AI & Partners

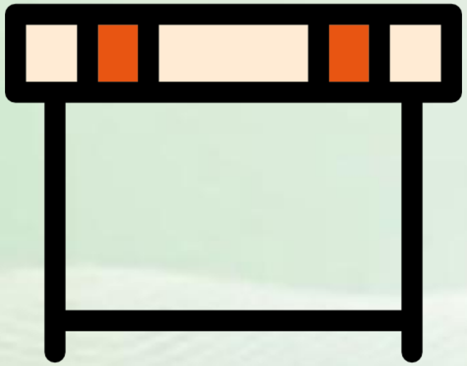
Amsterdam - London - Singapore

EU AI Act

;

Ten Key AI Regulatory Hurdles

January 2025



Contents

Executive Summary

Ten Key AI Regulatory Hurdles

On behalf of AI & Partners, we are delighted to issue the first edition of our annual Ten Key AI Regulatory Hurdles.

This 2025 edition takes into account various regulatory changes brought about following the EU AI Act's entry into force on **1st August 2024,** and implementation of national AI strategies along with such factors as technology advances, disruptive events, and regulatory divergence.

We foresee 2025 to be the Year of AI Regulatory change—across areas of technology and data risks, consumer/ investor protections, and risk management and governance.

In the upcoming slides, we anticipate how this Regulatory Change will alter AI regulatory actions and how companies will need to '*roll-forward*' to mitigate and respond to these emerging risks.

We, naturally, welcome the help you in these and related areas to meet the challenges ahead.

Abbreviation of Terms

AI & Partners
Amsterdam - London - Singapore

AI: Artificial Intelligence

AML: Anti-Money Laundering

CCPA: California Consumer Privacy Act

CISA: Cybersecurity and Infrastructure Security Agency

CTF: Countering the Financing of Terrorism

DPIA: Data Protection Impact Assessment

DMA: Digital Markets Act

EU: European Union

EU AI Act: European Union Artificial Intelligence Act

FCA: Financial Conduct Authority

GDPR: General Data Protection Regulation

GPAI: Global Partnership on AI

IEEE: Institute of Electrical and Electronics Engineers

ISO: International Organisation for Standardisation

ITU: International Telecommunication Union

KYC: Know Your Client

MRA: Mutual Recognition Agreement

NIS2: Network and Information Systems

OECD: Organisation for Economic Cooperation and Development

PIPL: Personal Information Protection Law

RegTech: Regulatory Technology

UNESCO: United Nations Educational, Scientific, and Cultural Organisation

US: United States

WHO: World Health Organisation

Regulatory Divergence

AI & Partners
Amsterdam - London - Singapore

Problem Statement

Regulatory Trends

Required Actions

When different countries or regions create separate rules for artificial intelligence (AI), it causes problems for businesses working across borders. These differences in laws make it harder and more expensive for companies to follow the rules, slow down innovation, and limit how AI tools can be used globally. For example, an AI product might need to be redesigned to meet local legal requirements in different areas.

This lack of consistency creates confusion, wastes time and money, and increases the risk of breaking rules. Companies will need to spend more on teams to manage compliance, adjust their AI systems to fit local regulations, and handle overlapping or conflicting laws. This situation could make it harder for AI to reach its full potential and benefit everyone.

Regulatory Divergence

Problem Statement

Regulatory Trends

Required Actions

Regional Fragmentation

Different countries and regions are making their own AI rules to match their unique political and social needs. This is causing a split in how AI is regulated. For example, tensions between major powers like the U.S., EU, and China lead to different rules for AI. Some governments are also using regulations to protect their local businesses from foreign competition.

Technology-Specific Rules

AI and other technologies are changing so quickly that laws can't keep up. This means some places have strict rules for AI ethics, data use, or cybersecurity, while others have very loose guidelines. For example, one country might require detailed AI checks, but another might only have voluntary standards. This creates confusion for companies working across borders.

Cross-Industry Impact

AI regulations don't just affect tech companies—they impact industries like finance, healthcare, and online shopping too. For instance, cybersecurity laws often apply to all these areas, creating extra work for businesses. Companies need flexible plans to handle these overlapping rules.

Regulatory Divergence

AI & Partners
Amsterdam - London - Singapore

Problem Statement

Regulatory Trends

Required Actions

✓ **Create** a shared database where teams can find all the latest regulatory information.

