enforcement capacity under existing law [\[3-7\]](#), creating institutional readiness for a new statute; (c) Brazil's civil-law tradition and consumer-protection culture favor comprehensive legislative frameworks; and (d) international developments (the EU AI Act, the Council of Europe Convention, UNESCO RAM assessments in the region [\[5-12\]](#)) create external pressure for legislative action. The alternative scenario would require sustained political opposition or a change in government priorities, which is possible but less likely given the bill's advanced procedural status.

17.5 UK Binding AI Legislation

Central scenario: The UK maintains its regulator-led approach through 2026–2027, with cross-sector AI legislation remaining under parliamentary debate [\[6-9\]](#) but not enacted during this period.

Alternative scenario: The government introduces binding AI legislation sooner than expected, potentially catalyzed by the Council of Europe Convention ratification process [\[5-1\]](#)[\[5-3\]](#) or by competitive pressure from the EU's operational AI Act.

Assessment: The central scenario is more likely because: (a) the AI Opportunities Action Plan emphasizes growth [\[1-8\]](#)[\[1-34\]](#); (b) no specific legislative timeline has been announced; and (c) the UK's political preference for sector-led regulation has been consistent. However, the active parliamentary debate [\[6-9\]](#) indicates the issue is closer to legislative action than at any previous point, and the Convention's ratification requirement for domestic measures [\[5-3\]](#) could accelerate the timeline.

17.6 Convergence Through Governance Infrastructure

Central scenario: The non-binding governance infrastructure layer and the transnational superstructure will become increasingly influential, creating practical convergence that partially offsets legal fragmentation.

Alternative scenario: These layers remain marginal, with compliance driven entirely by jurisdiction-specific requirements.

Assessment: The central scenario is more likely because: (a) ISO/IEC 42001 is published and globally applicable [\[3-1\]](#); (b) NIST AI 600-1 fills the federal U.S. gap [\[3-4\]](#); (c) the OECD incident framework is backed by an Expert Group [\[3-2\]](#)[\[3-3\]](#); (d) EU harmonised standards will create presumption-of-conformity pathways [\[3-5\]](#)[\[3-6\]](#); (e) the HAIP Reporting Framework is producing comparable disclosures across organizations and countries [\[5-8\]](#)[\[5-9\]](#)[\[5-10\]](#); (f) the Council of Europe Convention will require signatory states to adopt domestic measures consistent with its standards [\[5-3\]](#); and (g) recurring themes across all these instruments indicate genuine convergence in expected organizational controls [\[3-1\]](#)[\[3-2\]](#)[\[3-4\]](#)[\[3-5\]](#)[\[3-9\]](#)[\[5-5\]](#)[\[5-6\]](#).

18. Strategic Implications for Espadon

1. **EU compliance is the highest-priority, highest-burden obligation** and is becoming more operationally demanding through implementation tools rather than solely through the statute itself [\[2-1\]](#)[\[2-8\]](#)[\[2-9\]](#)[\[3-5\]](#)[\[3-6\]](#). The GPAI Code of Practice's two-track presumption structure [\[6-14\]](#) makes a sign-or-justify decision necessary for GPAI providers. The implementation friction [\[6-12\]](#)[\[6-15\]](#) creates near-term uncertainty but does not reduce underlying legal obligations.
2. **The distinction between GPAI/model provider and deployer compliance is now institutionally embedded** in the EU, the U.S., and the transnational HAIP framework [\[2-1\]](#)[\[2-2\]](#)[\[4-1\]](#)[\[6-4\]](#)[\[4-12\]](#)[\[5-8\]](#). Organizations that are both providers and deployers face dual compliance tracks.
3. **U.S. compliance burden is substantially higher than enacted AI-specific statutes alone would suggest**, but the specific allocation of burden has shifted. Colorado's revision [\[6-1\]](#)[\[6-2\]](#)[\[6-3\]](#) reduces the deployer-side burden, making California's CPPA ADMT regulations [\[6-4\]](#)[\[6-5\]](#)[\[6-6\]](#) the most operationally significant U.S. deployer-facing AI-adjacent regime. The FTC's AI-washing enforcement [\[4-3\]](#)[\[4-4\]](#) and EEOC's employment AI expectations [\[4-11\]](#)[\[4-12\]](#) remain the primary federal provider- and deployer-side risks, respectively.
4. **Colorado's revised regime still matters for developer-to-deployer documentation infrastructure.** The SB26-189 documentation transfer requirement [\[6-1\]](#) means providers must build and maintain the information packages that

deployers need. This is a narrower but still meaningful compliance obligation that aligns with EU-style provider documentation logic.

5. **China compliance is structurally different** from all other jurisdictions due to the content-control dimension and requires a separate compliance architecture [\[1-4\]](#) [\[1-5\]](#).
6. **South Korea's regime is more concrete than commonly assumed.** The Enforcement Decree's provisions on transparency methods, high-impact AI criteria, and domestic-agent requirements [\[6-7\]](#)[\[6-8\]](#) mean foreign providers must establish in-country compliance infrastructure.
7. **Build a global governance backbone using ISO/IEC 42001 and NIST-aligned lifecycle controls.** The convergence in governance expectations across jurisdictions, the transnational layer (HAIP, Council of Europe Convention), and the governance infrastructure layer (ISO, NIST, OECD) means that a well-designed internal AI management system can serve as a reusable compliance foundation [\[3-1\]](#)[\[3-4\]](#)[\[5-5\]](#)[\[5-8\]](#).
8. **Participate in the HAIP Reporting Framework.** The framework produces governance disclosures that map onto compliance artifacts required under binding regimes [\[5-6\]](#)[\[5-8\]](#)[\[5-9\]](#), provides internal capacity-building benefits [\[5-7\]](#), and generates public evidence of governance maturity.
9. **Invest in vendor-documentation infrastructure.** Both the EU and Colorado's revised regime require providers to furnish deployers with detailed documentation packages [\[1-1\]](#)[\[6-1\]](#), and the EEOC pushes deployers to demand testing evidence from vendors [\[4-12\]](#).
10. **Monitor the EU harmonised-standards pathway.** CEN-CENELEC JTC 21 standards [\[3-6\]](#) will become the most practical route to demonstrating conformity with EU high-risk system requirements [\[3-5\]](#).
11. **Prepare for California's staggered CPPA obligations.** Risk assessments from January 2026; ADMT-specific compliance from January 2027; risk-assessment information submission by April 2028 [\[6-4\]](#)[\[6-5\]](#)[\[6-6\]](#).
12. **Track Brazil's Chamber of Deputies proceedings.** The bill's passage through the Senate [\[6-10\]](#)[\[6-11\]](#) makes enactment more likely, and the ANPD's Technology Radar work [\[3-7\]](#) is creating regulatory expectations under existing law.

13. **Monitor the UK's parliamentary debate on cross-sector AI legislation** [6-9] and the Council of Europe Convention's ratification progress [5-1][5-2].
14. **Soft-law jurisdictions (Japan, GCC) present lower immediate compliance burdens** but should be monitored for movement toward binding regulation through the Council of Europe Convention [5-1] and UNESCO RAM processes [5-12][5-13].

References

- [1-1] EU Artificial Intelligence Act Explorer / Regulation (EU) 2024/1689 materials (2024) <https://artificialintelligenceact.eu/chapter/5>
- [1-2] South Korea's AI Basic Act: Overview and Key Takeaways (2026) <https://www.cooley.com/news/insight/2026/2026-01-27-south-koreas-ai-basic-act-overview-and-key-takeaways>
- [1-3] U.S. State AI Law Tracker – All States (2026) <https://ai-law-center.orrick.com/us-ai-law-tracker-see-all-states>
- [1-4] Interim Measures for the Management of Generative Artificial Intelligence Services (2023) <https://www.chinalawtranslate.com/en/generative-ai-interim>
- [1-5] Provisions on the Administration of Deep Synthesis Internet Information Services (2022) <https://www.chinalawtranslate.com/en/deep-synthesis>
- [1-6] Translation: Internet Information Service Algorithmic Recommendation Management Provisions (2022) <https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022>
- [1-7] Measures for Labeling of AI-Generated Synthetic Content (2025) <https://www.chinalawtranslate.com/en/ai-labeling>
- [1-8] AI Opportunities Action Plan (2025) <https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan>
- [1-9] Guidance on AI and data protection | ICO (N/A) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection>
- [1-10] Outline of "AI Guidelines for Business Ver1.1" (2024) https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240419_15.pdf
- [1-11] AI Library Brazil (N/A) <https://www.mofo.com/artificial-intelligence/brazil>

- [\[1-12\]](#) MeitY advisory (PDF) (2024)
<https://www.meity.gov.in/static/uploads/2024/02/9f6e99572739a3024c9cdaec53a0a0ef.pdf>
- [\[1-13\]](#) The Digital Personal Data Protection Act, 2023 (official PDF) (2023)
<https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>
- [\[1-14\]](#) GCC Navigating AI Regulations - the Current Landscape (2025)
<https://www.twobirds.com/en/insights/2025/united-arab-emirates/gcc-navigating-ai-regulations---the-current-landscape>
- [\[1-15\]](#) DIFC Regulation 10 (2023) <https://www.difc.com/business/registrars-and-commissioners/commissioner-of-data-protection/regulation-10>
- [\[1-16\]](#) Generative Artificial Intelligence Guidelines For Government (2024)
<https://sdaia.gov.sa/en/SDAIA/about/Files/GenAIGuidelinesForGovernmentENCompressed.pdf>
- [\[1-17\]](#) Summary of Artificial Intelligence 2025 Legislation (2025)
<https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation>
- [\[1-18\]](#) Artificial Intelligence (AI) Legislation Tracker 2026: All 50 States (2026)
<https://www.multistate.ai/artificial-intelligence-ai-legislation>
- [\[1-19\]](#) Colorado AI Act (SB 205) text summary (2024)
<https://agora.eto.tech/instrument/1376>
- [\[1-20\]](#) Complying With Colorado's AI Law: Your SB24-205 Compliance Guide (2025) <https://trustarc.com/resource/colorado-ai-law-sb24-205-compliance-guide>
- [\[1-21\]](#) Utah scales back reach of generative AI consumer protection law (2025)
<https://www.davispolk.com/insights/client-update/utah-scales-back-reach-generative-ai-consumer-protection-law>
- [\[1-22\]](#) Utah Becomes First State To Enact AI-Centric Consumer Protection Law (2024) <https://www.skadden.com/insights/publications/2024/04/utah-becomes-first-state>
- [\[1-23\]](#) Texas Enacts New AI Law (2025)
<https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20250721-texas-enacts-new-ai-law>
- [\[1-24\]](#) Texas Responsible AI Governance Act Enacted (2025)
<https://www.wiley.law/alert-Texas-Responsible-AI-Governance-Act-Enacted>
- [\[1-25\]](#) NYC's Law Governing Automated Employment Decision Tools Takes Effect July 5 (2023) <https://www.gtlaw.com/en/insights/2023/6/nycs-law-governing-automated-employment-decision-tools-takes-effect-july-5>

- [\[1-26\]](#) 820 ILCS 42/ - Artificial Intelligence Video Interview Act (2025)
<https://law.justia.com/codes/illinois/chapter-820/act-820-ilcs-42>
- [\[1-27\]](#) US State Privacy Legislation Tracker (2026)
<https://iapp.org/resources/article/us-state-privacy-legislation-tracker>
- [\[1-28\]](#) Connecticut Revamps Its Privacy Law (Again) (2025)
<https://www.shb.com/intelligence/newsletters/pds/hansen-connecticut-privacy-law-2025>
- [\[1-29\]](#) Connecticut Amends the Connecticut Data Privacy Act (2025)
<https://www.hunton.com/privacy-and-cybersecurity-law-blog/connecticut-amends-the-connecticut-data-privacy-act>
- [\[1-30\]](#) Virginia's Consumer Data Privacy Act (2021)
<https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2021/03/virginia-s-consumer-data-privacy-act.html>
- [\[1-31\]](#) Virginia Contemplates Sweeping New Data Protection Law (2021)
<https://www.hinshawlaw.com/en/insights/privacy-cyber-and-ai-decoded-alert/virginia-contemplates-sweeping-new-data-protection-law>
- [\[1-32\]](#) Enacted AI Legislation Chart (2026) <https://fpf.org/wp-content/uploads/2026/02/Enacted-AI-Legislation-Chart-.pdf>
- [\[1-33\]](#) California 2025 legislative wrap-up: More privacy and first-of-its kind AI laws adopted (2025) <https://iapp.org/news/a/california-2025-legislative-wrap-up-more-privacy-and-first-of-its-kind-ai-laws-adopted>
- [\[1-34\]](#) AI Opportunities Action Plan Government Response (2025)
https://assets.publishing.service.gov.uk/media/678639913a9388161c5d2376/ai_opportunities_action_plan_government_repsonse.pdf
- [\[1-35\]](#) Japan AI Safety Institute (J-AISI) (2025)
https://aisi.go.jp/assets/pdf/20250501_AISI_en.pdf
- [\[1-36\]](#) General Understanding on AI and Copyright in Japan (2024)
https://www.bunka.go.jp/english/policy/copyright/pdf/94055801_01.pdf
- [\[1-37\]](#) South Korea Artificial Intelligence (AI) Basic Act (2025)
<https://www.trade.gov/market-intelligence/south-korea-artificial-intelligence-ai-basic-act>
- [\[1-38\]](#) Recent Developments in AI Basic Act (2025)
https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=33805
- [\[1-39\]](#) Artificial intelligence reignites debates in the Brazilian House of Representatives (2025) <https://www.demarest.com.br/en/inteligencia-artificial-reacende-debates-na-camara-dos-deputados>
- [\[1-40\]](#) Press Release Page | Press Information Bureau (2025)
<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268>

