

SPOTLIGHT NOTE

**THE STATE OF AI REGULATION:
A GLOBAL OVERVIEW**

WORKING GROUP

Legal & Regulatory Watch



JANUARY 2025

TABLE OF CONTENTS

1. INTRODUCTION: THE RAPID EVOLUTION OF AI REGULATION	3
2. THE EUROPEAN UNION: A GLOBAL GAME CHANGER IN AI REGULATION	4
3. LUXEMBOURG: A PIONEER IN NATIONAL AI IMPLEMENTATION	8
4. THE UNITED KINGDOM: LIGHT-TOUCH, PRINCIPLES-BASED REGULATION.....	10
5. THE UNITED STATES: A SECTOR-SPECIFIC REGULATORY LANDSCAPE.....	12
6. LATEST INTERNATIONAL MARKET UPDATES.....	14
7. CONCLUSION: INNOVATION AND OVERSIGHT IN BALANCE	16

1. INTRODUCTION: THE RAPID EVOLUTION OF AI REGULATION

The landscape of artificial intelligence (AI) regulation is rapidly evolving, with significant developments in the European Union (EU), United States (US) and United Kingdom (UK). This note provides an overview of the diverse regulatory approaches these jurisdictions are adopting, particularly in the financial sector.

In the EU, the use of AI is regulated by the AI Act, the world's first comprehensive and cross-sectoral AI legislation¹. Meanwhile, non-binding policy guidance, such as principles, guidelines and white papers, is prevalent across common law jurisdictions such as in the UK and in the US. This note will dive deeper into these regulatory developments, exploring their implications for the financial sector and the broader AI landscape.

Disclaimer: *This note reflects information as of 11 December 2024. Subsequent changes or developments are not included.*

¹ [EU AI Act: first regulation on artificial intelligence | Topics | European Parliament.](#)

2. THE EUROPEAN UNION: A GLOBAL GAME CHANGER IN AI REGULATION

The EU produced the first comprehensive regulation for the AI industry worldwide: The AI Act (EU Regulation 2024/1689), which entered into force on 01 August 2024. It aims to ensure a high level of protection from the harmful effects of AI systems in the EU, while supporting innovation and improving the functioning of the internal market. The AI Act is part of a broader EU Digital Strategy that aims to ensure EU digital sovereignty. It is built around five pillars:

1. **Strategy for data**, with the Data Act² and Data Governance Act³;
2. **Cybersecurity**, with the Network and Information Security (NIS2) Directive⁴ and the Digital Operational Resilience Act (DORA)⁵;
3. **Digital services**, with the Digital Services Act⁶ and the Digital Market Act⁷;
4. **AI**, with the AI Act, the Product Liability Directive⁸ and a proposal for an AI Liability Directive;
5. **Digital privacy**, with the General Data Protection Regulation⁹ and a proposal for an e-Privacy Regulation.

The AI Act seeks to provide all market players with clear requirements and obligations regarding specific uses of AI. Accordingly, it sets out directly applicable rules for the placing on the market, putting into service and use of AI systems within the EU, following a risk-based approach.

The AI Act has been designed as cross-sectoral legislation, rather than being specific to the financial sector. Consequently, there is ongoing debate about whether additional specific AI regulation is necessary for the financial sector. In this context, caution must be exercised, as the financial sector in the EU is already heavily regulated. In this respect, in June 2024, the European Commission published a consultation on the use of AI in the financial sector, clarifying that the aim of the consultation was “[...] not to lead to policy work that would generate new duplicative

² [Regulation \(EU\) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation \(EU\) 2017/2394 and Directive \(EU\) 2020/1828 \(Data Act\).](#)

³ [Regulation \(EU\) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation \(EU\) 2018/1724 \(Data Governance Act\).](#)

⁴ [Directive \(EU\) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation \(EU\) No 910/2014 and Directive \(EU\) 2018/1972, and repealing Directive \(EU\) 2016/1148 \(NIS 2 Directive\).](#)

