Global AI Compliance & Governance Developments Monthly Report April 2025

Prepared by:
Certifyi Global Reports Team

Date of Issue:
May 3, 2025

certifyi

Global AI Governance, Risk, and Compliance Report: April 2025 Edition

Executive Summary

April 2025 marked a pivotal month in global AI governance, with regulatory advancements, enforcement actions, and cybersecurity threats shaping the compliance landscape. The United States shifted toward pro-innovation policies while maintaining safeguards, the EU refined its AI Act implementation, and Asia-Pacific nations adopted divergent strategies-from China's strict content labeling to Japan's minimal-intervention approach. Key developments include the FTC's crackdown on misleading AI claims, new EU guidelines for general-purpose AI models, and emerging vulnerabilities in large language models (LLMs). This report synthesizes critical updates and offers actionable strategies for organizations navigating this evolving terrain.

Introduction

This report provides a comprehensive analysis of April 2025's AI governance developments across major jurisdictions, frameworks, and industries. Designed for compliance officers, risk managers, and executives, it highlights regulatory shifts, enforcement trends, and emerging risks while emphasizing scalable solutions for maintaining trust and compliance.

Regional Regulatory Updates

United States: Pro-Innovation with Guardrails

The U.S. prioritized AI innovation through executive and regulatory actions:

- **Executive Order on AI Education**: Signed April 23, 2025, this order establishes a White House task force to expand AI literacy via public-private partnerships, targeting K–12 programs and workforce training.
- **OMB Memoranda M-25-21/M-25-22**: Issued April 3, these directives accelerate federal AI adoption, rescind prior Biden-era guidance, and mandate agency AI strategies within 180 days. Chief AI Officers are reframed as "change agents" to drive innovation.
- **FTC Enforcement**: On April 28, the FTC proposed a settlement requiring Workado, LLC to substantiate its "98% accuracy" claims for an AI content detector, signaling heightened scrutiny of AI marketing.

European Union: Refining the AI Act

The EU advanced its regulatory framework:

- **Draft GPAI Guidelines**: Published April 22, these clarify obligations for general-purpose AI providers, including thresholds for classifying models (e.g., training compute $>10^{22}$ FLOP) and open-source exemptions.
- **AI Continent Action Plan**: Unveiled April 9, this strategy aims to position Europe as an AI leader via five pillars: computing infrastructure, data access, skills, sectoral adoption, and regulatory simplification. Key initiatives include AI Factories and a Cloud & AI Development Act.
- **Member State Alignment**: Spain and Italy drafted laws to align national sanctions with the EU AI Act, while Czechia proposed oversight roles for its telecom regulator.

United Kingdom: Collaborative Governance

The UK emphasized stakeholder engagement:

- **AI-Copyright Consultation**: Over 11,500 responses delayed legislative timelines, but working groups will address text/data mining challenges.
- **ICO-CMA Joint Statement**: Released April 29, this guidance avoids favoring open/closed AI models but stresses transparency and contractual controls for personal data use.

Asia-Pacific: Divergent Strategies

- **China**: Enforced strict AIGC labeling rules (effective September 2025), requiring visible and metadata tags for AI-generated content. Cybersecurity Law amendments tightened data controls.
- **Japan**: Submitted its "AI Promotion Law" to parliament, prioritizing R&D with no direct penalties for non-compliance. Amendments to data laws aim to ease personal data use for AI.
- **India/Singapore**: Advanced AI ethics frameworks, though no major legislation emerged in April.

AI Governance Frameworks and Standards

Evolution of Global Standards and Best Practices

Global organizations and standards bodies continued to promote structured AI risk management approaches in April 2025, providing organizations with valuable frameworks for responsible AI governance. The new US Office of Management and Budget memoranda explicitly require each federal agency to develop an enterprise-wide AI strategy within 180 days – a mandate that includes mapping current and planned AI uses, setting maturity goals, and documenting risk mitigations. This government-sector requirement parallels similar frameworks being adopted in the private sector, where many companies are leveraging established standards like the NIST AI Risk Management Framework (RMF) and ISO/IEC 42001:2023 for AI management systems to systematically identify, assess, and control AI lifecycle risks. These frameworks provide essential structure for organizations implementing AI governance programs.