- [\[1-41\]](#) FALQs: AI Regulations in the Gulf Cooperation Council Member States – Part Two (2024) <https://blogs.loc.gov/law/2024/12/falqs-ai-regulations-in-the-gulf-cooperation-council-member-states-part-two>
- [\[1-42\]](#) SDAIA Supports Saudi Arabia's Leadership in Shaping ... (N/A) <https://my.gov.sa/en/news/640446>
- [\[1-44\]](#) National Artificial Intelligence Strategy for Qatar (2021) https://policy.mada.org.qa/wp-content/uploads/2022/06/national_ai_strategy_-_english_0.pdf
- [\[1-45\]](#) Qatar | Jurisdictions (N/A) <https://www.dataguidance.com/jurisdictions/qatar>
- [\[1-46\]](#) Japan's first AI legislation becomes law — AI Promotion Act, White & Case (2025) <https://www.whitecase.com/insight-alert/japans-first-ai-legislation-becomes-law-focus-promoting-research-and-development-no>
- [\[1-47\]](#) New York RAISE Act — Governor Hochul signs frontier-model AI legislation, Dec. 19, 2025 (2025) <https://www.governor.ny.gov/news/governor-hochul-signs-nation-leading-legislation-require-ai-frameworks-ai-frontier-models>
- [\[1-48\]](#) California enacts SB 53 / Transparency in Frontier Artificial Intelligence Act, White & Case (2025) <https://www.whitecase.com/insight-alert/california-enacts-landmark-ai-transparency-law-transparency-frontier-artificial>
- [\[1-49\]](#) The TAKE IT DOWN Act (Public Law 119-12), Congressional Research Service LSB11314 (2025) <https://www.congress.gov/crs-product/LSB11314>
- [\[2-1\]](#) European AI Office | Shaping Europe's digital future (2026) <https://digital-strategy.ec.europa.eu/en/policies/ai-office>
- [\[2-2\]](#) Market Surveillance Authorities under the AI Act (2026) <https://digital-strategy.ec.europa.eu/en/policies/market-surveillance-authorities-under-ai-act>
- [\[2-3\]](#) AI Act Advisory Forum | Shaping Europe's digital future (2026) <https://digital-strategy.ec.europa.eu/en/policies/ai-advisory-forum>
- [\[2-4\]](#) AI Act Scientific Panel | Shaping Europe's digital future (2026) <https://digital-strategy.ec.europa.eu/en/policies/ai-scientific-panel>
- [\[2-5\]](#) AI Pact | Shaping Europe's digital future (2026) <https://digital-strategy.ec.europa.eu/en/policies/ai-pact>
- [\[2-6\]](#) AI Act | Shaping Europe's digital future (2026) <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
- [\[2-7\]](#) Over a hundred companies sign EU AI Pact pledges to drive trustworthy and safe AI development (2024) https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4864
- [\[2-8\]](#) The General-Purpose AI Code of Practice (2026) <https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai>

- [2-9] Commission presents template for General-Purpose AI model providers to summarise the data used to train their model (2025) <https://digital-strategy.ec.europa.eu/en/news/commission-presents-template-general-purpose-ai-model-providers-summarise-data-used-train-their>
- [3-1] ISO/IEC 42001:2023 - AI management systems (2023) <https://www.iso.org/standard/42001>
- [3-2] Towards a common reporting framework for AI incidents (2025) https://www.oecd.org/en/publications/towards-a-common-reporting-framework-for-ai-incidents_f326d4ac-en.html
- [3-3] AI incidents Overview - OECD.AI (2025) <https://oecd.ai/en/site/incidents>
- [3-4] Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (2024) <https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence>
- [3-5] Standardisation of the AI Act | Shaping Europe's digital future (2026) <https://digital-strategy.ec.europa.eu/en/policies/ai-act-standardisation>
- [3-6] European AI Standardization | CEN-CENELEC JTC 21 (2026) <https://jtc21.eu>
- [3-7] ANPD releases English version of Technology Radar (2024) <https://legismap.com.br/conteudos/artigos-e-noticias/anpd-releases-english-version-of-technology-radar>
- [3-8] The UAE Charter for the Development and Use of Artificial Intelligence (2024) <https://uaelegislation.gov.ae/en/policy/details/the-uae-charter-for-the-development-and-use-of-artificial-intelligence>
- [3-9] AI Ethics Principles (2023) <https://sdaia.gov.sa/en/SDAIA/about/Documents/ai-principles.pdf>
- [3-10] Saudi Arabia: SDAIA publishes AI Ethics Principles version 2.0 (2023) <https://www.dataguidance.com/news/saudi-arabia-sdaia-publishes-ai-ethics-principles>
- [3-11] Saudi Arabia - AI Ethics Principles (2023) <https://regulations.ai/regulations/RAI-SA-NA-PCAESXX-2023>
- [4-1] Artificial Intelligence | Federal Trade Commission (N/A) <https://www.ftc.gov/industry/technology/artificial-intelligence>
- [4-2] EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairness (2021) <https://www.eeoc.gov/newsroom/eeoc-launches-initiative-artificial-intelligence-and-algorithmic-fairness>
- [4-3] FTC Announces Crackdown on Deceptive AI Claims and Schemes (2024) <https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes>
- [4-4] FTC Finalizes Order with DoNotPay That Prohibits Deceptive 'AI Lawyer' Claims, Imposes Monetary Relief, and Requires Notice to Past Subscribers (2025)

<https://www.ftc.gov/news-events/news/press-releases/2025/02/ftc-finalizes-order-donotpay-prohibits-deceptive-ai-lawyer-claims-imposes-monetary-relief-requires>

- [\[4-5\]](#) DoNotPay | Federal Trade Commission (N/A) <https://www.ftc.gov/legal-library/browse/cases-proceedings/donotpay>
- [\[4-6\]](#) California Finalizes Regulations to Strengthen Consumers' Privacy (2025) <https://coppa.ca.gov/announcements/2025/20250923.html>
- [\[4-7\]](#) California Finalizes CCPA Regulations for Automated Decision-Making Technology, Risk Assessments and Cybersecurity Audits (2025) <https://www.skadden.com/insights/publications/2025/10/california-finalizes-coppa-regulations>
- [\[4-8\]](#) California Finalizes CCPA Regulations on Automated Decision-Making Technology, Risk Assessments, and Cybersecurity Audits (2025) <https://www.coblentzlaw.com/news/california-finalizes-ccpa-regulations-on-automated-decision-making-technology-risk-assessments-and-cybersecurity-audits>
- [\[4-9\]](#) Senate Bill 24-205 - Colorado General Assembly (2024) https://leg.colorado.gov/bill_files/47770/download
- [\[4-10\]](#) SB24-205 Consumer Protections for Artificial Intelligence | Colorado General Assembly (2024) <https://leg.colorado.gov/bills/sb24-205>
- [\[4-11\]](#) What is the EEOC's role in AI? (2024) https://www.eeoc.gov/sites/default/files/2024-04/20240429_What%20is%20the%20EEOCs%20role%20in%20AI.pdf
- [\[4-12\]](#) Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964 (2023) https://data.aclum.org/storage/2025/01/EOCC_www_eeoc_gov_laws_guidance_select-issues-assessing-adverse-impact-software-algorithms-and-artificial.pdf
- [\[5-1\]](#) The Framework Convention on Artificial Intelligence (2026) <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>
- [\[5-2\]](#) Chart of signatures and ratifications of Treaty 225 (2026) <https://www.coe.int/en/web/Conventions/full-list?module=signatures-by-treaty&treaty=225>
- [\[5-3\]](#) Council of Europe Convention on Artificial Intelligence - eucrim (2024) <https://eucrim.eu/news/council-of-europe-convention-on-artificial-intelligence>
- [\[5-4\]](#) Hiroshima AI Process (2026) <https://www.soumu.go.jp/hiroshimaaiprocess/en/index.html>

- [\[5-5\]](#) Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems (2023) <https://g7g20-documents.org/database/document/2023-g7-japan-leaders-leaders-annex-hiroshima-process-international-code-of-conduct-for-organizations-developing-advanced-ai-systems>
- [\[5-6\]](#) How are AI developers managing risks? (OECD PDF) (2025) https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/09/how-are-ai-developers-managing-risks_fbaeb3ad/658c2ad6-en.pdf
- [\[5-7\]](#) Reporting Framework | Hiroshima AI Process (2025) <https://www.soumu.go.jp/hiroshimaaiprocess/en/report.html>
- [\[5-8\]](#) HAIP Reporting Framework - OECD.AI (2025) <https://oecd.ai/en/transparency/overview>
- [\[5-9\]](#) How are AI developers managing risks? Insights from responses to the reporting framework of the Hiroshima AI Process Code of Conduct (2025) <https://oecd.ai/en/ai-publications/how-are-ai-developers-managing-risks-insights-from-responses-to-the-reporting-framework-of-the-hiroshima-ai-process-code-of-conduct>
- [\[5-10\]](#) Ethics of Artificial Intelligence - UNESCO (2026) <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>
- [\[5-11\]](#) Artificial Intelligence Assessments (UNDP-UNESCO) (2024) <https://www.undp.org/sites/g/files/zskgke326/files/2024-12/undp-unesco-offer-web-7-aug-2024.pdf>
- [\[5-12\]](#) UNESCO AI Readiness Assessment Report: Anchoring Ethics in AI Governance in the Philippines (2024) <https://philippines.un.org/en/306159-unesco-ai-readiness-assessment-report-anchoring-ethics-ai-governance-philippines>
- [\[5-13\]](#) UNESCO AI Readiness Assessment Methodology (RAM) - Consultation Sessions (2025) <http://mpaai.gov.tt/news/unesco-ai-readiness-assessment-methodology-ram-consultation-sessions>
- [\[5-14\]](#) Lao PDR to unveil UNESCO AI Ethics Readiness Assessment report at national workshop (2026) <https://www.unesco.org/en/articles/lao-pdr-unveil-unesco-ai-ethics-readiness-assessment-report-national-workshop>
- [\[6-1\]](#) SB26-189 Automated Decision-Making Technology (2026) <https://leg.colorado.gov/bills/sb26-189>
- [\[6-2\]](#) Colorado AI Act Amended and Effective Date Delayed (2026) <https://www.hunton.com/privacy-and-cybersecurity-law-blog/colorado-ai-act-amended-and-effective-date-delayed>
- [\[6-3\]](#) Colorado Governor Signs SB 189, Significantly Amending the State's AI Law (2026) <https://www.hklaw.com/en/insights/publications/2026/05/colorado->

governor-signs-sb-189

- [\[6-4\]](#) California Finalizes Regulations to Strengthen Consumers' Privacy (2025) <https://cppa.ca.gov/announcements/2025/20250923.html>
- [\[6-5\]](#) Newly Approved CCPA Regulations Have Staggered Deadlines for Compliance (2025) <https://www.hunton.com/privacy-and-cybersecurity-law-blog/newly-approved-ccpa-regulations-have-staggered-deadlines-for-compliance>
- [\[6-6\]](#) California Finalizes CCPA Regulations on Automated Decision-Making Technology, Risk Assessments, and Cybersecurity Audits (2025) <https://www.coblentzlaw.com/news/california-finalizes-ccpa-regulations-on-automated-decision-making-technology-risk-assessments-and-cybersecurity-audits>
- [\[6-7\]](#) South Korea AI Basic Act (2026) <https://www.trade.gov/market-intelligence/south-korea-ai-basic-act>
- [\[6-8\]](#) The MSIT Releases Draft Enforcement Decree of the AI Basic Act (2025) https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=32909
- [\[6-9\]](#) AI regulation in the UK: Debate on the need for cross-sector legislation (2026) <https://lordslibrary.parliament.uk/ai-regulation-in-the-uk-debate-on-the-need-for-cross-sector-legislation>
- [\[6-10\]](#) Artificial intelligence reignites debates in the Brazilian House of Representatives (2025) <https://www.demarest.com.br/en/inteligencia-artificial-reacende-debates-na-camara-dos-deputados>
- [\[6-11\]](#) PL 2338/2023: the impacts of regulating Artificial Intelligence in Brazil (2026) <https://www.sidi.org.br/en/blog/the-impacts-of-regulating-artificial-intelligence-in-brazil>
- [\[6-12\]](#) AI Act: EU's Final GPAI Code Imposes Disproportionate Burden, Improvements Required (2025) <https://ccianet.org/news/2025/07/ai-act-eus-final-gpai-code-imposes-disproportionate-burden-improvements-required>
- [\[6-13\]](#) ITI Reacts to Publication of AI Act GPAI Code of Practice (2025) <https://www.itic.org/news-events/news-releases/iti-reacts-to-publication-of-ai-act-gpai-code-of-practice>
- [\[6-14\]](#) EU AI Act Update: What the New Code of Practice Means for Business (2025) <https://ai-analytics.wharton.upenn.edu/wharton-accountable-ai-lab/eu-ai-act-update-what-the-new-code-of-practice-means-for-business>
- [\[6-15\]](#) European Commission misses deadline for AI Act guidance on high-risk systems (2025) <https://iapp.org/news/a/european-commission-misses-deadline-for-ai-act-guidance-on-high-risk-systems>
- [\[6-16\]](#) European Commission hints at delaying the AI Act (2025) <https://www.insideglobaltech.com/2025/06/12/european-commission-hints-at>

delaying-the-ai-act

- [\[6-17\]](#) AI Regulatory Horizon Tracker - United Arab Emirates (2026)
<https://www.twobirds.com/en/capabilities/artificial-intelligence/ai-legal-services/ai-regulatory-horizon-tracker/uae>
- [\[6-18\]](#) UAE's International Stance on Artificial Intelligence Policy (N/A)
<https://uaelegislation.gov.ae/en/policy/details/uae-s-international-stance-on-artificial-intelligence-policy>

Appendix

Research 1:

Findings on the current global AI regulation patchwork (as of June 2026)

1. Cross-jurisdiction picture
2. The EU and South Korea have enacted comprehensive AI-specific cross-sector laws. The EU AI Act entered into force on 1 August 2024 and applies in phases; South Korea's AI Basic Act took effect on 22 January 2026.[\[1\]\[2\]](#)
3. The United States does not have a single federal AI law. State regulation is a mix of enacted AI-specific laws, privacy laws with profiling/automated-decision rules, biometric laws, deepfake laws, employment rules, executive policies, and many pending bills. Orrick's 50-state tracker shows state-by-state AI-related measures, including privacy-law automated decision-making rights in multiple states.[\[3\]](#)
4. China has a layered AI regime based on binding rules for algorithmic recommendation, deep synthesis, generative AI services, and AI-generated content labeling, overlaid by the Cybersecurity Law, Data Security Law, and Personal Information Protection Law.[\[4\]\[5\]\[6\]\[7\]](#)
5. The UK continues to use a regulator-led, sectoral approach rather than a single AI law; the government's 2025 AI Opportunities Action Plan response states that regulation, safety, and assurance are part of the UK's AI growth agenda.[\[8\]\[9\]](#)
6. Japan enacted the AI Promotion Act (Act on the Promotion of Research and Development and Utilization of AI-Related Technologies) on 28 May 2025, in full effect from September 2025, but it is a non-binding framework law with no AI-specific penalties, so Japan's framework remains primarily soft law in effect ([White & Case, 2025](#)). METI/MIC's AI Guidelines for Business were issued in April 2024 and updated to Version 1.1 on 28 March 2025.[\[10\]](#)

7. Brazil's main cross-sector AI bill remains proposed rather than enacted; PL 2338/2023 is still under congressional consideration.[\[11\]](#)
8. India's current regime remains a mix of advisories, IT intermediary/platform rules, cyber measures, and the Digital Personal Data Protection Act 2023 rather than a dedicated AI law.[\[12\]](#)[\[13\]](#)
9. In the GCC, no single harmonized AI law exists across the six states; the landscape is composed of national strategies, data protection/cyber laws, government guidance, and selective sectoral or free-zone rules. UAE and Saudi Arabia are the most institutionally developed within the region.[\[14\]](#)[\[15\]](#)[\[16\]](#)
10. European Union Legal status and scope
11. Regulation (EU) 2024/1689 is a binding cross-sector regulation. The Act covers providers, deployers, importers, distributors, product manufacturers, and providers of general-purpose AI models, including some non-EU actors where outputs are used in the EU market.[\[1\]](#)
12. The Act classifies AI by risk and contains rules for prohibited AI practices, high-risk AI systems, transparency obligations for certain AI systems, and general-purpose AI (GPAI) models.[\[1\]](#)