✓ **Use** tools to track, understand, and predict changes in laws worldwide.

✓ **Use** technology platforms like RegTech to simplify compliance, manage data better, and automate reporting.

✓ **Design** flexible compliance systems that can quickly adjust to local AI rules.

Trustworthy AI Principles

AI & Partners
Amsterdam - London - Singapore

Problem Statement

Regulatory Trends

Required Actions

AI is being used more and more across industries, offering great opportunities but also big challenges and risks. One of the key challenges is ensuring that AI systems are fair, transparent, responsible, and ethical. These principles, commonly referred to as **Trustworthy AI**, aim to reduce risks like bias, discrimination, privacy problems, and misuse while encouraging innovation that helps society.

However, differences in how trustworthy AI is defined and regulated around the world make things uncertain for companies trying to use AI globally. As AI becomes more complex and widespread, the lack of shared rules increases the risk of breaking laws, harming reputations, and slowing down innovation. It also raises ethical concerns and worries about the impact of AI that isn’t well-regulated.

Trustworthy AI Principles

Problem Statement

Risk-Based Rules for AI

Many governments are creating rules based on the level of risk AI systems pose. For example, high-risk uses like facial recognition or managing critical infrastructure have stricter rules, while lower-risk uses have fewer restrictions. The EU's AI Act is a good example of this approach.

Regulatory Trends

Making AI Easy to Understand

Regulators want AI systems to be clear and easy to explain. This helps users and others affected by AI decisions understand how they work, especially in important areas like hiring, loans, or healthcare.

Required Actions

Checking AI for Accountability

There's a growing push for regular checks and audits of AI systems. These reviews look at whether AI is fair, unbiased, and performing as intended, ensuring companies take responsibility for their AI systems.

Trustworthy AI Principles

Problem Statement
Regulatory Trends
Required Actions

- ✓ **Identify** which AI systems pose high risks and create specific strategies to reduce these risks.
- ✓ **Perform** assessments, such as Data Protection Impact Assessments (DPIA), to check how AI might affect people's rights and freedoms.
- ✓ **Use** techniques like synthetic data, or federated learning to reduce risks when working with sensitive data.
- ✓ **Regularly** review data sources to ensure they are diverse, fair, and collected ethically.

Cybersecurity and Data Protection

Problem Statement

Regulatory Trends

Required Actions

The rapid adoption of AI in cybersecurity and data protection presents both opportunities and challenges. While AI can enhance threat detection, automate responses, and strengthen defences, it also introduces risks such as algorithmic bias, misuse of sensitive data, and vulnerabilities to adversarial attacks. Ensuring AI systems in this field are trustworthy—secure, transparent, and ethical—is essential to maintaining trust and protecting sensitive data.

The lack of unified global standards for AI in cybersecurity further complicates the issue, leaving businesses exposed to inconsistent regulations, potential non-compliance, and reputational harm. Additionally, the use of poorly managed AI systems heightens the risk of security breaches, ethical dilemmas, and societal harm, making it critical to address these challenges proactively while fostering innovation.

Cybersecurity and Data Protection

AI & Partners
Amsterdam - London - Singapore

Problem Statement

Regulatory Trends

Required Actions

Increased Focus on Critical Infrastructure

Governments are prioritizing the protection of critical infrastructure such as energy grids, healthcare systems, and financial institutions. Regulations like the U.S. Cybersecurity and Infrastructure Security Agency's (CISA) directives and the EU's revised Network and Information Systems (NIS2) Directive require enhanced security measures for critical sectors.

Mandatory Reporting of Cyber Incidents

Regulators are increasingly mandating that organizations report cyber incidents within tight timeframes. For example, the EU's AI Act requires notification of serious incidents within 72 hours.

Emphasis on Ransomware Resilience

With ransomware attacks on the rise, regulators are focusing on resilience measures such as robust data backups, incident response plans, and reporting mechanisms.

Cybersecurity and Data Protection

Problem Statement

Regulatory Trends

Required Actions

✓ **Create** and regularly test incident response plans that outline procedures for identifying cyberattacks.

✓ **Establish** communication protocols for notifying stakeholders and affected individuals in the event of a breach.