⁵ [Regulation \(EU\) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations \(EC\) No 1060/2009, \(EU\) No 648/2012, \(EU\) No 600/2014, \(EU\) No 909/2014 and \(EU\) 2016/1011.](#)

⁶ [Regulation \(EU\) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC \(Digital Services Act\).](#)

⁷ [Regulation \(EU\) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives \(EU\) 2019/1937 and \(EU\) 2020/1828 \(Digital Markets Act\).](#)

⁸ [Directive \(EU\) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC.](#)

⁹ [Regulation \(EU\) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC \(General Data Protection Regulation\).](#)

requirements in relation to the use of AI by the financial sector, or to new requirements that have the potential to stifle AI innovation”¹⁰.

Nevertheless, it must be acknowledged that the financial sector has its own sectorial characteristics that may need to be addressed. For this purpose, the market welcomes technical guidance at the international level to foster harmonization and avoid additional regulatory burdens. See Section 5 for more details on the latest international market updates on AI.

The AI Act provides a regulatory definition of AI systems and models¹¹, making it one of the first AI comprehensive AI legislations to do so. This definition is intentionally broad to ensure the AI Act remains relevant in the future by adopting a technology-neutral and uniform approach. Specifically, the AI Act defines AI systems¹², as well as General Purpose AI (GPAI) models¹³. AI systems are the tangible products introduced to the market, which, therefore, require regulation according to the AI Act’s objectives¹⁴. AI models, on the other hand, were not specifically regulated in the initial AI Act proposal of 2021. However, following the raise and widespread use of ChatGPT in 2022, the final AI Act was revisited to include specific requirements for GPAI models (such as GPT-4), while specific regulation for other types of AI models was not deemed necessary, as they are considered part of AI systems¹⁵¹⁶.

Nevertheless, due to the fast-changing nature of the technology and its low explainability, the definition of AI systems was the subject of a consultation launched by the European Commission in November 2024¹⁷, in order to collect stakeholders’ feedback and deliver targeted European Commission Guidelines on the subject.

¹⁰ [Targeted consultation on artificial intelligence in the financial sector - European Commission.](#)

¹¹ According to the Explanatory Memorandum of the AI Act, AI constitutes a “fast evolving family of technologies”, therefore the AI Act itself does not provide a general definition of AI, nor is there an international consensus on its definition. This is partly due to the complexities involved in broadly defining the matter of “intelligence”. Consequently, the AI Act emphasizes the regulation of the AI “product”, specifically the concrete technologies to be regulated, such as AI systems and models. This focus aligns with the AI Act’s objective of ensuring the proper functioning of the internal market.

¹² AI Act, Article 3(1): ‘AI system’ means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

¹³ AI Act, Article 3(63): ‘general-purpose AI model’ means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market.

¹⁴ AI Act, Article 1(1): The purpose of this Regulation is to improve the functioning of the internal market [...].

¹⁵ AI Act, Recital 97: [...] AI models are essential components of AI systems, they do not constitute AI systems on their own. AI models require the addition of further components, such as for example a user interface, to become AI systems. AI models are typically integrated into and form part of AI systems [...].

¹⁶ AI systems are the technologies with which users interact (e.g., ChatGPT, which includes the model as well as various components such as the user interface, servers, etc.). In contrast, AI models are the underlying technologies of AI systems, i.e., programs trained on datasets (e.g., the most recent, at the time of writing, GPT-4o).

¹⁷ [Commission launches consultation on AI Act prohibitions and AI system definition | Shaping Europe’s digital future.](#)

The AI Act sets a four-tiered risk-based approach, with specific rules that apply to AI systems depending on the risk category they fall into:

1. **Unacceptable risk:** AI systems considered a threat to safety, livelihood and rights of people and therefore prohibited;
2. **High risk:** AI systems that trigger a set of detailed, complex and stringent obligations;
3. **Limited risk:** AI systems with associated transparency obligations; and
4. **Minimal risk:** AI systems not falling into the above categories, without specific obligations, besides voluntary adherence to codes of conduct.