Risk model - The EU regime uses a risk-based structure: prohibited practices (Article 5), high-risk systems (Articles 6 and Annex III), transparency obligations for specified AI systems (Article 50), and GPAI/GPAI with systemic risk (Articles 51, 53, 55).[\[1\]](#)

Developer/provider obligations - Providers of high-risk AI systems have obligations covering risk management, data governance, technical documentation, logging, transparency and instructions for use, human oversight design, accuracy/robustness/cybersecurity, quality management systems, conformity assessment, registration where applicable, post-market monitoring, and serious incident reporting.[\[1\]](#) - Providers of GPAI models must prepare technical documentation, provide information and documentation to downstream providers, comply with EU copyright law obligations, and publish a sufficiently detailed summary about the content used for training.[\[1\]](#) - Providers of GPAI models with systemic risk face additional obligations including model evaluation, systemic-risk assessment and mitigation, adversarial testing where appropriate, incident reporting, and cybersecurity protections.[\[1\]](#)

Deployer obligations - Deployers of high-risk AI systems must use systems in accordance with provider instructions, ensure relevant human oversight, monitor

operation, keep logs when under their control, and notify serious incidents. Certain public-sector or listed use cases require fundamental-rights impact assessments.^[1]

Timeline - The AI Act entered into force on 1 August 2024.^[1] - Prohibited AI practices and AI literacy obligations started applying on 2 February 2025.^[1] - Governance rules and GPAI obligations started applying on 2 August 2025.^[1] - Most stand-alone Annex III high-risk obligations apply from 2 August 2026, and embedded-product (Annex I) high-risk obligations from 2 August 2027, under the original statutory timeline.^[1] The provisional "Digital Omnibus" agreement (7 May 2026, pending Official Journal adoption) would defer these to 2 December 2027 and 2 August 2028 respectively.^[6]

Penalties - The Act provides fines up to EUR 35 million or 7% of worldwide annual turnover for certain prohibited-practice breaches; up to EUR 15 million or 3% for certain other violations; and up to EUR 7.5 million or 1.5% for supplying incorrect information, with lower caps possible for SMEs/startups in some cases.^[1]

1. United States: 50-state patchwork National structure
2. NCSL's 2025 legislation summary and Multistate's tracker show the scale of the state patchwork: 1,561 AI-related bills had been introduced in 45 states by March 2026, and 99 AI-related bills were enacted in 2024.^{[17][18]}
3. The U.S. state landscape is not a single regime. It includes: (a) AI-specific transparency laws, (b) high-risk/consequential decision laws, (c) employment-specific AI rules, (d) biometric/privacy/deepfake laws, and (e) comprehensive privacy laws with profiling opt-outs and impact assessments.^{[3][17][18]}

High-impact enacted state regimes - Colorado SB 24-205 created the first enacted broad state high-risk AI law. It regulates developers and deployers of high-risk AI systems used in consequential decisions and was signed on 17 May 2024, with obligations originally scheduled to apply from 1 February 2026 and later delayed to 30 June 2026, before SB26-189 repealed and reenacted the regime (developer obligations now begin 1 January 2027).^{[19][20]} - Colorado's law requires developers to use reasonable care to protect consumers from algorithmic discrimination, make specified documentation available, disclose known or reasonably foreseeable risks, and notify the attorney general under certain circumstances. Deployers must use reasonable care, implement risk management policies, conduct impact assessments, review for algorithmic discrimination, provide consumer notices where consequential decisions are made, and offer disclosures on request.^{[19][20]} - Utah's Artificial Intelligence Policy Act was enacted on 13 March 2024 and took effect 1 May 2024. It imposes disclosure obligations when consumers interact with generative AI in covered contexts and establishes the Office of Artificial Intelligence Policy and an AI Learning Laboratory

Program.[\[21\]\[22\]](#) - Texas enacted the Texas Responsible Artificial Intelligence Governance Act on 22 June 2025. Public analyses describe it as imposing prohibited-practice rules and public-sector notice duties, while removing many of the broader private-sector developer/deployer obligations from earlier drafts; it takes effect on 1 January 2026 and applies to developers and deployers through its prohibited-use and disclosure provisions.[\[23\]\[24\]](#)

Local and sectoral examples - New York City Local Law 144 requires annual independent bias audits for automated employment decision tools used in hiring or promotion, public posting of audit summaries, and at least 10 business days' advance notice to applicants/employees, including information about the tool and alternative assessment requests.[\[25\]](#) - Illinois' Artificial Intelligence Video Interview Act requires employers using AI to analyze recorded applicant videos to notify applicants, explain how the AI works and what characteristics it evaluates, obtain consent, limit sharing, and comply with destruction/deletion-related rules.[\[26\]](#) - Illinois BIPA remains a major biometric enforcement law relevant to AI systems using faceprints/voiceprints or other biometric identifiers.[\[26\]](#)

Privacy-law automated decision/profiling provisions - Many states use comprehensive privacy laws to regulate automated decision-making indirectly through profiling rights, opt-outs, and data-protection assessments. Orrick's all-state tracker shows this across states, and IAPP tracks comprehensive state privacy laws separately.[\[3\]\[27\]](#) - Connecticut's privacy law requires opt-outs for profiling in decisions producing legal or similarly significant effects, and 2025 amendments added explicit impact assessment requirements for such profiling and additional AI/LLM training disclosures effective 2026.[\[28\]\[29\]](#) - Virginia's Consumer Data Protection Act gives consumers the right to opt out of profiling in furtherance of decisions that produce legal or similarly significant effects and requires data processing assessments for specified risky processing.[\[30\]](#) [\[31\]](#) - Alabama's enacted privacy law includes an opt-out right for solely automated significant decisions, effective 1 May 2027, according to Orrick's state tracker.[\[3\]](#)

All 50 U.S. states: structured tracker snapshot - Alabama: enacted privacy law with automated-decision opt-out right effective 2027.[\[3\]](#) - Alaska: no major enacted cross-sector AI law identified in the search set; patchwork consists mainly of general laws and pending activity.[\[3\]\[17\]](#) - Arizona: no major enacted cross-sector AI law identified in the search set; pending/activity tracked in state trackers.[\[3\]\[17\]](#) - Arkansas: enacted AI-related transparency legislation appears in FPF's enacted chart for 2025 generative AI transparency.[\[32\]](#) - California: high legislative activity; enacted 2024-2025 AI laws include generative AI transparency, training-data disclosures, election/deepfake measures, and health and chatbot provisions—plus the Transparency in Frontier

Artificial Intelligence Act (SB 53), signed 29 September 2025, which regulates frontier-model developers; multiple additional proposals remain pending or changed over time. [\[32\]\[33\]](#) - Colorado: enacted comprehensive high-risk AI law (SB 24-205). [\[19\]\[20\]](#) - Connecticut: privacy/profiling regime with impact-assessment amendments. [\[28\]\[29\]](#) - Delaware: AI innovation/task-force style activity appears in trackers. [\[17\]\[32\]](#) - Florida: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set. [\[3\]\[17\]](#) - Georgia: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set. [\[3\]\[17\]](#) - Hawaii: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set. [\[3\]\[17\]](#) - Idaho: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set. [\[3\]\[17\]](#) - Illinois: AI Video Interview Act; BIPA; employment/health updates appear in trackers. [\[26\]\[32\]](#) - Indiana: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set. [\[3\]\[17\]](#) - Iowa: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set. [\[3\]\[17\]](#) - Kansas: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set. [\[3\]\[17\]](#) - Kentucky: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set. [\[3\]\[17\]](#) - Louisiana: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set. [\[3\]\[17\]](#) - Maine: enacted 2025 chatbot law appears in FPF chart. [\[32\]](#) - Maryland: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set. [\[3\]\[17\]](#) - Massachusetts: active proposals referenced in analysis pieces; no enacted comprehensive AI law identified in retrieved set. [\[17\]\[27\]](#) - Michigan: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set. [\[3\]\[17\]](#) - Minnesota: privacy/AI related activity appears in trackers. [\[32\]](#) - Mississippi: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set. [\[3\]\[17\]](#) - Missouri: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set. [\[3\]\[17\]](#) - Montana: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set. [\[17\]\[18\]](#) - Nebraska: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set. [\[3\]\[17\]](#) - Nevada: health-related AI law appears in FPF enacted chart for 2025. [\[32\]](#) - New Hampshire: enacted 2025 chatbot law appears in FPF chart. [\[32\]](#) - New Jersey: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set. [\[3\]\[17\]](#) - New Mexico: proposal activity referenced in analysis pieces; no enacted comprehensive AI law identified in retrieved set. [\[17\]\[27\]](#) - New York: local employment AEDT rule in NYC (Local Law 144); the state RAISE Act was subsequently enacted on 19 December 2025 (Chapter 699), effective 1 January 2027, regulating frontier-model developers ([Governor of New York, 2025](#)). [\[25\]\[18\]](#) - North Carolina: state AI activity tracked; no comprehensive enacted cross-sector

AI law identified in the retrieved set.[\[3\]\[17\]](#) - North Dakota: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set.[\[3\]\[17\]](#) - Ohio: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set.[\[3\]\[17\]](#) - Oklahoma: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set.[\[3\]\[17\]](#) - Oregon: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set.[\[3\]\[17\]](#) - Pennsylvania: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set.[\[3\]\[17\]](#) - Rhode Island: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set.[\[3\]\[17\]](#) - South Carolina: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set.[\[3\]\[17\]](#) - South Dakota: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set.[\[3\]\[17\]](#) - Tennessee: enacted 2024 IP/digital replica law appears in FPF chart.[\[32\]](#) - Texas: enacted TRAIGA 2025.[\[23\]\[24\]](#) - Utah: enacted AI disclosure law 2024; updated in 2025.[\[21\]\[32\]](#) - Vermont: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set.[\[3\]\[17\]](#) - Virginia: privacy/profiling regime; 2024 AI-specific bills failed according to NCSL summary.[\[17\]\[30\]\[31\]](#) - Washington: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set.[\[3\]\[17\]](#) - West Virginia: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set.[\[3\]\[17\]](#) - Wisconsin: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set.[\[3\]\[17\]](#) - Wyoming: state AI activity tracked; no comprehensive enacted cross-sector AI law identified in the retrieved set.[\[3\]\[17\]](#)

1. China Legal status and scope
2. China has binding AI-specific administrative measures for public-facing generative AI services, deep synthesis internet information services, algorithmic recommendation services, and AI-generated/synthetic content labeling.[\[4\]\[5\]\[6\]\[7\]](#)
3. The Interim Measures for the Management of Generative Artificial Intelligence Services apply to using generative AI to provide services to the public in mainland China for generating text, images, audio, video, or other content.[\[4\]](#)

Risk and regulatory model - China's structure is not an EU-style single risk-tier law. It is activity- and content-based, with strong emphasis on public-facing services, content control, security assessment, algorithm filing, data/personal-information compliance, and state oversight.[\[4\]\[5\]\[6\]](#)

Developer/provider obligations - Generative AI service providers must uphold content-law requirements, adopt measures for data and model security, protect personal

information, label or handle illegal content, and for some services complete security assessments and algorithm filing procedures.[\[4\]](#) - Deep synthesis rules prohibit producing or disseminating prohibited information, require identity/authenticity-related measures, and impose labeling obligations in specified contexts.[\[5\]](#) - Algorithm recommendation rules require algorithmic recommendation service providers to establish management systems, protect users, provide options to turn off recommendation services in some contexts, and undergo filing/security oversight where required.[\[6\]](#) - On 14 March 2025, CAC and three other agencies released final Measures for Labeling Artificial Intelligence-Generated and Synthetic Content and GB 45438-2025, imposing explicit and implicit labeling duties and traceability-related duties for providers.[\[7\]](#)

Enforcement and penalties - The algorithm recommendation provisions state that certain violations may trigger warnings, criticism notices, orders to rectify, suspension of information updates, and fines of RMB 10,000 to RMB 100,000 where no other law provides otherwise; other violations are handled under other applicable laws and regulations.[\[6\]](#) - China's AI rules are enforced by CAC and other agencies, with the Cybersecurity Law, Data Security Law, and PIPL available as overlays.[\[4\]\[5\]\[6\]](#)

1. United Kingdom Legal status and structure
2. The UK has not enacted a single comprehensive AI law equivalent to the EU AI Act. The current model relies on existing regulators and laws, with AI-specific guidance and public-policy programs.[\[8\]\[9\]](#)
3. The ICO's "Guidance on AI and data protection" remains a core regulatory document for privacy-law compliance in AI systems under UK GDPR/data protection law.[\[9\]](#)

Institutional and policy direction - The UK government published the AI Opportunities Action Plan on GOV.UK and issued a formal government response in January 2025.[\[8\]\[34\]](#) - The Action Plan states the UK should invest in compute, data infrastructure, talent, and regulation, and that regulation, safety, and assurance can support AI adoption and growth.[\[8\]\[34\]](#)

Obligations by source of law - For model developers/providers and deployers, binding duties arise mainly through existing laws: UK GDPR/data protection, consumer protection, equality law, product-safety rules, online safety/content rules, procurement, and sectoral supervision.[\[9\]](#) - The ICO guidance addresses lawfulness, fairness, transparency, governance, accuracy, security, and individual rights for AI processing personal data.[\[9\]](#)

1. Japan Legal status

2. Japan now has AI-specific legislation—the AI Promotion Act (passed 28 May 2025, in full effect September 2025)—but it is a non-binding framework law with no penalties, so Japan's cross-sector framework remains soft law in effect rather than a prescriptive binding regime ([White & Case, 2025](#)). METI and MIC published the AI Guidelines for Business Version 1.0 in April 2024 and Version 1.1 on 28 March 2025.[\[10\]](#)

Scope and actor categories - The guidelines distinguish AI business actors, including developers, providers, and business users, and organize expected actions by role.[\[10\]](#)

Obligations and themes - The guidelines address governance, safety, transparency, security, privacy, human rights/fairness, and role-based responsibilities rather than statutory fines.[\[10\]](#) - Japan AI Safety Institute materials note the updated guideline version and describe the governance framework as part of Japan's safety infrastructure.[\[35\]](#)

Copyright/training-data overlay - Japan's Agency for Cultural Affairs published "General Understanding on AI and Copyright in Japan," clarifying copyright issues around AI training and outputs.[\[36\]](#)

1. South Korea Legal status and timeline
2. South Korea adopted the Framework Act on Artificial Intelligence Development and Establishment of a Foundation for Trustworthiness in January 2025, with effect from 22 January 2026.[\[2\]](#)[\[37\]](#)

