Global Impact: Adapting to the EU Artificial Intelligence Act

May 7, 2024

Jason Epstein, Nelson Mullins
Mallory Acheson, Nelson Mullins
Dr. Nils Rauer, MJI, Pinsent Masons
Bella Phillips, Pinsent Masons

NELSON MULLINS

Pinsent Masons

Agenda

1. What is the EU AI Act?
2. Why and to whom does the AI Act apply?
3. The AI Act Applicability Timelines
4. Two Concepts One Regulation
5. Risk Based Approach
6. General Purpose AI Models
7. Open Source
8. AI Regulatory Sandbox
9. Regulatory Bodies & Enforcement

NELSON MULLINS

Pinsent Masons

What is the EU AI Act?

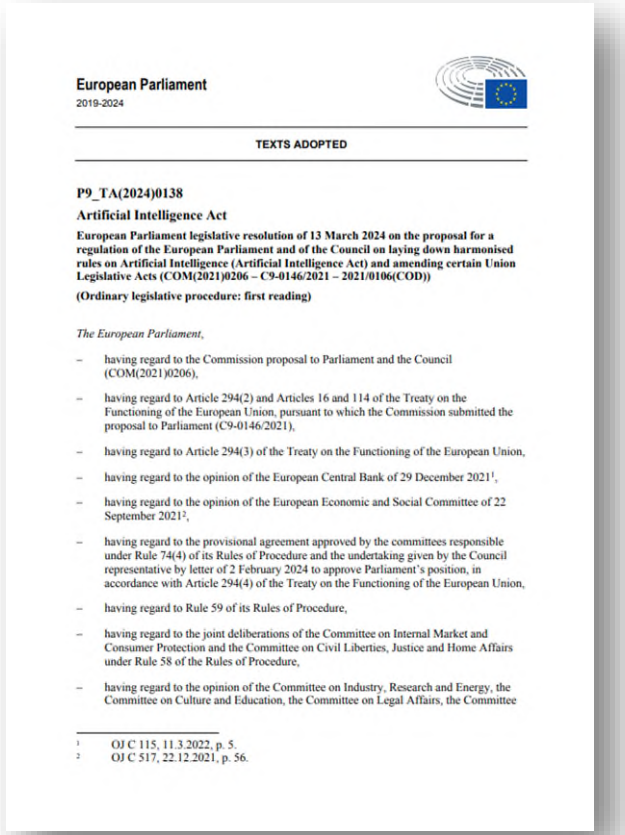
Perspective

China	United States	United Kingdom	European Union
15 August 2023 Interim Measures for the Management of Generative Artificial Intelligence Services	30 October 2023 Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence	6 February 2024 A pro-innovation approach to AI regulation (principles-based, non-statutory, and cross-sector framework)	13 March 2024 Plenary vote on Artificial Intelligence Regulation by the European Parliament (enactment to follow)

What is the EU AI Act?

Purpose

"The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in the Union, in accordance with Union values, to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of fundamental rights of the European Union (the 'Charter'), […]." – **Recital 1**



European Parliament
2019-2024

TEXTS ADOPTED

P9_TA(2024)0138

Artificial Intelligence Act

European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))

(Ordinary legislative procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to Parliament and the Council (COM(2021)0206),

– having regard to Article 294(2) and Articles 16 and 114 of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C9-0146/2021),

– having regard to Article 294(3) of the Treaty on the Functioning of the European Union,

– having regard to the opinion of the European Central Bank of 29 December 2021[1],

– having regard to the opinion of the European Economic and Social Committee of 22 September 2021[2],

– having regard to the provisional agreement approved by the committees responsible under Rule 74(4) of its Rules of Procedure and the undertaking given by the Council representative by letter of 2 February 2024 to approve Parliament's position, in accordance with Article 294(4) of the Treaty on the Functioning of the European Union,

– having regard to Rule 59 of its Rules of Procedure,

– having regard to the joint deliberations of the Committee on Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs under Rule 58 of the Rules of Procedure,

– having regard to the opinion of the Committee on Industry, Research and Energy, the Committee on Culture and Education, the Committee on Legal Affairs, the Committee

[1] OJ C 115, 11.3.2022, p. 5.
[2] OJ C 517, 22.12.2021, p. 56.

Development

Marketing

Service

Use

Health

Safety

Fundamental Rights

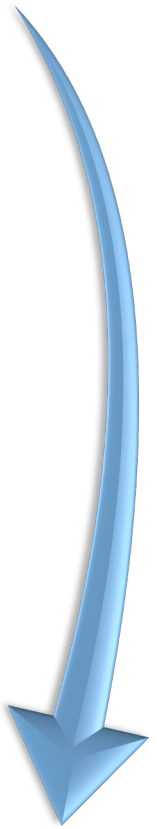
NELSON MULLINS

Pinsent Masons

What is the EU AI Act?