✓ **Conduct** compliance audits to identify gaps in meeting regulatory requirements in each jurisdiction where the organization operates.

✓ **Implement** localized solutions for data storage and processing.

AI in Financial Crimes

Problem Statement

Regulatory Trends

Required Actions

AI is transforming the financial services sector, offering enhanced tools for detecting and preventing financial crimes such as money laundering, fraud, market manipulation, and terrorist financing. While AI systems can analyze vast datasets, detect anomalies, and identify suspicious patterns far more efficiently than traditional methods, their deployment also introduces significant challenges.

FCA

Regulators, such as the Financial Conduct Authority (FCA), are grappling with how to oversee AI in financial crime prevention effectively. The challenge is to strike a balance between fostering innovation and ensuring accountability. Inconsistent regulatory standards across jurisdictions create further difficulties, leaving financial institutions exposed to compliance risks, and reputational damage.

AI in Financial Crimes

Problem Statement

Mandated Explainability and Transparency

Regulators are increasingly requiring that AI systems used for financial crime detection be explainable and transparent. This ensures accountability and fairness, as stakeholders must understand how decisions are made, particularly in high-stakes areas like fraud detection or anti-money laundering (AML).

Regulatory Trends

Integration of AI into Existing Compliance Frameworks

Regulatory bodies are incorporating AI-specific requirements into existing AML and counter-terrorism financing (CTF) frameworks. For instance, financial institutions may need to demonstrate how AI systems enhance compliance and meet reporting obligations.

Required Actions

Proactive Risk Management

Regulators expect financial institutions to proactively assess and mitigate the risks associated with AI deployment. This includes regular audits, stress testing, and scenario analysis.

AI in Financial Crimes

AI & Partners
Amsterdam - London - Singapore

Problem Statement

Regulatory Trends

Required Actions

- ✓ **Align** AI systems with existing AML, countering the financing of terrorism (CTF), and Know Your Customer (KYC) requirements.
- ✓ **Demonstrate** how AI enhances compliance efforts by improving detection rates and reducing false positives.
- ✓ **Embed** ethical considerations into AI development and deployment, focusing on fairness, accountability, and privacy.
- ✓ **Establish** AI committees and appoint AI officers to oversee system implementation.

Addressing AI Bias and Fairness

Problem Statement

Regulatory Trends

Required Actions

As AI systems increasingly influence critical decisions—from hiring and lending to criminal justice and healthcare—ensuring fairness and mitigating bias have become pressing challenges. AI bias can arise from various sources, such as unrepresentative training data, biased algorithms, or human oversight failures. When left unaddressed, these biases can perpetuate discrimination, amplify social inequalities, and erode public trust in AI systems.

From a regulatory perspective, addressing AI bias and fairness presents unique challenges. AI systems often operate as “black boxes,” making it difficult to understand and explain their decisions. The lack of standardized definitions and metrics for fairness further complicates regulatory oversight.

Addressing AI Bias and Fairness

AI & Partners
Amsterdam - London - Singapore

Problem Statement

Focus on Transparency and Explainability

Regulators are emphasizing the importance of transparency in AI systems, requiring organizations to provide explanations for algorithmic decisions. This ensures that affected individuals can understand and challenge potentially biased outcomes.

Regulatory Trends

Cross-Border Collaboration

Recognizing the global nature of AI, regulatory bodies are increasingly collaborating to harmonize standards and share best practices for addressing bias and fairness, including the Global Partnership on AI (GPAI).

Required Actions

Standardization Efforts

Industry groups and standards organizations are working to develop common definitions, metrics, and benchmarks for fairness in AI. Initiatives like the IEEE's Global Initiative on Ethics of Autonomous and Intelligent Systems aim to provide a foundation for regulatory consistency.

Addressing AI Bias and Fairness

Problem Statement

Regulatory Trends

Required Actions

- ✓ **Use** fairness metrics such as demographic parity, equal opportunity, or disparate impact to evaluate algorithmic decisions.
- ✓ **Test** AI systems for disparate impacts across different demographic groups and document the results.
- ✓ **Use** interpretable models where possible to enhance transparency and explainability.
- ✓ **Develop** user-friendly tools that allow stakeholders to interrogate and understand algorithmic decisions.