In addition to the above, the AI Act sets out specific rules that apply to GPAI models, with additional requirements if the GPAI model poses a systemic risk. These are GPAI models demonstrating particularly high-impact capabilities due to their technical strength or market reach. In such cases, the AI Act introduces benchmarks and technical tools to determine these models and imposes more stringent obligations in addition to the requirements for GPAI models.

The AI Act imposes various obligations throughout the entire value chain, from providers¹⁸, importers¹⁹ and distributors²⁰, to deployers²¹ of AI solutions within the EU. These obligations vary according to the level of risk of AI systems and/or the type of GPAI model, aiming to ensure transparency, accountability and safety throughout the value chain.

The AI Act also establishes a two-tiered governance system, where national authorities are responsible for overseeing and enforcing rules for AI systems, while the EU level is responsible for governing GPAI models.

The AI Act will apply two years after entry into force, on 2 August 2026, except for the following specific provisions:

1. The prohibitions, definitions and provisions related to AI literacy will apply 6 months after entry into force on 2 February 2025;
2. The rules on governance and the obligations for GPAI become applicable 12 months after entry into force on 2 August 2025;

¹⁸ AI Act, Article 3(3): 'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.

¹⁹ AI Act, Article 3(6) 'importer' means a natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country.

²⁰ AI Act, Article 3(7): 'distributor' means a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market.

²¹ AI Act, Article 3(4): 'deployer' means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.

The obligations for high-risk AI systems that classify as high-risk because they are embedded in regulated products, listed in Annex II (list of Union harmonisation legislation), apply 36 months after entry into force on 2 August 2027²².



Key objectives of the EU AI Act:

- Ensure safety and ethics: Protect users from harmful AI practices.
- Encourage innovation: Balancing regulatory oversight with technological progress.
- Digital sovereignty: Strengthening the EU's position in the global AI landscape.

The four-tier risk approach:

- Unacceptable risk: AI systems banned due to safety or rights concerns.
- High Risk: Stringent obligations for high-impact systems (e.g., healthcare).
- Limited Risk: Transparency obligations for lower risk applications.
- Minimal Risk: Voluntary codes of conduct for most AI systems.

²² [EU Commission Questions and Answers.](#)

3. LUXEMBOURG: A PIONEER IN NATIONAL AI IMPLEMENTATION

According to the AI Act, each Member State must establish or designate at least one notifying authority and one market surveillance authority as national competent authorities. In December 2024, the National Commission for Data Protection (CNPD) announced²³ that the Luxembourg Government approved a bill of law which implements the provisions of the AI Act and designates the competent authorities at the national level for the application of the AI Act, thus positioning Luxembourg among the first EU countries to begin the national implementation of the AI Act.

The CNPD is one of the competent authorities and will be assigned several roles, including:

1. The single point of contact and the national coordination of the competent authorities;
2. The market surveillance authority by default (supervision of high-risk AI systems as per Annex III of the AI Act, and AI systems that do not fall under the competence of sectoral authorities);
3. The authority in charge of fundamental rights with the Luxembourg Independent Audiovisual Authority and the Inspectorate of Labor and Mines;
4. The authority in charge of setting up an AI regulatory sandbox.

In the meantime, the Commission de Surveillance du Secteur Financier (CSSF), the supervisory authority for the Luxembourg financial sector, has developed an ambitious AI roadmap. An internal CSSF task force has begun identifying an initial list of pilot projects to be deployed in the first quarter of 2025. The goal is to integrate AI into critical processes to enhance performance, transparency and efficiency while improving interactions with the public and supervised entities. In this context, the CSSF has signed a strategic agreement on AI with Clarence, Luxembourg's sovereign air-gapped cloud. According to the press release, this solution is designed to meet the needs of businesses, administrations and public institutions. Clarence's technology will enable the CSSF to leverage cutting-edge technologies for its sensitive data while ensuring confidentiality, complete control and full sovereignty²⁴.