Legislative Process

- Proposal published by the EU Commission on 21 April 2021, COM(2021) 206 final
- Intensive negotiations throughout the years 2021/22
- Trilogue between Commission, Parliament and Council in 2023
- Political agreement reached on 9 December 2023
- Final text "leaked" on 17 January 2024
- Committee of Permanent Representatives of Member States agrees on final wording on 2 February 2024
- Majority of parliamentary committees IMCO and LIBE vote in favour of proposed language on 13 February 2024
- Plenary vote of the European Parliament on 13 March 2024
- On 19 April 2024, the corrigendum of the EU Artificial Intelligence Act was released. This document corrects and clarifies language in the act and is required before it can fully come into effect. Further substantive changes from this text are not expected.



NELSON MULLINS

Pinsent Masons

Why and to whom does the AI Act apply?

Effects on the U.S. – Scope

The AI Act is broad in scope, similar to GDPR. Similar to GDPR, we may see future guidance on interpretation and narrowing the scope.

- Provider placing on the market or putting into service AI systems/GPAI **in the EU**
- Deployer with place of establishment or located **within the EU**
- Provider or deployer in a 3rd country where output of AI system is **used in the EU**
- Importers and distributors of AI systems
- Product manufacturers placing on the market or putting into service AI systems **in the EU**
- Authorized representatives of non-EU providers
- Affected persons **in the EU**

Why and to whom does the AI Act apply?

Effects on the U.S. –Scope

- US companies need to comply with its standards if they meet the requirements of the AI Act.
- The EU AI Act is inspiring similar regulations in the US, promoting a more cautious approach to AI development.
  - Just like the GDPR impacted state laws, the EU AI Act will likely impact AI regulation in the United States (future slides: e.g., Colorado, Connecticut, Biden's Executive Order, State and Regulatory Executive Orders).
- The EU AI Act may create an increased focus on ethical considerations in AI design and deployment.

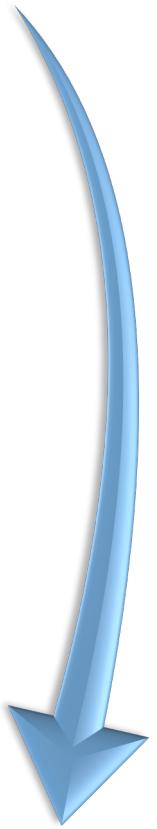
NELSON MULLINS

Pinsent Masons

The AI Act Applicability Timelines

Legislative Process

- Following its adoption by the European Parliament and the Council, the AI Act shall enter into force on the twentieth day following that of its publication in the official Journal. It will be fully applicable 24 months after entry into force, with a graduated approach as follows:
  - **6 months** after entry into force, Member States shall **phase out prohibited systems**;
  - **12 months**: obligations for **general purpose AI governance** become applicable;
  - **24 months**: all rules of the AI Act become applicable including obligations for **high-risk systems** defined in **Annex III** (list of high-risk use cases);
  - **36 months**: obligations for high-risk systems defined in **Annex I** (list of Union harmonization legislation) apply.

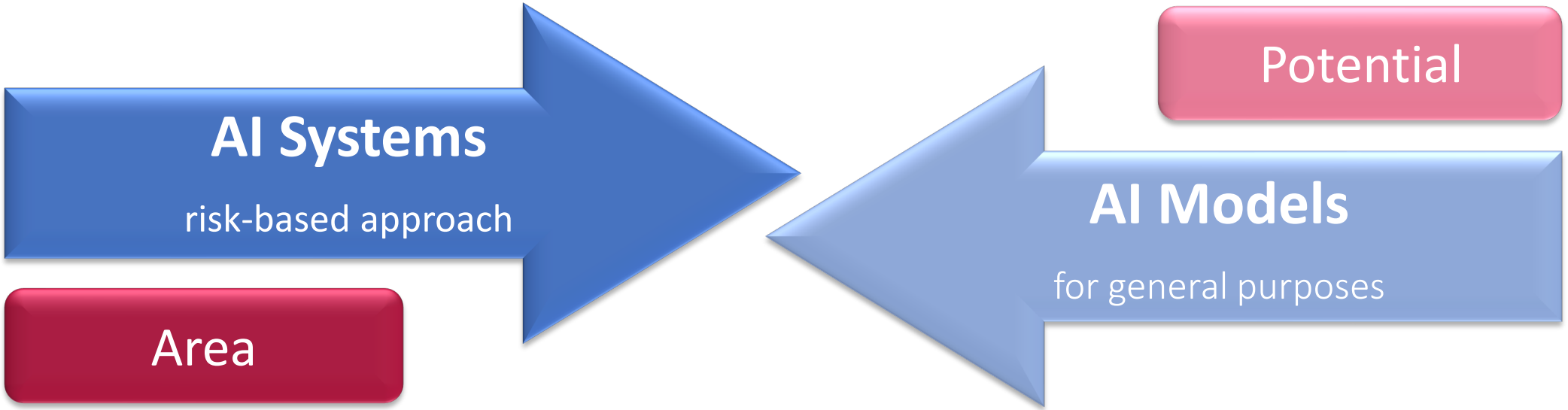


NELSON MULLINS

Pinsent Masons

Two concepts in One Regulation

Risk-based Categories and General-purpose Models



- **Starting Point** – Risk-based approach: Prohibition to gentle regulation
- **Core Criteria** – (1) safety component (**Annex I**) or (2) use in sensitive areas (**Annex III**)
- **Why second layer?** – "**ChatGPT hype**" – the power of large language models recognised
- **How to combine?** – (1) core criteria to be checked, then (2) GPAI test to be applied and systemic risk to be verified