Operational Resilience in AI Systems

AI & Partners
Amsterdam - London - Singapore

Problem Statement

Regulatory Trends

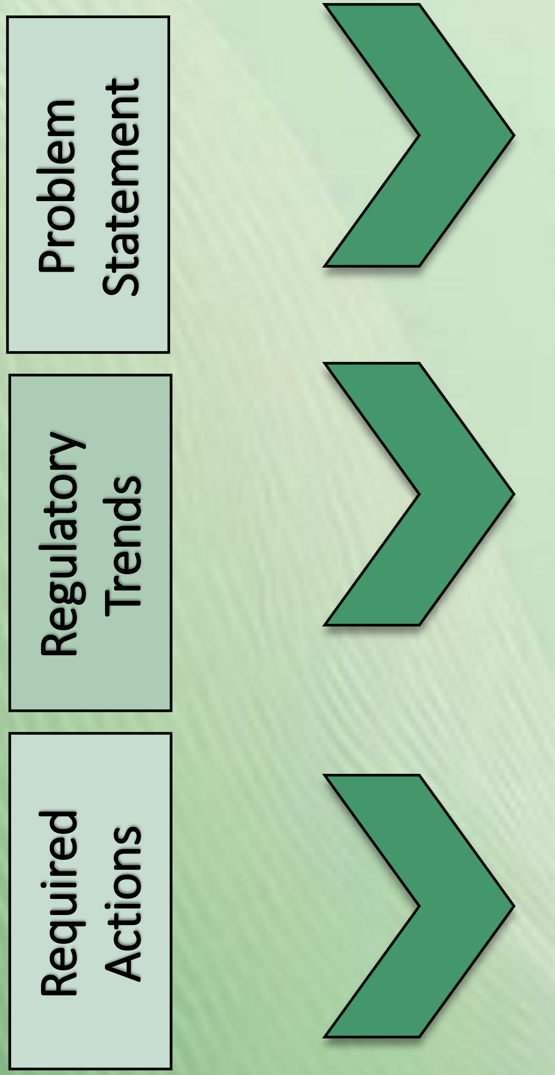
Required Actions

Operational resilience in AI systems is becoming a critical concern as AI continues to underpin essential services in sectors such as finance, healthcare, transportation, and critical infrastructure. Resilience refers to an AI system's ability to continue functioning effectively under adverse conditions, including cyberattacks, system failures, data breaches, or unforeseen events.

The increasing complexity of AI systems, coupled with their dependency on vast datasets and external infrastructures, makes them particularly vulnerable to disruptions. For example, a malfunction in an AI-driven trading algorithm can lead to financial market instability. In addition, the reliance on cloud-based services and third-party vendors introduces further points of vulnerability, e.g. systemic risks.

Operational Resilience in AI Systems

AI & Partners
Amsterdam - London - Singapore



Introduction of AI-Specific Resilience Standards

Regulators are developing specific guidelines and standards to address operational resilience in AI systems. For instance, the EU’s AI Act mandates risk management practices for high-risk AI applications under Article 9.

Focus on Incident Response and Recovery

Regulatory bodies are emphasizing the importance of robust incident response and recovery frameworks to mitigate the impact of AI system failures. Organizations are required to demonstrate their ability to restore operations quickly and effectively.

Integration with Cybersecurity Regulations

Given the overlap between operational resilience and cybersecurity, regulators are aligning AI resilience requirements with existing cybersecurity frameworks. For example, the National Institute of Standards and Technology (NIST) has introduced AI-specific risk management guidelines to complement other cybersecurity standards.

Operational Resilience in AI Systems

Problem Statement

Regulatory Trends

Required Actions

- Conduct comprehensive risk assessments to identify potential vulnerabilities in AI systems.
- Implement controls to mitigate risks, including safeguards against cyberattacks, data breaches, and system failures.
- Develop and regularly update incident response plans to address AI-specific risks.
- Implement backup systems and redundancies to ensure continuity of operations.

AI Accountability for Parties & Providers

Problem Statement

Regulatory Trends

Required Actions

As AI becomes increasingly integrated into critical systems and decision-making processes, ensuring accountability among developers, providers, and users has emerged as a major regulatory challenge. AI accountability refers to clearly defining responsibilities for the outcomes of AI systems, especially when those outcomes have ethical, legal, or societal implications.