²³ [Mise en oeuvre nationale de l'« AI Act » : la CNPD désignée comme autorité compétente - Actualités - Commission nationale pour la protection des données - Luxembourg](#). (This page is available in French only).

²⁴ [The CSSF adopts Clarence to develop artificial intelligence with full sovereignty: a major breakthrough for the financial sector – CSSF](#), December 2024.



National implementation highlights:

- The CNPD has been designated as the national authority for AI oversight.
- A robust AI sandbox will encourage innovation and compliance testing.

The CSSF's AI roadmap:

- Initial pilot projects for AI integration by early 2025.
- Collaboration with Clarence, Luxembourg's sovereign air-gapped cloud.

Key insight: "Luxembourg's proactive approach positions it among the first EU nations to implement the AI Act".

Takeaway: "The EU AI Act adopts a future-proof, technology-neutral approach, ensuring it remains relevant as AI evolves".

4. THE UNITED KINGDOM: LIGHT-TOUCH, PRINCIPLES-BASED REGULATION

The UK has so far taken a light-touch regulatory approach to the AI sector, following the common law principle of only imposing regulatory obligations where necessary to address identifiable risks.

In March 2023, the UK government published the AI Regulation White Paper²⁵, setting out its proposed regulatory framework for AI. Unlike the EU AI Act, the UK government is developing a principles-based framework for existing regulators to interpret and apply within their sector-specific domains.

The UK government's roadmap for AI²⁶ fosters a national, cross-sectoral adoption (including the financial sector) and revolves around:

1. Continuing to develop a domestic policy position on AI regulation;
2. Monitoring and evaluating a plan to assess the efficacy of its regime as AI technologies change;
3. Promoting AI opportunities while also tackling AI risks; and
4. Supporting international collaboration on AI governance.

In addition, the UK Financial Conduct Authority (FCA) has issued an AI update²⁷ in April 2024, which welcomes the government's principles-based AI approach, and has committed to furthering its understanding of AI usage in the UK financial markets, through surveys in collaboration with the Bank of England.

Moreover, in October 2024, the UK Department for Science, Innovation and Technology announced the creation of the new Regulatory Innovation Office (RIO)²⁸. The RIO will work alongside various regulatory bodies in the UK to update regulations, speed up approvals and ensure a cohesive regulatory approach, thereby enabling faster and safer deployment of innovations in emerging technologies, including, but not limited to, AI.

It should be noted that the current regulatory approach to AI might change under the new Labour government, which, in its 2024 manifesto, states that it will ensure the industrial strategy supports the development of the AI sector and removes planning barriers to new data centres²⁹.

In his speech in July 2024, King Charles III also stated that the new government “will seek to establish the appropriate legislation to place requirements on those working

²⁵ [A pro-innovation approach to AI regulation - GOV.UK](#).

²⁶ [AI Roadmap - GOV.UK](#).

²⁷ FCA, [AI Update](#), April 2024.

²⁸ [Game-changing tech to reach the public faster as dedicated new unit launched to curb red tape - GOV.UK](#).

²⁹ [Kickstart economic growth – The Labour Party](#).

to develop the most powerful AI models”³⁰. His statement was backed by Baroness Jones, who, in a House of Lords debate in July 2024, confirmed that the government will “establish legislation to ensure the safe development of AI models by introducing targeted requirements on a handful of companies developing the most powerful AI systems”³¹.

Finally, it is worth mentioning the US and UK memorandum of understanding, signed at the beginning of 2024, which provides for closer ties between the UK AI Safety Institute, a research organization within the UK government’s Department for Science, Innovation and Technology and its counterpart in the US. The agencies will, among other objectives, “develop a shared approach to model evaluations, including the underpinning methodologies, infrastructures and processes” and “perform at least one joint testing exercise on a publicly accessible model”³².



Framework overview:

- Principles-based approach: Flexible interpretation by sector-specific regulators.
- Regulatory Innovation Office (RIO): Accelerating approvals for emerging technologies.

Looking ahead:

- Potential regulatory changes under the Labour government’s industrial strategy.
- Collaboration with the US on AI safety testing.