Scope and reach - The Act applies to AI development business operators and AI utilization business operators and has extraterritorial application for certain businesses offering products or services in Korea.[\[2\]](#)

Risk model - The Act distinguishes "generative AI" and "high-impact AI." High-impact AI is defined as AI significantly affecting human life, physical safety, or fundamental rights.[\[2\]](#)

Developer/provider obligations - Businesses providing generative AI or high-impact AI have transparency duties. Articles discussed in legal summaries describe requirements to notify users when operations use generative or high-impact AI and to label outputs produced by generative AI, including deepfakes.[\[2\]](#)[\[38\]](#) - High-impact AI operators face obligations concerning safety and reliability.[\[38\]](#)

Penalties - Public analyses describe lower financial penalties than the EU model; the U.S. Department of Commerce trade note identifies the Act as a comprehensive framework creating new compliance requirements.[\[2\]](#)[\[37\]](#)

1. Brazil Legal status
2. Brazil's principal AI framework is still proposed rather than enacted. PL 2338/2023 remains under legislative processing in Congress.[\[11\]](#)

Core bill structure in current summaries - Available summaries describe a risk-based bill establishing general standards for development, implementation, and responsible use of AI systems, with governance duties and impact assessments for high-risk systems.[\[11\]](#)
[\[39\]](#)

Current binding overlays - Until any AI bill is enacted, Brazil's binding controls relevant to AI come primarily from LGPD data protection law and sectoral/consumer frameworks.
[\[11\]](#)

1. India Legal status and scope
2. India does not yet have a dedicated enacted cross-sector AI statute in the retrieved materials. The current framework is based on the Digital Personal Data Protection Act, the IT Act, the Intermediary Guidelines and Digital Media Ethics Code Rules 2021 (as amended), cyber advisories, and MeitY advisories.[\[12\]](#)[\[13\]](#)

MeitY advisory and platform obligations - MeitY's 2024 advisory instructed intermediaries and platforms to ensure that AI/LLM/generative AI software or algorithms do not permit users to host, display, upload, modify, publish, transmit, store, update, or share unlawful content under the IT Rules framework.[\[12\]](#)

Data protection overlay - The DPDP Act 2023 applies extraterritorially where processing outside India is connected with offering goods or services to individuals in India.[\[13\]](#)

Deepfakes and online harms - A 2025 government statement to Parliament identifies the IT Act 2000 and the IT Rules 2021 as the core legal framework used to address deepfakes and related cyber harms, including sections on identity theft, impersonation, privacy violations, obscene/sexually explicit content, blocking orders, and intermediary notice/removal powers.[\[40\]](#)

1. Gulf region (GCC) Regional overview
2. The GCC remains a patchwork of AI strategies, data protection laws, cybersecurity rules, sector guidance, and selective AI-specific governance measures. No GCC-wide binding AI law was identified in the retrieved materials.[\[14\]](#)[\[16\]](#)[\[41\]](#)

United Arab Emirates - There is no dedicated federal AI law in force in the UAE in the retrieved materials; the applicable framework is built from personal-data and sector rules plus strategy/policy documents.[\[15\]](#) - The UAE's Protection of Personal Data Law and Emirate/free-zone rules are the primary binding overlays for AI involving personal

data.[\[14\]](#)[\[15\]](#) - DIFC Regulation 10, enacted 1 September 2023, specifically regulates processing personal data through autonomous and semi-autonomous systems, including AI. DIFC states Regulation 10 is a risk- and outcomes-based framework and provides accreditation/certification architecture.[\[15\]](#) - Abu Dhabi created the Artificial Intelligence and Advanced Technology Council under Law No. 3 of 2024, according to GCC/UAE legal summaries.[\[14\]](#)

Saudi Arabia - Saudi Arabia's binding baseline is the Personal Data Protection Law and related data/cyber rules; current AI-specific materials identified in the search set are guidance and strategy rather than a general AI act.[\[16\]](#)[\[42\]](#) - SDAIA's Generative Artificial Intelligence Guidelines for Government require alignment with personal data protection, cybersecurity standards, data-classification rules, and AI Ethics Principles, and address legal/ethical compliance, privacy and security, and government-data use.[\[42\]](#) - Saudi government/public statements confirm SDAIA has issued AI ethics principles.[\[43\]](#)

Qatar - Qatar has a National Artificial Intelligence Strategy and a federal data protection law, Law No. 13 of 2016 Concerning Privacy and Protection of Personal Data.[\[44\]](#)[\[45\]](#) - The national AI strategy includes an "AI Ethics and Governance" pillar and states that explainability guidelines are needed for different types of AI decisions.[\[44\]](#)

Bahrain - The retrieved sources characterize Bahrain as active on digital policy and data protection, but no enacted cross-sector AI law was identified in the retrieved official/near-official materials.[\[14\]](#)[\[41\]](#)

Kuwait - The Law Library of Congress summary states Kuwait is in early stages of developing an AI regulatory framework aligned with Vision 2035.[\[41\]](#)

Oman - The same Law Library of Congress summary states Oman has a draft National Artificial Intelligence Policy defining governance for data management and development/use of AI systems.[\[41\]](#)

1. Convergence themes visible across jurisdictions
2. Transparency/disclosure: EU Article 50 disclosures; Utah consumer disclosures; South Korea generative-AI notices/labeling; China's mandatory explicit/implicit labeling; NYC applicant notice; Illinois candidate notice; Qatar strategy references explainability; Saudi/UAE guidance emphasizes transparency.[\[1\]](#)[\[7\]](#)[\[21\]](#)[\[25\]](#)[\[26\]](#)[\[38\]](#)[\[42\]](#)[\[44\]](#)
3. Risk/impact assessments: EU conformity/risk management and some deployer FRIAs; Colorado deployer impact assessments; privacy-law data protection

assessments in states such as Virginia and Connecticut; DIFC Regulation 10 high-risk processing architecture.[\[1\]\[19\]\[28\]\[30\]\[15\]](#)

4. Human oversight/contestability: explicit in EU high-risk rules and reflected in UK data protection guidance and U.S. privacy/employment frameworks.[\[1\]\[9\]\[25\]](#)
5. Data governance/privacy/security: central in EU, China, UK ICO guidance, India DPDP, UAE/DIFC, and Saudi PDPL/SDAIA guidance.[\[1\]\[4\]\[9\]\[13\]\[15\]\[42\]](#)
6. Documentation/model information: explicit for EU GPAI and high-risk providers, Colorado developers, and China filing/security processes.[\[1\]\[19\]\[4\]](#)
7. Content labeling and synthetic media controls: strong in China; present in South Korea and several U.S. states; active in California and Arkansas trackers.[\[7\]\[38\]\[32\]](#)
8. Main differences by actor type in the current patchwork
9. Developer/provider-focused regimes are strongest in the EU (high-risk providers and GPAI providers), China (public-facing service providers plus filing/security), South Korea (AI development operators), and Colorado (developers of high-risk AI).[\[1\]\[4\]\[2\]\[19\]](#)
10. Deployer/user/integrator-focused rules are especially visible in Colorado deployer duties, NYC employment-tool use, Utah consumer-facing disclosure, UK existing-law compliance, and privacy-law profiling/assessment obligations in states such as Connecticut and Virginia.[\[19\]\[25\]\[21\]\[28\]\[30\]](#)
11. Several jurisdictions regulate specific use contexts rather than general model development: NYC employment, Illinois hiring/video interviews, sectoral privacy rules, China online information services, and Gulf government-sector guidance.[\[25\]\[26\]\[5\]\[42\]](#)
12. Binding-law versus guidance snapshot by covered jurisdiction
13. Binding AI-specific enacted law/regulation: EU, South Korea, China, Colorado, Utah, Texas, NYC (local), Illinois hiring law, China labeling/deep synthesis/algorithm/generative AI rules.[\[1\]\[2\]\[4\]\[5\]\[6\]\[7\]\[19\]\[21\]\[23\]\[25\]\[26\]](#)
14. Binding through sectoral/privacy/consumer law instead of general AI act: UK, Japan, Brazil (currently), India, many U.S. states, UAE, Saudi Arabia, Qatar, Bahrain, Kuwait, Oman.[\[9\]\[10\]\[11\]\[13\]\[15\]\[42\]\[45\]\[41\]](#)
15. Soft law/guidance/strategy dominant: Japan AI Guidelines, UK action-plan/regulator-guidance model, Saudi guidelines, Qatar strategy, much of the GCC outside specific free-zone/data regimes.[\[10\]\[8\]\[42\]\[44\]\[41\]](#)

Sources:

- [1] EU Artificial Intelligence Act Explorer / Regulation (EU) 2024/1689 materials (2024) <https://artificialintelligenceact.eu/chapter/5>
- [2] South Korea's AI Basic Act: Overview and Key Takeaways (2026) <https://www.cooley.com/news/insight/2026/2026-01-27-south-koreas-ai-basic-act-overview-and-key-takeaways>
- [3] U.S. State AI Law Tracker – All States (2026) <https://ai-law-center.orrick.com/us-ai-law-tracker-see-all-states>
- [4] Interim Measures for the Management of Generative Artificial Intelligence Services (2023) <https://www.chinalawtranslate.com/en/generative-ai-interim>
- [5] Provisions on the Administration of Deep Synthesis Internet Information Services (2022) <https://www.chinalawtranslate.com/en/deep-synthesis>
- [6] Translation: Internet Information Service Algorithmic Recommendation Management Provisions (2022) <https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022>
- [7] Measures for Labeling of AI-Generated Synthetic Content (2025) <https://www.chinalawtranslate.com/en/ai-labeling>
- [8] AI Opportunities Action Plan (2025) <https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan>
- [9] Guidance on AI and data protection | ICO (N/A) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection>
- [10] Outline of "AI Guidelines for Business Ver1.1" (2024) https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240419_15.pdf
- [11] AI Library Brazil (N/A) <https://www.mofo.com/artificial-intelligence/brazil>
- [12] MeitY advisory (PDF) (2024) <https://www.meity.gov.in/static/uploads/2024/02/9f6e99572739a3024c9cdaec53a0a0ef.pdf>
- [13] The Digital Personal Data Protection Act, 2023 (official PDF) (2023) <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>
- [14] GCC Navigating AI Regulations - the Current Landscape (2025) <https://www.twobirds.com/en/insights/2025/united-arab-emirates/gcc-navigating-ai-regulations---the-current-landscape>

- [15] DIFC Regulation 10 (2023) <https://www.difc.com/business/registrars-and-commissioners/commissioner-of-data-protection/regulation-10>
- [16] Generative Artificial Intelligence Guidelines For Government (2024) <https://sdaia.gov.sa/en/SDAIA/about/Files/GenAIGuidelinesForGovernmentENCompressed.pdf>
- [17] Summary of Artificial Intelligence 2025 Legislation (2025) <https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation>
- [18] Artificial Intelligence (AI) Legislation Tracker 2026: All 50 States (2026) <https://www.multistate.ai/artificial-intelligence-ai-legislation>
- [19] Colorado AI Act (SB 205) text summary (2024) <https://agora.eto.tech/instrument/1376>
- [20] Complying With Colorado's AI Law: Your SB24-205 Compliance Guide (2025) <https://trustarc.com/resource/colorado-ai-law-sb24-205-compliance-guide>
- [21] Utah scales back reach of generative AI consumer protection law (2025) <https://www.davispolk.com/insights/client-update/utah-scales-back-reach-generative-ai-consumer-protection-law>
- [22] Utah Becomes First State To Enact AI-Centric Consumer Protection Law (2024) <https://www.skadden.com/insights/publications/2024/04/utah-becomes-first-state>
- [23] Texas Enacts New AI Law (2025) <https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20250721-texas-enacts-new-ai-law>
- [24] Texas Responsible AI Governance Act Enacted (2025) <https://www.wiley.law/alert-Texas-Responsible-AI-Governance-Act-Enacted>
- [25] NYC's Law Governing Automated Employment Decision Tools Takes Effect July 5 (2023) <https://www.gtlaw.com/en/insights/2023/6/nycs-law-governing-automated-employment-decision-tools-takes-effect-july-5>
- [26] 820 ILCS 42/ - Artificial Intelligence Video Interview Act (2025) <https://law.justia.com/codes/illinois/chapter-820/act-820-ilcs-42>
- [27] US State Privacy Legislation Tracker (2026) <https://iapp.org/resources/article/us-state-privacy-legislation-tracker>
- [28] Connecticut Revamps Its Privacy Law (Again) (2025) <https://www.shb.com/intelligence/newsletters/pds/hansen-connecticut-privacy-law-2025>
- [29] Connecticut Amends the Connecticut Data Privacy Act (2025) <https://www.hunton.com/privacy-and-cybersecurity-law-blog/connecticut-amends-the-connecticut-data-privacy-act>

- [30] Virginia's Consumer Data Privacy Act (2021)
<https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2021/03/virginia-s-consumer-data-privacy-act.html>
- [31] Virginia Contemplates Sweeping New Data Protection Law (2021)
<https://www.hinshawlaw.com/en/insights/privacy-cyber-and-ai-decoded-alert/virginia-contemplates-sweeping-new-data-protection-law>
- [32] Enacted AI Legislation Chart (2026) <https://fpf.org/wp-content/uploads/2026/02/Enacted-AI-Legislation-Chart-.pdf>
- [33] California 2025 legislative wrap-up: More privacy and first-of-its kind AI laws adopted (2025) <https://iapp.org/news/a/california-2025-legislative-wrap-up-more-privacy-and-first-of-its-kind-ai-laws-adopted>
- [34] AI Opportunities Action Plan Government Response (2025)
https://assets.publishing.service.gov.uk/media/678639913a9388161c5d2376/ai_opportunities_action_plan_government_repsonse.pdf
- [35] Japan AI Safety Institute (J-AISI) (2025)
https://aisi.go.jp/assets/pdf/20250501_AISI_en.pdf
- [36] General Understanding on AI and Copyright in Japan (2024)
https://www.bunka.go.jp/english/policy/copyright/pdf/94055801_01.pdf
- [37] South Korea Artificial Intelligence (AI) Basic Act (2025)
<https://www.trade.gov/market-intelligence/south-korea-artificial-intelligence-ai-basic-act>
- [38] Recent Developments in AI Basic Act (2025)
https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=33805
- [39] Artificial intelligence reignites debates in the Brazilian House of Representatives (2025) <https://www.demarest.com.br/en/inteligencia-artificial-reacende-debates-na-camara-dos-deputados>
- [40] Press Release Page | Press Information Bureau (2025)
<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268>
- [41] FALQs: AI Regulations in the Gulf Cooperation Council Member States – Part Two (2024) <https://blogs.loc.gov/law/2024/12/falqs-ai-regulations-in-the-gulf-cooperation-council-member-states-part-two>
- [42] SDAIA Supports Saudi Arabia's Leadership in Shaping ... (N/A)
<https://my.gov.sa/en/news/640446>
- [43] National Artificial Intelligence Strategy for Qatar (2021)
https://policy.mada.org.qa/wp-content/uploads/2022/06/national_ai_strategy_-_english_0.pdf
- [44] Qatar | Jurisdictions (N/A) <https://www.dataguidance.com/jurisdictions/qatar>

Research 2:

Additional angle selected: **Deepening research** — EU AI Act implementation and enforcement architecture, focusing on the operational machinery that turns legal obligations into actual compliance pressure. This angle was only lightly covered in the existing report, which focused mainly on substantive obligations and timelines, but not on who enforces them, what implementation tools now exist, and how this changes the practical burden for providers versus deployers.