The opaque nature of many AI systems complicates the assignment of accountability. For instance, when an AI-driven credit scoring system denies a loan unfairly, it can be difficult to determine whether the fault lies with the developer, the provider, or the firm using the system. Similarly, when AI systems malfunction or produce harmful outcomes, existing legal frameworks often lack clarity on who is legally liable.

AI Accountability for Parties & Providers

Problem Statement

Shared Responsibility Models

Some regulators are advocating for shared responsibility models that distribute accountability across the AI supply chain. This approach ensures that all parties—from data providers to end users—are held accountable for their roles in the development and deployment of AI systems.

Regulatory Trends

Transparency and Explainability Requirements

To enhance accountability, regulators are emphasizing transparency and explainability in AI systems. This includes requiring organizations to document how AI systems are trained, tested, and deployed.

Required Actions

Third-Party Audits and Certifications

Regulators are encouraging or mandating third-party audits of AI systems to verify compliance with ethical and legal standards. Certification schemes for AI systems are also being introduced to provide assurance of their reliability and fairness.

AI Accountability for Parties & Providers

Problem Statement
Regulatory Trends
Required Actions

- ✓ **Create** AI governance committees to oversee accountability efforts and ensure compliance with regulatory requirements.
- ✓ **Assign** specific individuals or teams' responsibility for monitoring and managing AI systems.
- ✓ **Collaborate** with partners across the AI value chain to establish shared responsibility.
- ✓ **Use** standardized contracts and guidelines to allocate accountability among all parties involved in AI development and deployment.

Governance Models for AI Risk

Problem Statement

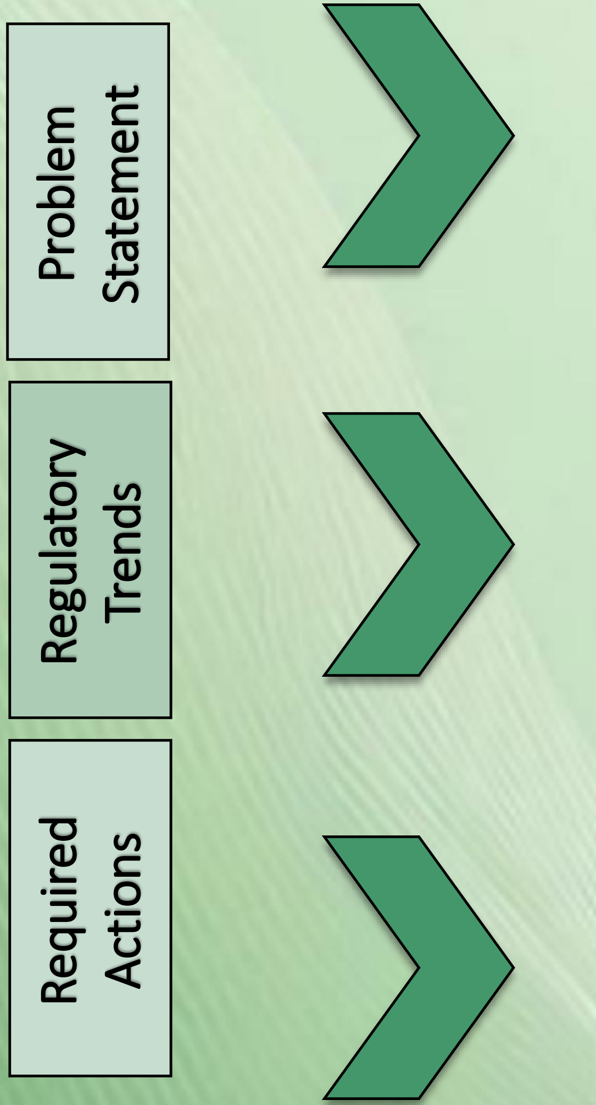
Regulatory Trends

Required Actions

As AI becomes an indispensable component of business operations, public services, and global economies, the need for robust governance models to manage AI risks has become a pressing concern. AI risk governance involves identifying, assessing, and mitigating the potential risks associated with AI systems, including ethical concerns, security vulnerabilities, biases, and accountability gaps.

Traditional governance frameworks are often ill-equipped to address the unique and multifaceted risks posed by AI. The dynamic nature of AI development, the complexity of its applications, and the interdependency between stakeholders in the AI lifecycle—from developers to end-users—make governance particularly challenging.