The Organization for Economic Co-operation and Development (OECD) expanded its AI governance toolkit in February 2025 by launching a voluntary High-risk AI Providers (HAIP) Reporting Framework that invites organizations to publicly disclose their AI governance practices under the G7 AI Code of Conduct. Firms developing advanced AI systems can submit a public report (with the first deadline being April 15) covering critical topics such as risk identification methodologies, data quality and security controls, transparency measures, governance structures, and content labeling practices. This voluntary disclosure mechanism allows leading organizations to demonstrate their commitment to responsible AI while establishing industry benchmarks for governance practices. The adoption of these varied but complementary frameworks indicates a growing global consensus around the need for structured approaches to AI risk management, even as specific regulatory requirements continue to evolve.

EU AI Act Implementation Guidance

Specific implementation guidance continued to emerge for the EU AI Act, providing much-needed clarity for organizations preparing for compliance. The April 22 EU draft guidelines released by the EU AI Office addressed several crucial definitional questions, including precisely when a model qualifies as "general-purpose" and what triggers the re-classification of a modified model for instance, establishing a one-third compute threshold as a key metric. These guidelines also clarify how the AI Act's provisions apply in practical scenarios, such as defining exactly when a provider is considered to have "placed on the market" a GPAI model, which triggers specific compliance obligations. This level of detail helps organizations determine whether and how particular aspects of the regulation apply to their AI systems.

Importantly, the European Commission indicated in these guidelines that a forthcoming EU Code of Practice for GPAI is in development. This code will offer significant benefits to compliant organizations, as providers who formally adhere to its provisions may potentially face a reduced compliance burden under the AI Act. Compliance officers and AI governance teams should closely monitor the development of these frameworks – including NIST guidelines, ISO standards, OECD reporting mechanisms, and EU codes of practice – and align their internal policies and controls accordingly to ensure comprehensive coverage of risk assessment, documentation, and monitoring requirements across all applicable jurisdictions. This harmonized approach to compliance can significantly reduce the complexity of managing multiple regulatory obligations.

Industry Practices and Corporate Compliance

Emerging Corporate Governance Structures

The corporate sector is increasingly adopting formal AI governance structures, even in advance of binding regulatory requirements. While no major new industry standards were issued in April 2025, firms are proactively implementing internal AI governance frameworks to address the unique risks posed by these technologies. Many large technology and financial services companies have established dedicated AI ethics committees, appointed senior AI risk officers with direct reporting lines to executive leadership, and implemented comprehensive internal model-audit procedures aligned with ISO 42001 concepts. These governance structures enable organizations to systematically identify and mitigate AI risks before they materialize into compliance violations or reputational damage. The trend toward formalized AI governance reflects growing recognition that effective risk management requires specialized expertise and dedicated oversight.

Several leading organizations are participating in pilot programs and public-private partnerships designed to test compliance tools and frameworks, contributing valuable practical insights to the development of effective governance approaches. The OECD's voluntary reporting framework has emerged as a valuable venue for companies to showcase their risk management efforts, with early adopters publishing their HAIP reports (due by April 15) to benchmark their controls for data quality, model evaluation, and transparency against industry peers. These public disclosures not only demonstrate compliance readiness but also contribute to the development of shared best practices across the AI ecosystem. Organizations should consider participation in these voluntary programs as opportunities to demonstrate leadership in responsible AI while gaining practical experience with the documentation and disclosure practices that regulatory compliance will ultimately require.

Transparency and Documentation Practices

A notable trend in industry practice is the growing emphasis on AI model transparency and documentation, which responds to mounting pressure from investors, customers, and regulators for greater visibility into AI development processes. Some firms, particularly cloud providers and specialized AI vendors, have begun voluntarily disclosing detailed information about their model training data and safety testing methodologies. Others are proactively developing sophisticated "AI audit logs" that provide comprehensive traceability for data lineage and model outputs, creating accountability throughout the AI lifecycle. These transparency initiatives anticipate the disclosure requirements that emerging regulations are likely to impose while building trust with stakeholders concerned about AI risks.