1. The EU AI Act now has a multi-layer enforcement architecture, not just a statute.

The European Commission's AI Office is the central EU-level body for implementing the AI Act, especially for general-purpose AI (GPAI). The Commission states that the AI Office's tasks include enforcing and supervising GPAI rules, contributing to the consistent application of the AI Act, and promoting tools such as codes of practice and innovation measures.^[1] This adds an institutional layer that the current report only briefly noted.

2. EU enforcement is split between Union-level and Member State-level actors.

The Commission states that the AI Office and national market surveillance authorities are jointly responsible for implementing, supervising, and enforcing the AI Act.^[2] In practical terms, this means the EU is not using a single regulator for all AI: GPAI oversight is centralized more heavily at EU level, while rules for AI systems in Member States are supervised through national authorities.^{[1][2]}

3. Member States must designate market surveillance authorities and single points of contact.

The Commission's market-surveillance page states that each Member State must have market surveillance authority capacity under the AI Act, and where multiple authorities exist, one single point of contact must be designated.^[2] This is significant for deployers and system providers because enforcement channels can differ by country even under one EU regulation.^[2]

4. Market surveillance authorities have affirmative investigative and reporting powers.

The Commission states these authorities can investigate and enforce compliance with prohibitions and high-risk AI rules, and must report annually to the Commission and relevant national authorities, while also informing the Commission and other Member States of measures adopted and risk-evaluation results.^[2] This indicates that the enforcement system is designed for active cross-border information exchange, not only complaint-based enforcement.^[2]

5. The European AI Board is the coordination mechanism for national enforcers.

The Commission states that national market surveillance authorities "come

together under the framework of the European AI Board” to facilitate cooperation, expertise exchange, and effective enforcement.^[2] This matters for the patchwork analysis because, inside the EU, national variation is meant to be managed through a formal coordination body rather than left entirely decentralized.^[2]

6. Two additional advisory bodies now support EU AI Act enforcement: the Advisory Forum and the Scientific Panel.

The Commission states that the Advisory Forum is established under Article 67 as a general advisory body to the Commission and the AI Board, while the Scientific Panel is an expert body established under Article 68 and Implementing Regulation (EU) 2025/454.^{[3][4]} This expands the EU regime beyond classic market surveillance toward a more technically intensive governance model.^{[3][4]}

7. The Scientific Panel is specifically focused on GPAI risks and technical evaluation.

According to the Commission, the Scientific Panel advises the AI Office and national authorities on implementation of the AI Act and on the impacts and risks of GPAI models; its core tasks include alerting the AI Office to systemic risks, advising on GPAI classification and evaluation methodologies, and supporting market-surveillance activities.^[4] This is directly relevant to foundation-model developers because it creates an expert route through which model-risk evidence can feed into enforcement.^[4]

8. The Advisory Forum adds structured stakeholder input to enforcement and implementation.

The Commission describes it as providing technical expertise and advice on a broad range of AI Act matters, including standardisation and implementation challenges, and notes that it complements the Scientific Panel.^[3] This shows that the EU implementation model is not only regulator-driven but also organized around formal expert and stakeholder consultation.^[3]

9. The EU has created voluntary pre-compliance tools that are already shaping market behavior ahead of full high-risk enforcement.

The Commission states that the AI Pact is a voluntary initiative launched to support future implementation and to invite providers and deployers from Europe and beyond to comply with key AI Act obligations early.^{[5][6]} This is a practical compliance-development tool that sits between soft law and binding law.^{[5][6]}

10. More than 100 companies signed the EU AI Pact pledges in 2024.

In a Commission press release, the Commission announced that over a hundred companies became the first signatories of the AI Pact and its voluntary pledges.^[7] This is concrete evidence that the AI Act is already influencing provider and deployer governance practices before all phases of the Act fully apply.^[7]

11. **The AI Pact is structured around organizational governance commitments, not just abstract principles.** The Commission press release says the pledges include an AI governance strategy to foster AI uptake in the organization and work toward future compliance with the AI Act.[\[7\]](#) This is important because it shows early convergence around internal governance systems as a compliance expectation, even before certain mandatory obligations bite.[\[7\]](#)
12. **A key 2025 implementation development is the GPAI Code of Practice.** The Commission's AI Act page states that the GPAI Code of Practice is a voluntary compliance tool submitted by independent experts to help providers comply with AI Act obligations related to transparency, copyright, and safety and security.[\[6\]](#) The Commission's dedicated page on the code describes its contents and presents it as one of the main implementation tools for GPAI obligations.[\[8\]](#)
13. **The GPAI Code of Practice directly targets model-provider obligations, not mainly deployer obligations.** The Commission states that the code is intended to help providers comply with obligations related to transparency, copyright, and safety and security.[\[6\]](#)[\[8\]](#) This reinforces the point that, within the EU framework, foundation-model/provider compliance is becoming operationalized through dedicated instruments separate from the high-risk system rules that affect many deployers.[\[6\]](#)[\[8\]](#)
14. **The Commission finalized a mandatory training-data transparency template for GPAI providers on 24 July 2025.** The Commission press release states it presented a template for GPAI model providers to summarize the data used to train their models.[\[9\]](#) This is a major implementation step because the existing report noted the underlying transparency duty, but this new tool shows that the obligation has moved from statutory text to a prescribed operational format.[\[9\]](#)
15. **The training-data summary template standardizes how GPAI providers must disclose training-content information.** The Commission's July 2025 release describes the template as the instrument GPAI providers use to summarize the data used for training.[\[9\]](#) This means training-data transparency is no longer only a principle-level obligation; it now has a defined reporting format that providers must use.[\[9\]](#)
16. **The emerging EU implementation trend is proceduralization: obligations are being converted into templates, codes, boards, expert panels, and reporting channels.** This is not a matter of opinion but an observable fact from the Commission's implementation pages and press materials: the AI Office exists,[\[1\]](#) national authorities are being designated,[\[2\]](#) the Advisory Forum and Scientific

Panel are operational,[\[3\]\[4\]](#) the AI Pact is active,[\[5\]\[7\]](#) the GPAI Code of Practice exists,[\[6\]\[8\]](#) and a mandatory training-data transparency template has been issued.[\[9\]](#) Collectively, these show that the EU is moving beyond legislation toward an administrative compliance system.

17. Implication for comparative burden: the EU's operational burden on model developers is increasing through implementation detail, not just legal text.

Factually, GPAI providers now face a central AI Office, expert-panel scrutiny pathways, a code of practice, and a mandatory training-data summary template.[\[1\]\[4\]\[6\]\[8\]\[9\]](#) By contrast, deployers are more exposed to national market-surveillance channels and Member State authority structures for system-level enforcement.[\[2\]](#) This deepens the existing report's conclusion that the EU imposes a high burden on both groups, but shows that the burden is being institutionalized differently for providers and deployers.[\[1\]\[2\]\[4\]\[6\]\[9\]](#)

18. This implementation architecture also helps explain why the EU may be operationally more coherent than the U.S. state patchwork despite national variation. Within the EU, national enforcement is explicitly linked through single points of contact, annual reporting obligations, and the European AI Board.[\[2\]](#) The current report discussed divergence across jurisdictions globally; this additional evidence shows that, internally, the EU is trying to reduce fragmentation through formal coordination machinery.[\[2\]](#)

19. A notable 2026 development in the Commission's official AI Act page is a further extension for certain AI systems embedded in regulated products. The Commission's AI Act page states that, as a result of the political agreement on the 'AI omnibus' simplification proposal, the rules for high-risk AI systems embedded into regulated products have an extended transition period until 2 August 2028.[\[6\]](#) This timing detail is incorporated in the body of this report (Section 2.8).

20. This 2028 extension is narrower than a general delay of the AI Act. The Commission page specifically ties the extended transition to "high-risk AI systems - embedded into regulated products," while separately maintaining the broader framework, including the GPAI Code of Practice and other implementation tools.[\[6\]](#) The fact pattern therefore suggests targeted timing relief for a subset of high-risk systems rather than wholesale postponement of the Act.[\[6\]](#) However, the same "AI omnibus" provisional agreement (reached by the Council and the European Parliament on 7 May 2026) is broader than the embedded-product extension alone: it also defers stand-alone Annex III high-risk obligations from 2 August 2026 to no later than 2 December 2027 by linking their application to the

availability of harmonised standards and support tools, while GPAI obligations and the core governance provisions keep their existing dates.^[6]

Overall, this deepening research shows that the EU is no longer just the jurisdiction with the most detailed AI statute; it is also the jurisdiction with the most developed implementation machinery currently visible in official sources. That machinery increasingly differentiates the compliance experience of **GPAI/model providers** from that of **system providers and deployers**, and it is likely to be a major practical driver of compliance burden in 2026–2028.^{[1][2][3][4][6][8][9]}

Sources:

- ^[1] European AI Office | Shaping Europe's digital future (2026) <https://digital-strategy.ec.europa.eu/en/policies/ai-office>
- ^[2] Market Surveillance Authorities under the AI Act (2026) <https://digital-strategy.ec.europa.eu/en/policies/market-surveillance-authorities-under-ai-act>
- ^[3] AI Act Advisory Forum | Shaping Europe's digital future (2026) <https://digital-strategy.ec.europa.eu/en/policies/ai-advisory-forum>
- ^[4] AI Act Scientific Panel | Shaping Europe's digital future (2026) <https://digital-strategy.ec.europa.eu/en/policies/ai-scientific-panel>
- ^[5] AI Pact | Shaping Europe's digital future (2026) <https://digital-strategy.ec.europa.eu/en/policies/ai-pact>
- ^[6] AI Act | Shaping Europe's digital future (2026) <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
- ^[7] Over a hundred companies sign EU AI Pact pledges to drive trustworthy and safe AI development (2024) https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4864
- ^[8] The General-Purpose AI Code of Practice (2026) <https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai>
- ^[9] Commission presents template for General-Purpose AI model providers to summarise the data used to train their model (2025) <https://digital-strategy.ec.europa.eu/en/news/commission-presents-template-general-purpose-ai-model-providers-summarise-data-used-train-their>

Research 3:

Additional angle selected: **Complementary research** — the growth of non-binding but operationally important governance infrastructure that sits below or alongside AI legislation. This angle adds new information not centered on statutes themselves: international standards, incident-reporting frameworks, national governance charters,

and privacy-regulator technical studies. These instruments matter because they can shape practical compliance burdens and create convergence even where jurisdictions have no binding omnibus AI law.

1. **A global layer of implementation infrastructure is emerging alongside formal AI laws.** The current report focuses mainly on legislation and regulator guidance. Additional research shows that, by 2026, multiple jurisdictions and international bodies are building practical governance tools below the level of statute: management-system standards, incident-reporting frameworks, technical standardisation, and national AI charters [\[1\]\[2\]\[3\]\[4\]\[5\]\[6\]\[7\]](#). These tools are not necessarily binding, but they are increasingly specific enough to influence procurement, internal governance, audits, and evidence of due care [\[1\]\[3\]\[4\]](#).
2. **ISO/IEC 42001 has created a cross-jurisdictional organizational governance baseline for both AI providers and AI users.** ISO states that ISO/IEC 42001:2023 is the world's first AI management system standard and that it specifies requirements for establishing, implementing, maintaining, and continually improving an AI management system (AIMS) within organizations [\[1\]](#). ISO also states that the standard is designed for entities **providing or utilizing AI-based products or services**, which is notable because it maps directly onto the developer/provider versus deployer/user split used in the main report [\[1\]](#). This means that, outside binding AI statutes, there is now a global governance template that applies to both sides of the AI value chain [\[1\]](#).
3. **ISO/IEC 42001 is process-focused rather than model- or sector-specific.** ISO describes the AIMS as a set of organizational elements used to establish policies, objectives, and processes for the responsible development, provision, or use of AI systems [\[1\]](#). Factually, this differs from the EU AI Act's use-case and risk-tier approach and from China's activity-specific rules; it offers a management-system structure rather than prescribing prohibited practices or high-risk categories [\[1\]](#).
4. **The U.S. governance stack now includes detailed voluntary generative-AI risk guidance from NIST, even without a federal AI statute.** NIST's official publication page states that the *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile* is an official NIST publication [\[4\]](#). The publication itself states that it is a cross-sectoral profile for generative AI and is intended to help organizations apply the AI RMF to generative AI contexts [\[4\]](#). This adds a concrete operational layer to the U.S. landscape described in the report: even though the United States lacks a federal AI law, it has increasingly detailed federal technical guidance for AI risk management [\[4\]](#).

5. **NIST's Generative AI Profile is oriented to lifecycle controls that resemble obligations found in binding laws elsewhere.** In the NIST AI 600-1 publication, examples of recommended inventory and governance information include acceptable-use policies, assumptions and limitations of use, disclosure information or notices, incident response plans, data provenance information, human-oversight roles and responsibilities, underlying foundation-model versions and access modes, and updated hierarchies of identified risks [\[4\]](#). These are objective indicators that the U.S. voluntary framework is converging operationally with concepts that appear in the EU AI Act and other regimes: documentation, transparency, incident handling, human oversight, provenance, and ongoing monitoring [\[4\]](#).
6. **The OECD has built a structured incident-reporting framework that could become a common language across otherwise divergent legal regimes.** The OECD's 2025 paper *Towards a common reporting framework for AI incidents* states that the framework contains **29 criteria** intended to help policymakers understand AI incidents across diverse contexts and identify high-risk systems [\[2\]](#). The OECD's AI Incidents and Hazards Monitor page further states that the OECD is developing definitions and monitoring through a common reporting framework, supported by an Expert Group on AI Incidents [\[3\]](#). This is significant because the current report emphasized divergence in legal architecture; the OECD work shows convergence at the level of post-deployment incident description and analysis [\[2\]](#) [\[3\]](#).
7. **The OECD framework defines both incidents and hazards, not only realized harms.** The OECD paper and related OECD materials distinguish between AI incidents and AI hazards, and the paper includes fields for quantifying harm such as economic losses, death, injury, number of affected stakeholders, and compensation [\[2\]](#). This is notable because many national regimes focus on serious incidents once obligations have already been triggered, whereas the OECD framework is designed to support broader international learning across both realized and potential harms [\[2\]](#)[\[3\]](#).
8. **The OECD incident framework is actor- and sector-neutral.** The OECD paper includes categories for the business function where an incident occurred, such as human resource management, sales, ICT management and information security, marketing and advertisement, logistics, citizen/customer service, procurement, compliance and justice, and research and development [\[2\]](#). Factually, this means the framework is not limited to a single sector like employment or healthcare, and it can capture both developer-side and deployer-side failures [\[2\]](#).