Governance Models for AI Risk



Problem Statement

Regulatory Trends

Required Actions

Global Collaboration on Governance Standards

Recognizing the borderless nature of AI, international organizations like the OECD and the GPAI are working to develop global governance principles and frameworks to ensure consistency and interoperability.

Role of Independent Oversight

Third-party oversight bodies, including certification agencies and auditing firms, are being incorporated into governance models to ensure impartial evaluation of AI systems. This trend is evident in initiatives like the EU's AI Act, which mandates conformity assessments for high-risk AI systems.

Sector-Specific Governance Requirements

Different industries are subject to varying levels of AI regulation based on the potential impact of AI systems. For instance, healthcare, finance, and autonomous vehicles are areas where stringent governance requirements are emerging due to the high stakes involved

Governance Models for AI Risk

AI & Partners
Amsterdam - London - Singapore

Problem Statement

Regulatory Trends

Required Actions

✓ **Implement** risk assessment processes to identify and categorize AI systems based on their potential impact and associated risks.

✓ **Allocate** resources and oversight efforts based on the risk profile of each AI system.

✓ **Create** governance committees that include representatives from diverse functions, e.g. IT, legal.

✓ **Include** external experts and stakeholders in governance processes to incorporate diverse perspectives.

AI Impact on Markets & Competition

Problem Statement

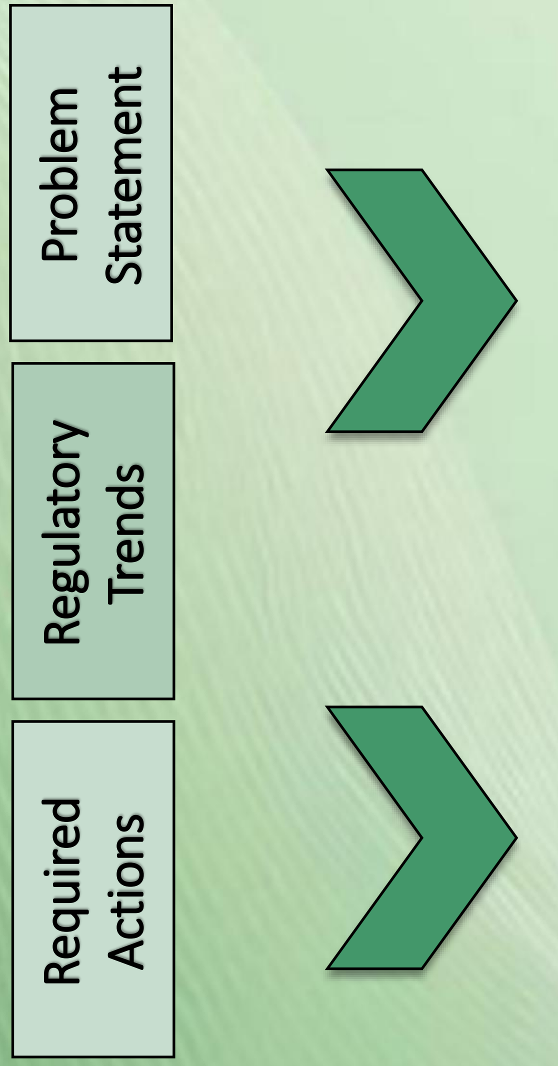
Regulatory Trends

Required Actions

AI has become a transformative force in global markets, driving innovation, efficiency, and new business models. However, its rapid integration into markets also raises significant concerns about its impact on competition. AI technologies can both disrupt traditional industries and consolidate power among dominant players, creating a complex regulatory challenge. Key concerns include monopolistic practices, and algorithmic collusion.

For example, AI-powered platforms can exploit their access to vast datasets to reinforce their market dominance, leaving smaller competitors struggling to compete. Algorithmic collusion—where AI systems independently learn to coordinate pricing or market behaviour—also poses a challenge to antitrust laws that are not designed to address non-human actors.

AI Impact on Markets & Competition



Problem Statement

Regulatory Trends

Required Actions

Modernization of Antitrust Laws

- Traditional antitrust laws are being updated to address the unique challenges posed by AI. For instance, the European Union has introduced the Digital Markets Act (DMA) to regulate the behaviour of large digital platforms that use AI to consolidate market power.
- Regulators are focusing on redefining concepts like dominance, abuse of market power, and anti-competitive practices in the context of AI.