These proactive transparency steps reflect market recognition that stakeholders are demanding evidence of robust AI governance even before hard regulatory rules are fully implemented. Organizations seeking to position themselves advantageously in this environment should work to integrate AI-specific controls and verification processes into their existing risk management programs. For example, compliance leaders can collaborate with internal audit and legal teams to verify that appropriate bias-mitigation controls are in place and that high-impact models maintain comprehensive auditability. Certifyi's AI compliance platform can significantly streamline this process by centralizing AI governance documentation and providing continuous monitoring capabilities that verify ongoing adherence to both internal standards and external regulatory requirements.

Enforcement Actions and Compliance Incidents

Regulatory Enforcement Trends

April 2025 regulatory authorities across multiple jurisdictions taking enforcement actions related to AI systems, indicating increasing scrutiny of compliance with existing regulations. In the United States, regulators signaled heightened attention to AI-related claims, with the Federal Trade Commission's proposed order against Workado on April 28 directly targeting inflated marketing claims about AI capabilities. The FTC's action requires the company to substantiate accuracy claims for its "**AI content detector**" with appropriate evidence, establishing that regulators will hold firms accountable for truthfulness in AI marketing. This enforcement posture was reinforced by statements from newly confirmed **FTC Commissioner Mark Meador**, who explicitly warned that the agency intends to leverage existing consumer protection and antitrust laws to address emerging AI risks, including deepfake content that could mislead consumers.

European data protection authorities also demonstrated active enforcement concerning AI systems and the data they process. Ireland's Data Protection Commission opened a formal inquiry into X's (formerly Twitter) new AI

chatbot "Grok," focusing on concerns that the system may be using users' public posts without proper consent for training or operation. This investigation highlights the continuing relevance of data protection laws to AI development, even in the absence of AI-specific regulations. In Germany, the Federal Court of Justice (BGH) issued a significant ruling in April 2025 that GDPR violations can support civil claims for unfair competition, substantially raising the potential financial stakes for companies using personal data to train or operate AI systems. These enforcement actions illustrate how existing regulatory frameworks are being applied to address novel AI risks while purpose-built AI regulations continue to develop.

Security Incidents and Vulnerabilities

While no major AI-specific data breaches were publicly reported in April 2025, several general cybersecurity incidents underscored the importance of robust security controls for AI systems and their supporting infrastructure. Security researchers claimed to have identified a breach affecting **Oracle Cloud in April 2025**, and a separate ransomware attack targeted a U.S. state official during the same period. Although not directly involving AI systems, these incidents highlight the broader cyber risk environment in which AI operates and emphasize the critical importance of securing both the AI training environment and deployment infrastructure against potential attacks. Organizations deploying AI solutions should ensure their security programs address these foundational elements alongside AI-specific vulnerabilities.

The absence of publicly reported major AI-specific breaches should not be interpreted as indicating low risk – rather, it likely reflects the early stage of both AI deployment and associated security monitoring capabilities. As AI adoption accelerates and monitoring improves, we can expect increased visibility into security incidents specifically affecting AI systems. Organizations should proactively implement comprehensive security controls for their AI assets, with particular attention to data protection, access management, and monitoring capabilities. Certifyi's platform can help organizations automate the continuous monitoring of security controls across their AI ecosystem, providing real-time visibility into compliance status and alerting teams to potential security gaps before they can be exploited.

Cybersecurity and AI Threats

Emerging Attack Vectors and Vulnerabilities

April 2025 revealed significant new vulnerabilities in popular language models, with security researchers publishing alarming findings about "jailbreak" techniques that can bypass safety filters in widely used LLMs. On April 29, researchers disclosed methods that allow attackers to circumvent AI safety guardrails through sophisticated prompt engineering. For example, one technique involves embedding a hidden scenario within a prompt that effectively excludes standard AI safety constraints, while another involves alternating between illicit and normal prompts to confuse the model's safety mechanisms. These methods were demonstrated to be effective against major commercial AI services including ChatGPT, Google Gemini, Anthropic Claude, Microsoft Copilot, Meta AI, and X's Grok – essentially all leading consumer-facing language models. When successfully executed, these jailbreak techniques can force AI systems to generate harmful content that would normally be blocked by safety filters, creating significant risks for organizations deploying these models.