9. **In the EU, standardisation is becoming a separate compliance layer in addition to the AI Act's legal obligations.** The European Commission's AI Act standardisation page states that harmonised standards will offer legal certainty under the AI Act, and that once standards are published by CEN and CENELEC, the Commission will assess them and then reference them in the Official Journal of the EU [\[5\]](#). The Commission also states that, on 19 November 2025, the Digital Omnibus proposed linking the application of rules for high-risk AI systems to the availability of support tools, including standards [\[5\]](#). This adds a new operational dimension to the EU landscape: practical compliance for high-risk systems will depend not only on the statute and AI Office machinery already covered, but also on the production and citation of harmonised standards [\[5\]](#).
10. **EU standardisation is designed to create presumption-of-conformity pathways.** CEN-CENELEC's JTC 21 states that its purpose is to develop European standards that provide manufacturers with a presumption of conformity with the AI Act [\[6\]](#). This matters because it shows that, for EU high-risk providers in particular, compliance may increasingly be evidenced through adherence to technical standards rather than only bespoke legal interpretation [\[5\]\[6\]](#).
11. **The EU's standards pathway is especially relevant to high-risk system providers, but it may indirectly shape deployers as well.** The Commission describes harmonised standards as a source of legal certainty under the Act [\[5\]](#). Because providers of high-risk systems need to demonstrate compliance and deployers often depend on provider documentation, the standards infrastructure is likely to affect the information packages, instructions, and conformity artifacts that downstream users receive [\[5\]\[6\]](#).
12. **Brazil's data protection authority has begun to translate AI governance into privacy-regulator technical analysis before any AI bill is enacted.** The Brazilian ANPD announced an English-language version of its *Technology Radar – Generative Artificial Intelligence* in December 2024, aimed at an international audience [\[7\]](#). According to ANPD-related reporting describing the official publication, the study addresses topics such as data scraping/web scraping and synthetic content generation, both of which may involve personal data processing [\[7\]](#). This adds a new fact pattern for Brazil beyond the pending PL 2338/2023 bill: the national privacy authority is already developing a technical interpretation layer for generative AI under existing LGPD-based oversight [\[7\]](#).
13. **Brazil's ANPD work shows how privacy regulators can shape AI governance without an AI-specific law.** The ANPD's Technology Radar series is expressly

about how emerging technologies affect the personal-data-protection landscape [7]. Factually, that means Brazil's immediate AI compliance burden is being shaped not only by the pending AI bill and LGPD enforcement generally, but by regulator-authored technical framing of issues like scraping, synthetic content, and personal-data risks in generative AI [7].

14. **The Gulf region is adding principle-based national AI governance instruments even where binding AI laws remain limited.** The UAE's official legislation portal states that the *UAE Charter for the Development and Use of Artificial Intelligence* aims to achieve the strategic goals of the UAE AI Strategy [8]. This provides a formal national governance reference point beyond the data-protection and free-zone rules already noted in the main report [8].
15. **The UAE Charter is a policy instrument rather than a standalone AI statute, but it is meant to guide development and use.** The official UAE policy page identifies the charter as a framework for the development and use of AI [8]. This is important because it adds a governance layer that applies conceptually across sectors even though the UAE still lacks a general binding AI law in the material reviewed [8].
16. **Saudi Arabia's AI ethics framework is more structured than a generic principles statement.** SDAIA's official *AI Ethics Principles* document sets out lifecycle-oriented controls covering planning and design, input data preparation, building and validation, and deployment and monitoring [9]. The document also includes substantive principles such as fairness, privacy and security, humanity, social and environmental benefits, reliability and safety, transparency and explainability, and accountability and responsibility [9]. This adds a finer-grained operational view to the Saudi discussion in the main report.
17. **Saudi Arabia's ethics framework incorporates a risk-based logic and defined organizational roles.** Secondary descriptions of SDAIA's 2023 AI Ethics Principles report that the framework includes risk categorisation and roles/responsibilities for adopting entities [10][11]. While these descriptions are not the same as statutory mandates, they indicate that Saudi Arabia's guidance is moving beyond abstract ethics into implementable governance design [10][11].
18. **These non-binding infrastructures create a new kind of convergence across very different legal systems.** Across ISO/IEC 42001, the NIST Generative AI Profile, the OECD incident framework, EU standardisation, Brazil's ANPD Technology Radar, the UAE Charter, and Saudi AI ethics materials, recurring factual themes include governance systems, documentation, data provenance, monitoring, human oversight, incident handling, transparency, and lifecycle

controls [\[1\]\[2\]\[4\]\[5\]\[7\]\[8\]\[9\]](#). This convergence is distinct from convergence in formal law: jurisdictions remain divergent on penalties, enforcement powers, and prohibited practices, but they are increasingly similar in the kinds of internal controls they expect organizations to build [\[1\]\[2\]\[4\]\[5\]\[9\]](#).

19. This trend changes the practical compliance picture for firms operating globally.

Even where there is no binding omnibus AI law, organizations may still face strong expectations to maintain governance systems, inventories, incident workflows, documentation, and risk-management processes because those elements are now embedded in standards and official technical guidance [\[1\]\[4\]\[7\]\[9\]](#). These expectations can influence procurement, regulator dialogue, assurance programs, and readiness for future binding rules [\[1\]\[5\]\[8\]](#).

20. Implication for the comparative report: the “global AI regulation patchwork” is not only a patchwork of laws; it is increasingly also a patchwork of interoperable compliance artifacts. The legal layer is still fragmented, but a second layer of governance infrastructure is becoming more standardized internationally through ISO, OECD, NIST, EU harmonised standards work, and national charters/guidance [\[1\]\[2\]\[4\]\[5\]\[8\]\[9\]](#). That second layer may become especially important for model developers and enterprise deployers trying to build one global control environment that can be reused across jurisdictions [\[1\]\[4\]\[5\]](#).

Sources:

- [\[1\]](#) ISO/IEC 42001:2023 - AI management systems (2023) <https://www.iso.org/standard/42001>
- [\[2\]](#) Towards a common reporting framework for AI incidents (2025) https://www.oecd.org/en/publications/towards-a-common-reporting-framework-for-ai-incidents_f326d4ac-en.html
- [\[3\]](#) AI incidents Overview - OECD.AI (2025) <https://oecd.ai/en/site/incidents>
- [\[4\]](#) Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (2024) <https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence>
- [\[5\]](#) Standardisation of the AI Act | Shaping Europe's digital future (2026) <https://digital-strategy.ec.europa.eu/en/policies/ai-act-standardisation>
- [\[6\]](#) European AI Standardization | CEN-CENELEC JTC 21 (2026) <https://jtc21.eu>
- [\[7\]](#) ANPD releases English version of Technology Radar (2024) <https://legismap.com.br/conteudos/artigos-e-noticias/anpd-releases-english-version-of-technology-radar>

- [8] The UAE Charter for the Development and Use of Artificial Intelligence (2024) <https://uaelegislation.gov.ae/en/policy/details/the-uae-charter-for-the-development-and-use-of-artificial-intelligence>
- [9] AI Ethics Principles (2023) <https://sdaia.gov.sa/en/SDAIA/about/Documents/ai-principles.pdf>
- [10] Saudi Arabia: SDAIA publishes AI Ethics Principles version 2.0 (2023) <https://www.dataguidance.com/news/saudi-arabia-sdaia-publishes-ai-ethics-principles>
- [11] Saudi Arabia - AI Ethics Principles (2023) <https://regulations.ai/regulations/RAI-SA-NA-PCAESXX-2023>

Research 4:

Additional angle selected: **Deepening research** — the U.S. enforcement-and-rulemaking layer that regulates AI through existing consumer protection, employment, and privacy authorities rather than through omnibus AI statutes. This angle adds detail not fully developed in the report's U.S. section, which already covers state enacted laws and privacy statutes, but gives less attention to how enforcement and sub-regulatory mechanisms create practical obligations for AI model developers, vendors, and deployers.

1. **In the United States, a major part of the AI compliance burden still comes from enforcement under existing laws rather than AI-specific statutes.** The FTC's AI page shows the agency has built a dedicated AI enforcement/policy hub under its existing authority, and the EEOC has separately created an AI and algorithmic fairness initiative for employment discrimination enforcement.[1][2] This confirms that U.S. AI regulation is not only legislative patchwork; it is also an enforcement patchwork.
2. **The FTC publicly framed AI enforcement as a crackdown on deceptive AI claims and AI-enabled schemes in 2024.** In September 2024, the FTC announced "Operation AI Comply," describing five enforcement actions targeting companies that allegedly used AI claims or AI-enabled tools in deceptive or unfair ways.[3] The FTC's press release stated that the actions built on earlier AI-related cases involving online storefront schemes, AI moderation claims, AI facial recognition, and AI-related accuracy claims.[3]
3. **This FTC activity is highly relevant to AI developers/providers because it targets representations about AI capability, not only end-use harms.** The FTC's 2024 Operation AI Comply announcement focused on false or misleading claims that

products were “AI-powered” or could reliably deliver specified outcomes.^[3] That means the U.S. federal enforcement layer can directly affect model vendors and AI application developers even without a federal AI statute.^[3]

4. **The FTC’s DoNotPay order is a concrete 2025 example of AI-specific enforcement through general consumer-protection law.** In February 2025, the FTC finalized an order against DoNotPay over claims that its service was “the world’s first robot lawyer.” The FTC stated the company had not tested whether its AI-generated legal documents could substitute for a human lawyer’s expertise and that the order prohibits deceptive AI-lawyer claims, imposes monetary relief, and requires notice to past subscribers.^{[4][5]} This shows that, in the U.S., AI vendor marketing and substantiation can itself be a regulated compliance domain.^{[4][5]}
5. **The practical U.S. burden for providers therefore includes substantiating capability claims and avoiding “AI-washing.”** The FTC’s official materials show that companies can face enforcement if they market tools as AI-powered or outcome-capable without adequate support.^{[1][3][4]} This is a different burden from the EU AI Act’s ex ante technical documentation and conformity-assessment system, but it is still a real burden on developers/providers.^{[1][3][4]}
6. **The FTC’s enforcement examples also show that U.S. AI oversight can attach to downstream harms such as fake reviews, child safety, and facial-recognition deployment.** The FTC’s Operation AI Comply press release explicitly pointed to prior cases involving anonymous messaging moderation claims, AI facial recognition used without reasonable safeguards, and business-opportunity schemes using “AI-powered” storefront tools.^[3] This indicates that federal U.S. enforcement spans both provider claims and deployer conduct.^[3]
7. **California’s privacy rulemaking has matured into one of the most operationally significant U.S. deployer-facing AI regimes, even though it is not a standalone AI law.** In September 2025, the California Privacy Protection Agency (CPPA) announced that the Office of Administrative Law approved regulations covering automated decisionmaking technology (ADMT), risk assessments, and cybersecurity audits.^[6] CPPA stated that businesses subject to risk-assessment requirements must begin compliance by January 1, 2026, while businesses have additional time for some ADMT-related obligations.^[6]
8. **California’s ADMT rules are important because they create procedural obligations around AI-like decision systems under privacy law rather than AI-specific law.** Secondary summaries of the final rules report that the regulations apply where ADMT is used to make “significant decisions” concerning consumers

and require businesses to provide notice, opt-out rights in covered cases, and related information/access mechanisms.[\[7\]](#)[\[8\]](#) The same summaries report that the regulations are narrower than earlier drafts and are focused on cases where technology replaces or substantially replaces human decision-making.[\[8\]](#)

9. **California therefore deepens the U.S. patchwork by adding a privacy-rule-based employer regime that resembles some AI-law concepts.** The approved CPPA rules connect automated decision systems with risk assessments, consumer rights, and governance obligations.[\[6\]](#)[\[7\]](#)[\[8\]](#) Functionally, this pushes California closer to the EU/Colorado pattern on impact assessment and significant-decision controls, even though the legal vehicle is CCPA rulemaking rather than an AI act.[\[6\]](#)[\[7\]](#)[\[8\]](#)
10. **The California rules also create a formal reporting channel for risk-assessment information.** Legal analyses of the finalized rules state that for risk assessments conducted in 2026 and 2027, businesses must submit information regarding the assessment to the CPPA by April 1, 2028, even if not the full assessment document itself.[\[7\]](#) This is a concrete operational obligation that increases audit-readiness and recordkeeping burdens for employers.[\[7\]](#)
11. **Colorado's AI Act is more detailed on developer-to-employer information transfer than many summaries suggest.** The official bill text requires developers of high-risk AI systems to provide employers with documentation that includes a general statement of reasonably foreseeable uses and known harmful or inappropriate uses; high-level summaries of training-data types; known or reasonably foreseeable limitations and risks of algorithmic discrimination; the system's purpose, intended benefits and uses; and additional information necessary for employers to comply with their own obligations.[\[9\]](#)[\[10\]](#)
12. **Colorado also requires developers to disclose evaluation and data-governance information to employers.** The official text requires documentation describing how the system was evaluated for performance and mitigation of algorithmic discrimination before being made available; what data-governance measures were used for training data and suitability/bias review; the intended outputs; risk-mitigation measures; and how the system should and should not be used and monitored by an individual when used to make or substantially influence a consequential decision.[\[9\]](#) This is a significant provider burden that mirrors some EU-style provider documentation logic.[\[9\]](#)
13. **This means Colorado's law operationally depends on provider documentation to make employer compliance possible.** Because employers must manage risk,

review for algorithmic discrimination, and give notices, the developer's disclosure package is a core compliance dependency.[\[9\]\[10\]](#) This is an important structural mechanism in the U.S. patchwork: some state AI obligations are transmitted downstream through vendor documentation rather than enforced purely as standalone rules on users.[\[9\]\[10\]](#)

14. **In employment, the EEOC has made clear that employer use of AI and algorithmic tools is already subject to Title VII disparate-impact analysis.** The EEOC's AI initiative announcement states the agency is focused on ensuring that AI and other emerging tools used in hiring and employment decisions comply with federal civil-rights laws.[\[2\]](#) The EEOC's public explainer on its role in AI lists recruiting, screening, hiring, monitoring employees, assessing productivity, setting wages, and deciding whom to promote or fire as areas where AI use may violate employment discrimination laws.[\[11\]](#)
15. **The EEOC's AI materials matter primarily for deployers/employers, but also indirectly for vendors.** The EEOC's Title VII technical-assistance document on adverse impact in software, algorithms, and AI used in employment selection procedures explains that if a tool has an adverse impact on a protected group, its use violates Title VII unless the employer can show the use is job-related and consistent with business necessity.[\[12\]](#) The document also states that employers considering whether to rely on a vendor may want to ask specifically whether the vendor assessed adverse impact using measures such as the four-fifths rule of thumb.[\[12\]](#)
16. **This creates a concrete vendor-management obligation for U.S. deployers using AI in employment.** The EEOC does not create a dedicated AI statute, but its guidance pushes employers to obtain evidence from vendors about testing and adverse-impact assessment.[\[12\]](#) In practice, this makes employment-AI vendors part of the compliance chain even when the legal duty remains on the employer.[\[11\]\[12\]](#)
17. **The U.S. patchwork therefore has a clearer provider/deployer split than an enacted-law inventory alone might suggest.** Federal consumer-protection enforcement by the FTC targets developers/providers and marketers making AI capability claims or enabling deceptive uses.[\[1\]\[3\]\[4\]](#) Employment and privacy rules, by contrast, often place the direct legal obligation on deployers/employers/businesses using the systems, while indirectly pressuring vendors to supply documentation, testing results, and substantiation.[\[6\]\[7\]\[9\]\[11\]\[12\]](#)