Highlight: “The UK’s agile regulatory strategy balances innovation with risk management”.

³⁰ [The King’s Speech 2024 - GOV.UK.](#)

³¹ [AI Technology Regulations - Hansard - UK Parliament.](#)

³² [Collaboration on the safety of AI: UK-US memorandum of understanding - GOV.UK.](#)

5. THE UNITED STATES: A SECTOR-SPECIFIC REGULATORY LANDSCAPE

The regulatory development around AI in the US has been slower than in the EU, with currently no comprehensive AI legislation at the federal level. The regulatory approach in the US seems rather vertical, with sector-specific rulemaking around AI, as opposed to the horizontal, cross-sectoral approach taken in the EU.

At the state level, several states have either enacted or are considering their own AI-specific laws. For instance, in May 2024, Colorado passed the Colorado AI Act³³, the first comprehensive AI legislation in the US, which will take effect in 2026. This law imposes responsibilities on both developers and users of AI.

In addition, California has recently passed several AI-related bills, included Assembly Bill 2013³⁴ on AI training data transparency, which requires developers to post on their internet website documentation the data used to train generative AI systems, and Senate Bill 896³⁵, on generative AI accountability, which requires the California Office of Emergency Services to perform a risk analysis of potential threats posed by generative AI to California's critical infrastructures.

At the federal level, a key law was issued by US President Joe Biden in October 2023: The Executive Order 14110³⁶ (EO) on the "Safe, Secure and Trustworthy Development and Use of AI". The EO tackles various sectors and focuses on federal agencies and developers of foundation models, mandates the development of federal standards, and requires developers of the most powerful AI systems to share safety test results and other critical information with the US government. The EO also calls on the Department of Commerce to issue guidance for content authentication and watermarking to label AI-generated content.

Nevertheless, with the election of Donald Trump as US President in November 2024, the new administration plans to repeal Biden's EO on AI. In late November 2024, Federal Reserve Governor Michelle Bowman acknowledged the risks posed by AI but stated that "an overly conservative regulatory approach could skew the competitive landscape by pushing activities outside of the regulated banking system or preventing the use of AI altogether". Bowman emphasized the importance of ongoing monitoring and expanding understanding of AI technology within the bank regulatory framework, without rushing to regulate³⁷.

In addition, in October 2024, the White House released the first National Security Memorandum on AI³⁸ (Memorandum). The Memorandum directs the Pentagon and

³³ [Colorado AI Act](#).

³⁴ [Bill Text - AB-2013 Generative artificial intelligence: training data transparency](#).

³⁵ [Bill Text - SB-896 Generative Artificial Intelligence Accountability Act](#).

³⁶ [Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence | The White House](#).

³⁷ [Speech by Governor Bowman on artificial intelligence in the financial system - Federal Reserve Board](#).

³⁸ [Memorandum on Advancing the United States' Leadership in Artificial Intelligence: Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence | The White House](#).

other US national security agencies to increase their adoption of AI technologies in a safe and responsible but expedited manner. The main objectives to promote these policy declarations are:

1. **Leadership in AI development:** The US must lead in creating safe, secure and trustworthy AI;
2. **Harnessing AI for national security:** The US should leverage AI capabilities with appropriate safeguards, respecting democratic values and understanding AI's limitations;
3. **International governance framework:** The US should promote a responsible international framework for AI development that upholds human rights and democratic values, collaborating with allies.

At the time of writing, the Trump administration has not yet made any specific comments on the Memorandum issued by the previous administration. However, the new administration is expected to take a different approach to AI regulation, potentially relaxing some dispositions and focusing more on AI export control and competition with China³⁹.



Federal developments:

- Executive Order 14110 on AI Safety and Transparency.
- National Security Memorandum prioritising the use of AI in defence.

State-level progress:

- Colorado's AI Act: The first comprehensive state law, effective 2026.