A comprehensive security report released by Check Point on April 30 further highlighted the rapidly evolving threat landscape surrounding AI systems. The report included concerning findings from analysis of public chat logs, revealing that approximately 7.7% of prompts submitted to AI systems contained sensitive or confidential data, with 1 in 80 prompts posing a high risk of data leakage. The report identified unauthorized AI tools operating on corporate networks and vulnerabilities in AI platforms as top enterprise threats, creating new attack surfaces that many organizations are not yet equipped to defend. These findings emphasize the urgent need for organizations to extend their security perimeters to encompass AI systems and to implement specific controls designed to address the unique threats these technologies face.

Recommended Security Controls and Mitigations

The cybersecurity developments of April 2025 highlight the critical need for organizations to treat AI systems as distinct attack surfaces requiring specialized security controls. Best practices now include regular adversarial testing of models using the latest jailbreak techniques to identify and address vulnerabilities before they can be exploited. Organizations should implement comprehensive monitoring for anomalous prompt usage patterns that might indicate attempted exploitation and establish strict access controls on AI tools to prevent unauthorized use. Additionally, incident response plans should be updated to specifically address AI-related security incidents, with clear procedures for containing and remediating compromised models.

Security teams are increasingly advised to **"fight AI with AI"** by implementing AI-powered security tools (such as Microsoft's new AI security agents) that can automate the detection of sophisticated phishing attempts and accelerate threat hunting activities. As one Chief Information Security Officer aptly summarized the situation, ***"malicious actors using AI will outpace traditional defenses"*** – making it essential for organizations to incorporate AI threat intelligence into their broader cybersecurity operations. Organizations should work to establish a security posture that accounts for the unique characteristics of AI systems while integrating AI specific protections into their overall security architecture. Certifyi's compliance automation platform can help organizations systematically implement and document these specialized AI security controls, providing both protection against emerging threats and evidence of due diligence for regulators and stakeholders.

Strategic Recommendations for Organizations

Adopt AI Governance Framework

Organizations should implement a comprehensive, risk-based approach to AI governance that addresses both current regulatory requirements and emerging best practices. A foundational element of this approach is maintaining a detailed inventory of all AI/ML systems in use throughout the organization, including foundation models, chatbots, analytics tools, and any other AI-powered applications. This inventory should categorize systems according to risk levels, potentially using the EU AI Act's taxonomy of high-risk categories as a framework even for organizations not directly subject to EU regulation. With this inventory as a foundation, organizations should leverage established frameworks such as the NIST AI Risk Management Framework or ISO 42001 to conduct periodic risk assessments, verify data quality, and monitor system performance. This structured approach helps ensure that limited compliance resources are allocated appropriately based on relative risk.

Clear governance structures with defined accountability are essential for effective AI risk management. Organizations should consider appointing dedicated AI risk officers (mirroring the "**Chief AI Officer**" role mandated for federal agencies) and establishing cross-functional AI governance boards or councils to coordinate risk management activities across departments. These governance bodies should provide regular updates to board members and executive leadership on the organization's AI compliance posture, reflecting the increasing prominence of AI and cybersecurity on board agendas. Comprehensive governance policies should address both ethical considerations like fairness and transparency and legal requirements related to privacy and consumer rights. Certifyi's automated compliance platform can significantly streamline the implementation and management of these governance structures by centralizing documentation, automating assessments, and providing real-time visibility into compliance status across the organization.

Data Governance and Security Implementation

Robust data governance and security controls are fundamental to AI compliance and risk management. Organizations should align their practices with emerging data protection guidance specific to AI systems, such as the EU Data Protection Board's LLM report from April 2025, which offers concrete measures for mitigating privacy risks in generative AI applications. These recommended practices can serve as valuable checklists when designing data handling processes for language models and other AI systems that process personal information. In regions implementing content labeling requirements, such as China's new AIGC rules, organizations should prepare systematic approaches to mandatory content labeling and user notifications. Across all AI initiatives, comprehensive documentation of data sources and model changes is essential not only for regulatory compliance but also to support explainability and facilitate effective incident investigation when issues arise.