Scrutiny of Algorithmic Practices

- Regulatory bodies are increasingly scrutinizing algorithmic practices, including pricing algorithms, recommendation systems, and ad targeting mechanisms, to identify potential anti-competitive behaviours.
- Efforts are underway to detect and prevent algorithmic collusion, even when it occurs without explicit human intent.

AI Impact on Markets & Competition

AI & Partners
Amsterdam - London - Singapore

Problem Statement

Regulatory Trends

Required Actions

- ✓ **Modernize** antitrust laws to address the unique characteristics of AI-driven markets, such as algorithmic collusion and data monopolies.
- ✓ **Establish** clear definitions and thresholds for anti-competitive practices in the context of AI.
- ✓ **Develop** tools and methodologies for monitoring and auditing AI algorithms to detect anti-competitive behaviours.
- ✓ **Require** businesses to conduct regular audits of their AI systems and report findings to regulators.

Harmonisation across Jurisdictions

AI & Partners
Amsterdam - London - Singapore

Problem Statement

Regulatory Trends

Required Actions

As technology advances and globalization deepens, industries increasingly operate across borders. However, regulatory frameworks remain fragmented, with jurisdictions applying different, and often conflicting, rules to the same technologies and industries. This lack of harmonization creates significant challenges for businesses, regulators, and consumers alike.

For businesses, conflicting regulations increase compliance costs, introduce legal uncertainties, and stifle innovation. For example, organizations may have to adapt their operations to comply with different data privacy laws, cybersecurity requirements, or AI ethics standards in each region they operate. This patchwork approach undermines operational efficiency and impedes scalability.

Harmonisation across Jurisdictions

Problem Statement

Regulatory Trends

Required Actions

Proliferation of Regional Frameworks

Regional frameworks, such as the European Union’s GDPR for data protection or the Digital Markets Act, are setting benchmarks that influence global regulatory practices. However, their adoption varies significantly across regions, creating both opportunities and friction.

Bilateral and Multilateral Agreements

Governments are increasingly entering bilateral and multilateral agreements to align regulations. For example, trade agreements often include provisions for digital trade, intellectual property, and technology standards.

Rise of Global Standard-Setting Bodies

International organizations, such as the International Telecommunication Union (ITU), OECD, and ISO, are spearheading efforts to develop global standards for emerging technologies, including AI.

Harmonisation across Jurisdictions

AI & Partners
Amsterdam - London - Singapore

Problem Statement

Regulatory Trends

Required Actions

- ✓ **Work** toward harmonizing AI regulations in key industries like finance and healthcare by aligning with global initiatives
- ✓ **Advocate** for agreements that allow AI compliance in one jurisdiction to be recognized across others,
- ✓ **Support** industry-wide efforts to create unified standards that address unique regulatory needs within specific domains.
- ✓ **Push** for mutual frameworks that enable businesses to navigate international AI regulations more efficiently and with fewer barriers.

Thank you!

AI & Partners

Amsterdam - London - Singapore

;

E-mail

contact@ai-and-partners.com

Website

https://www.ai-and-partners.com/

Disclaimer

For more information on this publication, visit https://www.ai-and-partners.com/.

About AI & Partners

'AI That You Can Trust' - Your trusted advisor for EU AI Act Compliance. Unlock the full potential of artificial intelligence while ensuring compliance with the EU AI Act by partnering with AI & Partners, a leading professional services firm. We specialise in providing comprehensive and tailored software solutions for companies subject to the EU AI Act, guiding them through the intricacies of regulatory requirements and enabling responsible and accountable AI practices. At AI & Partners, we understand the challenges and opportunities that the EU AI Act presents for organisations leveraging AI technologies. Our team of seasoned experts combines in-depth knowledge of AI systems, regulatory frameworks, and industry specific requirements to deliver strategic guidance and practical solutions that align with your business objectives.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.

Business Integrity

AI & Partners defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots professional services, regulatory interventions, and participating in industry groups such as AI Commons, we fight for fundamental rights in the artificial intelligence age.

AI & Partners' publications do not necessarily reflect the opinions of its clients, partners and/or stakeholders.