Note: *“The US's fragmented approach reflects its decentralised governance structure”.*

³⁹ [AI policy directions in the new Trump administration.](#)

6. LATEST INTERNATIONAL MARKET UPDATES

The Council of Europe⁴⁰ adopted in May 2024 the first-ever international legally binding international treaty in the field of AI: The Framework Convention on AI (Convention)⁴¹. According to the Council of Europe's former Secretary General, Marija Pejčinović⁴², the Convention "is a response to the need for an international legal standard supported by states in different continents which share the same values to harness the benefits of AI, while mitigating the risks". The Convention formulates fundamental principles and rules which safeguard human rights, democracy and the rule of law but, at the same time, are conducive to progress and technological innovations. It is complementary to the already existing international human rights, democracy and rule of law standards (such as the European Convention on Human Rights), and aims at filling any legal gaps that may have formed as a result of rapid technological advances in the sphere of human rights law and the protection of democracy. The Convention claims to span the entire AI life cycle, ranging from design and development to the use and decommissioning of AI systems. At the time of writing, the Convention has been signed by 11 countries, including the EU, the UK and the US.

Moreover, international organizations and associations are following a growing trend towards creating comprehensive and coordinated AI policies, to ensure the safe and effective use of AI in the financial sector.

In May 2024, the Organisation for Economic Co-operation and Development (OECD) has updated its OECD Principles on AI⁴³, initially adopted in 2019, in response to recent developments in AI technologies, notably the emergence of GPAI and generative AI. At the time of writing, 38 OECD Member countries have committed to the OECD Principles on AI (included Luxembourg, the UK, the US and the EU), as well as 8 non-Members (such as Brazil, Romania and Singapore).

Zooming in on the financial sector, in October 2024, the World Federation of Exchanges (WFE) published a paper on the opportunities and challenges surrounding AI⁴⁴. The paper reflects the industry's preference for principle and risk-based regulatory approaches, where requirements are proportional to the level of risk associated with AI applications. Additionally, government policy should support modernization by encouraging the use of advanced technologies such as AI, cloud computing and machine learning in capital markets.

⁴⁰ The [Council of Europe](#) is the continent's leading human rights organisation. It includes 46 member states, 27 of which are members of the European Union.

⁴¹ 'Conventions and agreements' of the Council of Europe are multilateral international treaties which derive their legal force from the consent of those Member States that wish to be bound by them ([Oxford Public International Law: Council of Europe \(COE\)](#)).

⁴² [Council of Europe adopts first international treaty on artificial intelligence - Portal](#).

⁴³ [OECD Legal Instruments](#).

⁴⁴ [Regulators needn't be spooked: The WFE says curtailing AI in financial markets might mean greater risks for investors | The World Federation of Exchanges](#).

In November 2024, the Financial Stability Board published a report outlining recent developments in the adoption of AI in finance and their potential implications for financial stability⁴⁵. According to the report, several AI-related vulnerabilities stand out for their potential to increase systemic risk. These include (i) third-party dependencies and service provider concentration; (ii) market correlations; (iii) cyber risks; and (iv) model risk, data quality and governance. The report notes that existing regulatory and supervisory frameworks address many of the vulnerabilities associated with AI adoption.



Global milestones:

- Council of Europe Framework Convention on AI: A legally binding treaty safeguarding human rights in AI.
- OECD Principles on AI: Updated to address generative AI advancements.

Sectoral focus:

- Financial Stability Board highlights AI-related systemic risks.
- World Federation of Exchanges advocates for risk-based regulatory approaches.

Insight: “Global cooperation is key to harmonizing AI governance and mitigating risks”.

⁴⁵ [The Financial Stability Implications of Artificial Intelligence - Financial Stability Board.](#)

7. CONCLUSION: INNOVATION AND OVERSIGHT IN BALANCE

Despite differences in regulatory approaches and legal systems, recent technological developments (especially the rise of generative AI and ChatGPT in 2022) have made governments and policymakers aware of the importance of discussing and providing guidance on the emerging topic of AI (refer to Figure 1 below for an overview of existing AI regulation globally). Whether the approach is progressive (like in the US and in the UK) or more comprehensive (like in the EU), the need for guidance at the international level is consistent. All these regulations could shape how technology companies build, use and sell AI technologies. However, regulators will need to balance the goal of ensuring safety and ethical standards in AI with the desire to foster innovation.