AI-specific security controls should be integrated into the organization's broader security program. Regular testing of models against known "jailbreak" prompts and other adversarial attacks can identify vulnerabilities before they can be exploited. Continuous monitoring of model outputs for anomalous or disallowed behavior, combined with technical safeguards such as rate limiting, content filters, and encryption for model files, provides defense-in-depth protection for AI assets. Organizations should ensure their information security teams receive specialized training on emerging AI threats and update incident response playbooks to include scenarios specifically addressing AI failure modes or data leak incidents. Certifyi's automated monitoring capabilities can help organizations continuously verify the effectiveness of these controls and quickly identify security gaps that require remediation, enhancing overall risk management while reducing the manual effort required for compliance activities.

Conclusion

The April 2025 developments in AI governance and regulation reflect an accelerating global focus on managing AI risks while fostering responsible innovation. Regional approaches continue to diverge somewhat with the U.S. emphasizing innovation alongside responsible oversight, the EU implementing its comprehensive regulatory framework, the UK pursuing collaborative governance, and Asian nations adopting varied approaches from China's strict content regulation to Japan's minimal-intervention strategy. Despite these differences, a common theme emerges: the increasing expectation that organizations will implement structured approaches to AI risk management, including formal governance structures, comprehensive risk assessments, and robust technical controls.

Organizations seeking to navigate this complex landscape should implement proactive, risk-based approaches that integrate AI governance into existing compliance frameworks while addressing the unique challenges these technologies present. By maintaining comprehensive AI inventories, establishing clear governance structures, implementing appropriate data and security controls, and staying engaged with evolving regulations, organizations can build compliance programs that not only satisfy regulatory requirements but also build stakeholder trust and create competitive advantage through responsible AI practices. Certifyi's automated compliance platform can help organizations streamline this process, providing continuous monitoring capabilities that verify ongoing compliance while reducing the manual effort required to manage evolving requirements. As AI regulation continues to mature, organizations that establish robust governance frameworks now will be well-positioned to adapt to new requirements and demonstrate leadership in responsible AI development and deployment.

References

1. https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf

2. https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf

3. https://static.carahsoft.com/concrete/files/9717/4412/5797/Guidance_M-25-21_Accelerating_Federal_Use_of_AI_through_Innovation_Governance_and_Public_Trust.pdf

4. https://digitalpolicyalert.org/event/29446-federal-trade-commission-issued-proposed-order-in-its-investigation-into-workado-over-its-alleged-ai-detection-accuracy-claims

5. https://digitalpolicyalert.org/event/29446-federal-trade-commission-issued-proposed-order-in-its-investigation-into-workado-over-its-alleged-ai-detection-accuracy-claims

6. https://artificialintelligenceact.eu/providers-of-general-purpose-ai-models-what-we-know-about-who-will-qualify/

7. https://artificialintelligenceact.eu/providers-of-general-purpose-ai-models-what-we-know-about-who-will-qualify/

8. https://www.csis.org/analysis/eu-ai-continent-action-plan

9. https://www.csis.org/analysis/eu-ai-continent-action-plan

10. https://www.osborneclarke.com/insights/Regulatory-Outlook-April-2025-Artificial-intelligence

11. https://www.osborneclarke.com/insights/Regulatory-Outlook-April-2025-Artificial-intelligence

12. https://jingdaily.com/intels/2025-03/20/china-issues-strict-aigc-labeling-rules-effective-september

13. https://jingdaily.com/intels/2025-03/20/china-issues-strict-aigc-labeling-rules-effective-september

14. https://digitalpolicyalert.org/change/13446-act-on-promotion-of-research-and-development-and-application-of-artificial-intelligence-related-technologies

15. https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2025/03/japans-inaugural-ai-regulations-a-pro-innovation-approach.html

16. https://www.linkedin.com/pulse/japans-ai-promotion-bill-blueprint-innovation-ayush-shrivastava-gjudc

17. https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2025/03/japans-inaugural-ai-regulations-a-pro-innovation-approach.html

18. https://www.oecd.org/en/about/news/press-releases/2025/02/oecd-launches-global-framework-to-monitor-application-of-g7-hiroshima-ai-code-of-conduct.html