18. **Compared with the EU, the U.S. model remains less centralized and less ex ante, but it is not light-touch in operational terms.** The U.S. system uses a combination of FTC deception/unfairness enforcement, EEOC anti-discrimination enforcement, CPPA privacy rulemaking, Colorado-style state AI statutes, and local employment rules rather than one omnibus law.^{[1][2][3][6][9]} The result is a compliance model that is fragmented by legal theory and regulator, not just by geography.^{[1][2][6][9]}
19. **A key implication for comparative analysis is that U.S. compliance burden is understated if measured only by enacted AI-specific statutes.** Official FTC, EEOC, and CPPA materials show that AI obligations in the U.S. are also being created through: (a) substantiation of AI claims, (b) consumer-protection enforcement against AI-enabled conduct, (c) anti-discrimination testing expectations in employment, and (d) privacy-rule-based notice, opt-out, and risk-assessment duties for automated decisionmaking.^{[1][3][4][6][11][12]}
20. **This deepening research supports a refined classification of the U.S. regime:** binding AI-specific law exists in a minority of states, but a large share of the practical burden comes from **enforcement through existing laws and rulemaking under existing privacy and discrimination authorities.**^{[1][2][6][9][12]} For model developers, the highest immediate federal risk visible in the sources is deceptive-claims/AI-washing enforcement by the FTC.^{[3][4]} For deployers, the strongest documented burdens in the sources are California ADMT/privacy obligations, Colorado consequential-decision duties, and EEOC-driven employment testing and vendor-management expectations.^{[6][7][9][12]}

Sources:

- ^[1] Artificial Intelligence | Federal Trade Commission (N/A)
<https://www.ftc.gov/industry/technology/artificial-intelligence>
- ^[2] EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairness (2021) <https://www.eeoc.gov/newsroom/eeoc-launches-initiative-artificial-intelligence-and-algorithmic-fairness>
- ^[3] FTC Announces Crackdown on Deceptive AI Claims and Schemes (2024)
<https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes>
- ^[4] FTC Finalizes Order with DoNotPay That Prohibits Deceptive 'AI Lawyer' Claims, Imposes Monetary Relief, and Requires Notice to Past Subscribers (2025)
<https://www.ftc.gov/news-events/news/press-releases/2025/02/ftc-finalizes-order-donotpay-prohibits-deceptive-ai-lawyer-claims-imposes-monetary-relief-requires>

- [5] DoNotPay | Federal Trade Commission (N/A) <https://www.ftc.gov/legal-library/browse/cases-proceedings/donotpay>
- [6] California Finalizes Regulations to Strengthen Consumers' Privacy (2025) <https://cppa.ca.gov/announcements/2025/20250923.html>
- [7] California Finalizes CCPA Regulations for Automated Decision-Making Technology, Risk Assessments and Cybersecurity Audits (2025) <https://www.skadden.com/insights/publications/2025/10/california-finalizes-cppa-regulations>
- [8] California Finalizes CCPA Regulations on Automated Decision-Making Technology, Risk Assessments, and Cybersecurity Audits (2025) <https://www.coblentzlaw.com/news/california-finalizes-ccpa-regulations-on-automated-decision-making-technology-risk-assessments-and-cybersecurity-audits>
- [9] Senate Bill 24-205 - Colorado General Assembly (2024) https://leg.colorado.gov/bill_files/47770/download
- [10] SB24-205 Consumer Protections for Artificial Intelligence | Colorado General Assembly (2024) <https://leg.colorado.gov/bills/sb24-205>
- [11] What is the EEOC's role in AI? (2024) https://www.eeoc.gov/sites/default/files/2024-04/20240429_What%20is%20the%20EEOCs%20role%20in%20AI.pdf
- [12] Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964 (2023) https://data.aclum.org/storage/2025/01/EOCC_www_eeoc_gov_laws_guidance_select-issues-assessing-adverse-impact-software-algorithms-and-artificial.pdf

Research 5:

Additional angle selected: **Complementary research — the emerging transnational governance layer above domestic AI law.** This angle adds information not separately covered in the current report: binding and voluntary international instruments that do not replace national law, but increasingly shape how states and firms operationalize AI governance across borders.

1. **The Council of Europe AI Framework Convention adds a new binding international-law layer to the AI patchwork.** The Council of Europe states that its Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law is the **first-ever international legally binding treaty** in this field.[1] It was opened for signature on **5 September 2024**. [1][2] This matters

because the current report focuses mainly on national and regional regimes; the Convention creates a separate treaty-level baseline that can influence domestic implementation across signatory states.[\[1\]\[2\]](#)

2. **The Convention is broader geographically than the EU and was negotiated with non-European participants.** The Council of Europe states that the Convention was drafted by its 46 member states with the participation of observer states including **Canada, Japan, Mexico, the Holy See, and the United States**, as well as the **European Union** and additional non-member states including **Australia, Argentina, Costa Rica, Israel, Peru, and Uruguay**.[\[1\]](#) This is a concrete sign that AI governance is no longer only being shaped by single jurisdictions such as the EU or China; there is now a multilateral treaty venue with participation from countries inside and outside Europe.[\[1\]](#)
3. **The Convention is designed as a framework treaty, not a directly self-executing AI rulebook.** The Council of Europe signature chart states the treaty is open for signature by participating states and, after entry into force, accession by other non-member states.[\[2\]](#) Council of Europe materials describe it as requiring parties to adopt or maintain **legislative, administrative, or other measures** to give effect to the Convention.[\[3\]](#) This means the Convention does not itself impose EU-style detailed provider or deployer duties; instead, it requires states to implement domestic measures consistent with the treaty's standards.[\[1\]\[3\]](#)
4. **The Convention applies across the AI lifecycle and is explicitly risk-based.** Council of Europe materials state the treaty aims to ensure that activities within the **lifecycle** of AI systems are consistent with human rights, democracy, and the rule of law.[\[1\]](#) Supporting summaries of the Convention explain that implementation measures are to be **graduated and differentiated** according to the severity and probability of adverse impacts.[\[3\]](#) This is important because it shows convergence with the risk-based logic seen in the EU AI Act, even though the Convention is structured as public international law rather than product regulation.[\[1\]\[3\]](#)
5. **The Convention's practical focus is on public-law outcomes rather than market-access compliance.** The Council of Europe describes the objective as ensuring compatibility with **human rights, democracy and the rule of law**, while also being conducive to innovation.[\[1\]](#) Compared with the EU AI Act, which creates direct obligations for providers and deployers placing systems on the market, the Convention is oriented toward what states must ensure in their legal systems.[\[1\]\[3\]](#) This makes it a different regulatory instrument: treaty-level minimum standards rather than a directly operational compliance code for firms.

6. **The Convention therefore creates an additional route for convergence outside the EU model.** Because the treaty is open beyond Europe and focuses on lifecycle safeguards and human-rights-consistent governance, it can influence domestic AI governance even in countries that do not adopt the EU AI Act structure.[\[1\]\[2\]\[3\]](#) For comparative analysis, this means “global AI regulation” now includes not only jurisdiction-specific statutes, but also treaty commitments that may shape future national laws and enforcement frameworks.[\[1\]](#)
7. **A second transnational layer is the G7 Hiroshima AI Process (HAIP), which created a structured voluntary code for advanced AI systems.** Japan’s official Hiroshima AI Process page states that the Process was launched in **May 2023** following the G7 Hiroshima Summit, and that the **Hiroshima AI Process Comprehensive Policy Framework** was agreed in **December 2023** and endorsed by G7 leaders the same month.[\[4\]](#) The framework includes guiding principles and an international code of conduct aimed at promoting safe, secure, and trustworthy advanced AI systems.[\[4\]](#)
8. **The Hiroshima Code of Conduct is targeted specifically at organizations developing advanced AI systems, including advanced foundation models and generative AI.** The official code states that it is intended for organizations developing the most advanced AI systems, including the most advanced **foundation models** and **generative AI systems**.[\[5\]](#) It also states that organizations should apply the actions across the lifecycle, including **design, development, deployment and use**.[\[5\]](#) This is notable because it is one of the clearest international instruments focused directly on frontier-model developers, rather than on governments alone.[\[5\]](#)
9. **The Code of Conduct’s subject matter overlaps strongly with obligations appearing in binding regimes.** The official code includes actions on identifying, evaluating, and mitigating risks across the AI lifecycle; publishing transparency reports; keeping documentation up to date; reporting evaluations of safety, security, and societal risks; documenting capabilities and limitations; discussing risks such as bias, discrimination, privacy, and fairness; and disclosing governance and risk-management policies.[\[5\]\[6\]](#) These are factual overlaps with themes already visible in the EU AI Act, Colorado’s provider documentation rules, and NIST’s generative AI guidance.[\[5\]\[6\]](#)
10. **In February 2025, HAIP added a Reporting Framework that turns the Code into a repeatable disclosure mechanism.** Japan’s official Reporting Framework page states that the framework was launched on **7 February 2025** as a direct outcome

of the G7 Hiroshima AI Process.^[7] OECD's HAIP transparency page likewise states that the Reporting Framework provides a **standardised structure** for organizations to report on their alignment with the Hiroshima Code of Conduct.^[8] This is important because it moves the process from high-level principles to an operational reporting tool.

11. **The Reporting Framework is no longer limited only to developers; it is open across the AI value chain.** OECD states that the Hiroshima AI Reporting Framework is open to organizations across the AI value chain, including **developers, deployers, and providers** of advanced AI systems.^[8] This expands the framework beyond its original title focus on organizations "developing" advanced AI systems and makes it relevant to the provider/deployer split used in the main report.^[8]
12. **The first reporting cycle produced a measurable disclosure dataset.** OECD states that the first round of the Hiroshima AI Process Reporting Framework resulted in **25 reports**.^[8] OECD's September 2025 publication *How are AI developers managing risks?* presents preliminary insights from submissions by **20 organisations across diverse sectors and countries**.^{[9][10]} Together, these sources show that the Reporting Framework has already generated a body of comparable governance disclosures, even though it is voluntary.^{[8][9][10]}
13. **OECD has become the publication and analysis platform for HAIP transparency.** OECD states that submitted Hiroshima reports will be published on the **OECD AI Policy Observatory** to promote transparency and support responsible development and use of AI.^[8] OECD also published the 2025 analytical report on how AI developers manage risks based on Reporting Framework responses.^{[9][10]} This gives OECD an operational role in cross-border AI governance beyond its earlier principles and incident-monitoring work.
14. **The HAIP framework creates a practical international transparency channel for advanced AI organizations without waiting for binding law.** Japan's official page says participants reported internal benefits from engaging in the reporting process, including value as a transparency tool and as a mechanism for internal capacity-building and coordination.^[7] Factually, this means the framework is serving not only as an external disclosure mechanism but also as an internal governance exercise for participating organizations.^[7]
15. **The HAIP transparency topics map closely onto the compliance artifacts firms are already being asked to produce in stricter jurisdictions.** OECD's 2025 HAIP report quotes Code-of-Conduct actions calling for transparency reports, technical

documentation, evaluation details, model capabilities and limitations, discussion of societal and rights-related risks, red-teaming results, and governance/risk-management policies.[\[6\]\[9\]](#) This is relevant for global firms because these are the same kinds of artifacts increasingly expected under the EU AI Act, U.S. enforcement/risk-management expectations, and standards-based governance frameworks.[\[6\]\[8\]\[9\]](#)

16. **UNESCO adds a different transnational layer focused on state readiness and implementation capacity.** UNESCO states that its Recommendation on the Ethics of AI is a global normative framework, and UNDP/UNESCO materials describe UNESCO's **Readiness Assessment Methodology (RAM)** as a tool directly linked to that Recommendation.[\[11\]\[12\]](#) RAM evaluates a country's AI ecosystem across multiple dimensions including **legal and regulatory, social and cultural, economic, scientific and educational, and technological and infrastructural** dimensions.[\[12\]](#)[\[13\]](#) This is complementary to law-focused analysis because it addresses how countries prepare governance capacity, not just whether they have enacted statutes.
17. **UNESCO RAM is being used in concrete country processes in 2025–2026.** Official and UN-linked materials show RAM consultations or reports in countries including **the Philippines** and **Trinidad and Tobago**, and UNESCO announced a 2026 workshop to unveil the **Lao PDR** RAM report.[\[11\]\[13\]\[14\]](#) This demonstrates that UNESCO's AI governance influence is being operationalized through country-level assessment exercises, not only through broad ethics language.[\[11\]\[13\]\[14\]](#)
18. **UNDP and UNESCO are explicitly packaging AI assessments as governance tools for governments.** A joint UNDP-UNESCO document states that UNESCO RAM and UNDP's AI Landscape Assessment are offered together as complementary support for governments, with RAM taking a deeper dive into the ethical dimensions of AI governance.[\[12\]](#) This creates a practical channel through which international organizations can shape how national governments diagnose regulatory gaps and prioritize future AI policy actions.[\[12\]](#)
19. **These transnational instruments do not impose the same kind of direct firm-level liability as the EU AI Act or China's administrative rules, but they still matter operationally.** The Council of Europe treaty works through state implementation.[\[1\]\[3\]](#) HAIP works through standardized voluntary disclosures by organizations.[\[7\]](#)[\[8\]](#) UNESCO RAM works through country-assessment and policy-capacity building.[\[12\]\[13\]](#) Together, they show that a meaningful part of the global AI governance landscape now operates through treaty commitments, reporting

frameworks, and diagnostic tools rather than only through statutes and enforcement actions.