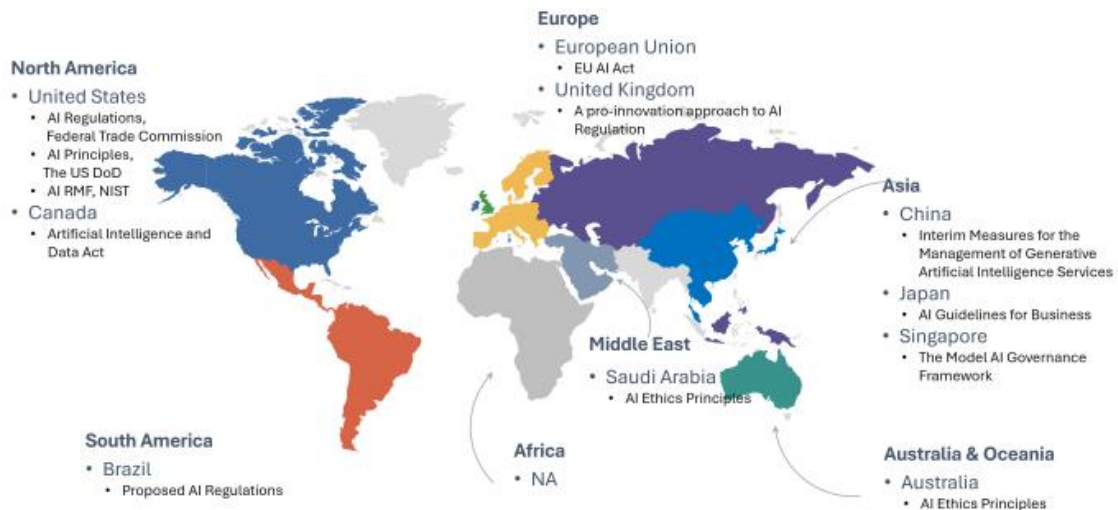


Figure 1: AI regulation globally⁴⁶.

⁴⁶ Source: Dr. Irina Steenbeek via [LinkedIn](#).



What's next?

Prepare for AI compliance challenges in 2025 and beyond.

- Promote global dialogue to harmonise regulatory standards.

“Global cooperation is key to harmonizing AI governance and mitigating risks”.

About the LuxCMA – Luxembourg Capital Markets Association

Created on 1 March 2019, the LuxCMA is a not-for-profit association (a.s.b.l.), registered at the RCSL (F12205), whose registered office is 6 rue Jean Monnet, L-2180 Luxembourg. The LuxCMA today represents memberships detailed on LuxCMA's website, which is composed by banks, law firms and services providers, amongst others.

Follow us on



Legal disclaimer: This document as well as the information contained herein (collectively the “**Publication**”) was prepared by the Luxembourg Capital Markets Association (LuxCMA).

This Publication has been prepared solely for information purposes. Although the LuxCMA has made reasonable efforts to ensure that the Publication is accurate and not misleading, the LuxCMA does not accept any responsibility or liability of any kind whether for the accuracy, reliability, or completeness of the Publication or for any action refrained or taken or results obtained from the use of this Publication. This Publication does not constitute and is not construed as any advice, recommendation, undertaking or commitment from or on behalf of the LuxCMA. This Publication shall not be substitute for the readers' own researches, investigations, verifications or consultation for professional or legal advice.

About the Legal & Regulatory Watch Working Group



The main purpose of the Legal & Regulatory Watch Working Group is to monitor legislative and regulatory developments, both at national level and on the broader European and international level.

Our work also involves interacting with entities and associations that are involved or consulted in the policy decision making and legislative process.

For more information, please visit our website at www.luxcma.com or contact info@luxcma.lu.