20. Implication for the main report: the “global AI regulation patchwork” now has a transnational superstructure with three distinct functions. First, the **Council of Europe Convention** provides a binding international human-rights baseline for states.^{[1][2][3]} Second, the **G7 Hiroshima AI Process** provides a voluntary but structured transparency and governance mechanism aimed especially at advanced AI organizations.^{[4][5][7][8]} Third, **UNESCO RAM** provides a state-readiness and governance-capacity tool that can influence future domestic regulation.^{[11][12][13]} These mechanisms are not substitutes for domestic law, but they are now concrete parts of the global AI governance architecture and help explain why some compliance concepts are converging internationally even while legal obligations remain fragmented.^{[1][8][12]}

Sources:

- ^[1] The Framework Convention on Artificial Intelligence (2026)
<https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>
- ^[2] Chart of signatures and ratifications of Treaty 225 (2026)
<https://www.coe.int/en/web/Conventions/full-list?module=signatures-by-treaty&treatynum=225>
- ^[3] Council of Europe Convention on Artificial Intelligence - eucrim (2024)
<https://eucrim.eu/news/council-of-europe-convention-on-artificial-intelligence>
- ^[4] Hiroshima AI Process (2026)
<https://www.soumu.go.jp/hiroshimaaiprocess/en/index.html>
- ^[5] Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems (2023) <https://g7g20-documents.org/database/document/2023-g7-japan-leaders-leaders-annex-hiroshima-process-international-code-of-conduct-for-organizations-developing-advanced-ai-systems>
- ^[6] How are AI developers managing risks? (OECD PDF) (2025)
https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/09/how-are-ai-developers-managing-risks_fbaeb3ad/658c2ad6-en.pdf
- ^[7] Reporting Framework | Hiroshima AI Process (2025)
<https://www.soumu.go.jp/hiroshimaaiprocess/en/report.html>
- ^[8] HAIP Reporting Framework - OECD.AI (2025)
<https://oecd.ai/en/transparency/overview>

- [9] How are AI developers managing risks? Insights from responses to the reporting framework of the Hiroshima AI Process Code of Conduct (2025) <https://oecd.ai/en/ai-publications/how-are-ai-developers-managing-risks-insights-from-responses-to-the-reporting-framework-of-the-hiroshima-ai-process-code-of-conduct>
- [10] Ethics of Artificial Intelligence - UNESCO (2026) <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>
- [11] Artificial Intelligence Assessments (UNDP-UNESCO) (2024) <https://www.undp.org/sites/g/files/zskgke326/files/2024-12/undp-unesco-offer-web-7-aug-2024.pdf>
- [12] UNESCO AI Readiness Assessment Report: Anchoring Ethics in AI Governance in the Philippines (2024) <https://philippines.un.org/en/306159-unesco-ai-readiness-assessment-report-anchoring-ethics-ai-governance-philippines>
- [13] UNESCO AI Readiness Assessment Methodology (RAM) - Consultation Sessions (2025) <http://mpaai.gov.tt/news/unesco-ai-readiness-assessment-methodology-ram-consultation-sessions>
- [14] Lao PDR to unveil UNESCO AI Ethics Readiness Assessment report at national workshop (2026) <https://www.unesco.org/en/articles/lao-pdr-unveil-unesco-ai-ethics-readiness-assessment-report-national-workshop>

Research 6:

Additional angle selected: **Adversarial research** — identifying facts that materially qualify or contradict elements of the current report.

1. **Colorado's regime changed materially from the original SB 24-205 baseline.** SB 24-205 was the first broad U.S. high-risk AI law, with developer/deployer duties and obligations originally scheduled for 1 February 2026 (later delayed to 30 June 2026). Official Colorado legislative materials for **SB26-189** state that the act **repeals and reenacts** those provisions with new requirements regarding the use of automated decision-making technology in consequential decisions, and that developer obligations start **1 January 2027**.^[1] The body of this report reflects the revised SB26-189 regime rather than the original SB 24-205 framework.
2. **Colorado's revised law is narrower and more disclosure-focused than the original SB 24-205.** Colorado's bill page states the reenacted law requires developers of covered ADMT to provide deployers with technical documentation on intended uses, categories of training data, known limitations, and instructions for appropriate use and human review, starting 1 January 2027.^[1] Secondary

analyses report that the 2026 amendment removed the original duty of care, deployer risk-management program requirement, impact-assessment requirement, and certain AG reporting duties.[\[2\]\[3\]](#) If accurate, this means the current report overstates Colorado's 2026 compliance burden for deployers and overstates convergence with the EU model.[\[1\]\[2\]\[3\]](#)

3. **The practical U.S. "highest burden for deployers" ranking in the current report may need revision because Colorado's deployer burden was scaled back.** After SB26-189, the remaining Colorado regime is centered more on documentation transfer, consumer notice, adverse-decision explanation, and human review-related rights than on the original ex ante risk-management architecture.[\[1\]\[2\]\[3\]](#) This weakens the report's conclusion that Colorado is the clearest U.S. analogue to the EU's high-risk deployer regime.[\[1\]\[2\]\[3\]](#)
4. **Colorado's key date is 1 January 2027 under SB26-189.** The earlier SB 24-205 schedule (originally 1 February 2026, later delayed to 30 June 2026) was superseded; official Colorado materials for SB26-189 specify that the new developer obligations begin **1 January 2027**, which is the date used in the body of this report.[\[1\]](#)
5. **California's ADMT rules are more staggered than the current report suggests.** The CPPA's official September 2025 announcement states the regulations were approved by the Office of Administrative Law and that businesses subject to **risk assessment** requirements must begin compliance by **1 January 2026**, but that there is additional time for some requirements, including ADMT.[\[4\]](#) Secondary legal summaries report that businesses using ADMT to make significant decisions must comply with the ADMT requirements beginning **1 January 2027**, and that risk-assessment submission information is due beginning **1 April 2028** for larger businesses.[\[5\]\[6\]](#) This qualifies any impression that California's deployer-facing ADMT obligations broadly began in 2026; the timeline is phased and some ADMT duties begin later.[\[4\]\[5\]\[6\]](#)
6. **California's final ADMT rules are narrower than many broad "AI law" descriptions imply.** Secondary summaries of the final CPPA rules state they apply when technology **replaces or substantially replaces human decision-making** and are limited to certain "significant decision" contexts, with explicit references to artificial intelligence removed from the final text compared with earlier drafts.[\[6\]](#) This qualifies the report's framing of California as moving toward an EU/Colorado-style regime: some functional convergence exists, but the final rule is narrower and privacy-law based rather than a broad AI statute.[\[4\]\[6\]](#)

7. **South Korea's regime is more operationalized than the current report indicates because the Enforcement Decree also took effect.** The U.S. International Trade Administration states that **South Korea's AI Basic Act and its Enforcement Decree took effect on 22 January 2026.**[\[7\]](#) The current report mentions the Act's effective date and notes that implementing posture remains to be observed, but the existence of an effective decree means South Korea has moved beyond statute-only status.[\[7\]](#)
8. **Draft-decree materials show South Korea's implementation details include domestic-agent obligations and more specific transparency methods.** Kim & Chang's analysis of the draft Enforcement Decree states it includes provisions on methods for implementing transparency obligations for generative and high-impact AI business operators, criteria for defining high-performance AI, standards for determining high-impact AI, and the scope of operators required to designate a **domestic agent.**[\[8\]](#) This suggests South Korea's regime may impose more concrete operational requirements on foreign providers than the current report captures.[\[7\]](#)[\[8\]](#)
9. **The UK still lacks a cross-sector AI law, but parliamentary materials show the issue remains active and unresolved rather than settled.** A 2026 House of Lords Library briefing says the UK government's approach remains based on the 2023 white paper's sector-led framework and discusses debate on whether cross-sector AI legislation is needed.[\[9\]](#) This does not contradict the report's statement that the UK has no comprehensive AI Act, but it does qualify any inference that the issue is dormant; cross-sector legislation remains under active parliamentary debate.[\[9\]](#)
10. **Brazil remains without an enacted AI law, but current materials confirm the center of gravity has shifted to the Chamber of Deputies after Senate approval.** Recent Brazil-focused materials state that PL 2338/2023 was approved in the Senate and is currently being processed by the **House of Representatives (Chamber of Deputies).**[\[10\]](#)[\[11\]](#) This supports the report's classification of Brazil as still pending, but it qualifies the procedural status: the bill is no longer merely an undifferentiated congressional proposal; it has passed one chamber and is in the next.[\[10\]](#)[\[11\]](#)
11. **Industry and stakeholder sources are openly contesting the EU GPAI implementation path, especially around clarity and burden.** CCIA Europe stated in July 2025 that the final GPAI Code of Practice still imposed a "disproportionate burden" and that key AI Office guidance was still missing.[\[12\]](#) ITI likewise reacted

publicly to the code's publication.[\[13\]](#) These are not official legal changes, but they are concrete evidence that an important stakeholder constituency disputes whether the EU's implementation machinery is currently delivering clarity. This qualifies the current report's portrayal of the EU implementation layer as a coherence-enhancing architecture; it may also be experienced as a source of uncertainty and burden by affected providers.[\[12\]\[13\]](#)

12. **The EU GPAI code is voluntary, and non-signatories do not automatically get a compliance presumption.** Wharton's summary of the July 2025 code states that providers choosing not to sign the Code still must meet the AI Act's legal requirements, but without the benefit of a presumption of compliance.[\[14\]](#) This fact sharpens the provider-side burden analysis: the code is not itself binding law, yet it functionally creates a two-track environment between signatories and non-signatories.[\[14\]](#)
13. **There was visible mid-2025 uncertainty around possible EU AI Act timing relief before the later targeted extension was formalized.** Reporting cited strong industry calls for delay and noted missed deadlines for guidance on high-risk systems.[\[15\]\[16\]](#) While the Commission's current page now reflects a targeted extension for high-risk AI embedded in regulated products, the documented delay debate and missed-guidance deadlines qualify any claim that EU implementation has been smooth or fully synchronized.[\[15\]\[16\]](#)
14. **No evidence was found in this search set of a binding UAE federal omnibus AI law, despite some public claims online.** More credible regulatory trackers continue to state that the UAE does **not** have a specific standalone AI law and instead relies on strategies, ethical frameworks, data-protection laws, and free-zone regimes such as DIFC Regulation 10.[\[17\]\[18\]](#) This supports the current report against contrary internet claims and is a useful adversarial check.

Bottom line from the adversarial lens: - The strongest factual contradiction to the current report is **Colorado**: the original AI Act framework was significantly revised and delayed, so the report's Colorado timeline, burden characterization, and provider/deployer analysis are now partly outdated.[\[1\]\[2\]\[3\]](#) - The strongest factual qualification is **California**: the CPPA ADMT regime is real but narrower and more staggered than broad summaries imply.[\[4\]\[5\]\[6\]](#) - A second important qualification is **South Korea**: the regime is more concrete than the report suggests because the **Enforcement Decree is already in effect**.[\[7\]\[8\]](#) - A third important qualification is **EU implementation**: the architecture is real, but stakeholder evidence shows that parts of it

remain contested and were accompanied by missed-guidance deadlines and timing uncertainty.^{[12][13][15][16]}

Sources mapping: ^[1] Colorado General Assembly SB26-189 bill page; ^[2] Hunton Andrews Kurth analysis of signed SB 189; ^[3] Holland & Knight analysis of SB 189; ^[4] CCPA official announcement; ^[5] Hunton summary of final California deadlines; ^[6] Coblenz summary of narrowed ADMT rule; ^[7] U.S. International Trade Administration on Korea AI Basic Act; ^[8] Kim & Chang on draft Enforcement Decree; ^[9] UK House of Lords Library briefing; ^[10] Demarest on PL 2338/2023 in Chamber; ^[11] SIDI summary of Senate approval and Chamber progression; ^[12] CCIA Europe statement; ^[13] ITI reaction; ^[14] Wharton summary of GPAI code effects; ^[15] IAPP report on missed EU guidance deadline; ^[16] Inside Global Tech on mid-2025 delay debate; ^[17] Bird & Bird UAE AI regulatory horizon tracker; ^[18] UAE legislation portal policy page.

Sources:

- ^[1] SB26-189 Automated Decision-Making Technology (2026) <https://leg.colorado.gov/bills/sb26-189>
- ^[2] Colorado AI Act Amended and Effective Date Delayed (2026) <https://www.hunton.com/privacy-and-cybersecurity-law-blog/colorado-ai-act-amended-and-effective-date-delayed>
- ^[3] Colorado Governor Signs SB 189, Significantly Amending the State's AI Law (2026) <https://www.hklaw.com/en/insights/publications/2026/05/colorado-governor-signs-sb-189>
- ^[4] California Finalizes Regulations to Strengthen Consumers' Privacy (2025) <https://cpa.ca.gov/announcements/2025/20250923.html>
- ^[5] Newly Approved CCPA Regulations Have Staggered Deadlines for Compliance (2025) <https://www.hunton.com/privacy-and-cybersecurity-law-blog/newly-approved-ccpa-regulations-have-staggered-deadlines-for-compliance>
- ^[6] California Finalizes CCPA Regulations on Automated Decision-Making Technology, Risk Assessments, and Cybersecurity Audits (2025) <https://www.coblentzlaw.com/news/california-finalizes-ccpa-regulations-on-automated-decision-making-technology-risk-assessments-and-cybersecurity-audits>
- ^[7] South Korea AI Basic Act (2026) <https://www.trade.gov/market-intelligence/south-korea-ai-basic-act>
- ^[8] The MSIT Releases Draft Enforcement Decree of the AI Basic Act (2025) https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=32909
- ^[9] AI regulation in the UK: Debate on the need for cross-sector legislation (2026) <https://lordslibrary.parliament.uk/ai-regulation-in-the-uk-debate-on-the-need-for->

cross-sector-legislation

- [10] Artificial intelligence reignites debates in the Brazilian House of Representatives (2025) <https://www.demarest.com.br/en/inteligencia-artificial-reacende-debates-na-camara-dos-deputados>
- [11] PL 2338/2023: the impacts of regulating Artificial Intelligence in Brazil (2026) <https://www.sidi.org.br/en/blog/the-impacts-of-regulating-artificial-intelligence-in-brazil>
- [12] AI Act: EU's Final GPAI Code Imposes Disproportionate Burden, Improvements Required (2025) <https://ccianet.org/news/2025/07/ai-act-eus-final-gpai-code-imposes-disproportionate-burden-improvements-required>
- [13] ITI Reacts to Publication of AI Act GPAI Code of Practice (2025) <https://www.itic.org/news-events/news-releases/iti-reacts-to-publication-of-ai-act-gpai-code-of-practice>
- [14] EU AI Act Update: What the New Code of Practice Means for Business (2025) <https://ai-analytics.wharton.upenn.edu/wharton-accountable-ai-lab/eu-ai-act-update-what-the-new-code-of-practice-means-for-business>
- [15] European Commission misses deadline for AI Act guidance on high-risk systems (2025) <https://iapp.org/news/a/european-commission-misses-deadline-for-ai-act-guidance-on-high-risk-systems>
- [16] European Commission hints at delaying the AI Act (2025) <https://www.insideglobaltech.com/2025/06/12/european-commission-hints-at-delaying-the-ai-act>
- [17] AI Regulatory Horizon Tracker - United Arab Emirates (2026) <https://www.twobirds.com/en/capabilities/artificial-intelligence/ai-legal-services/ai-regulatory-horizon-tracker/uae>
- [18] UAE's International Stance on Artificial Intelligence Policy (N/A) <https://uaelegislation.gov.ae/en/policy/details/uae-s-international-stance-on-artificial-intelligence-policy>