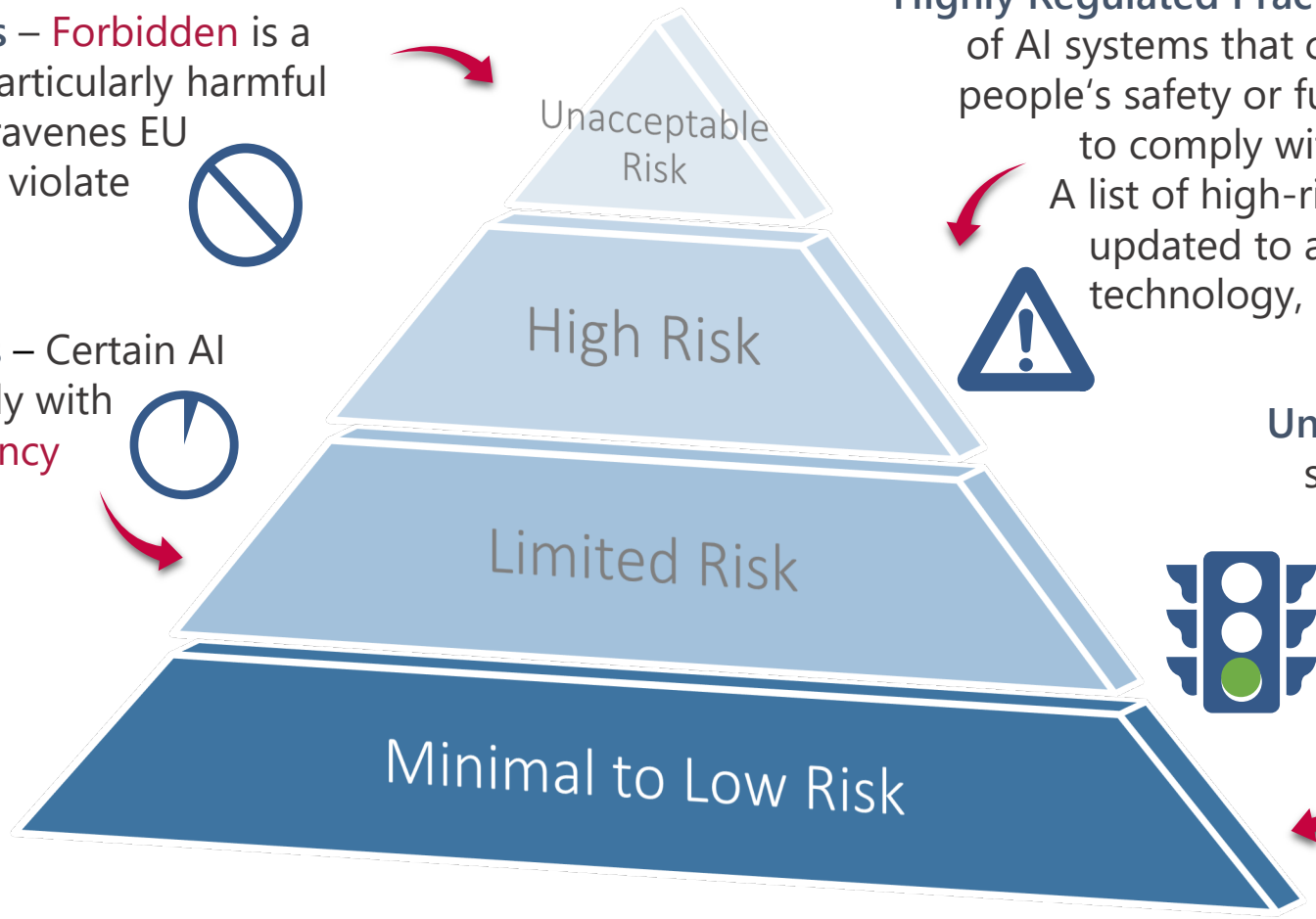
NELSON MULLINS Pinsent Masons

Two concepts in One Regulation

Risk-based Categories and General-purpose Models

Prohibited Practices – Forbidden is a very limited set of particularly harmful uses of AI that contravenes EU values because they violate fundamental rights.

Regulated Practices – Certain AI systems must comply with dedicated transparency requirements, e.g. to make clear the content is AI-generated.



Highly Regulated Practices – A limited number of AI systems that create adverse effects on people's safety or fundamental rights needs to comply with strict regulatory rules. A list of high-risk systems, meant to be updated to adapt to the evolution of technology, is annexed to the AI Act.

Unregulated Practices – AI systems not falling in the above categories can be developed and used subject to existing legislation. However, providers may choose to adhere to voluntary codes of conduct.

AI Systems

risk-based approach

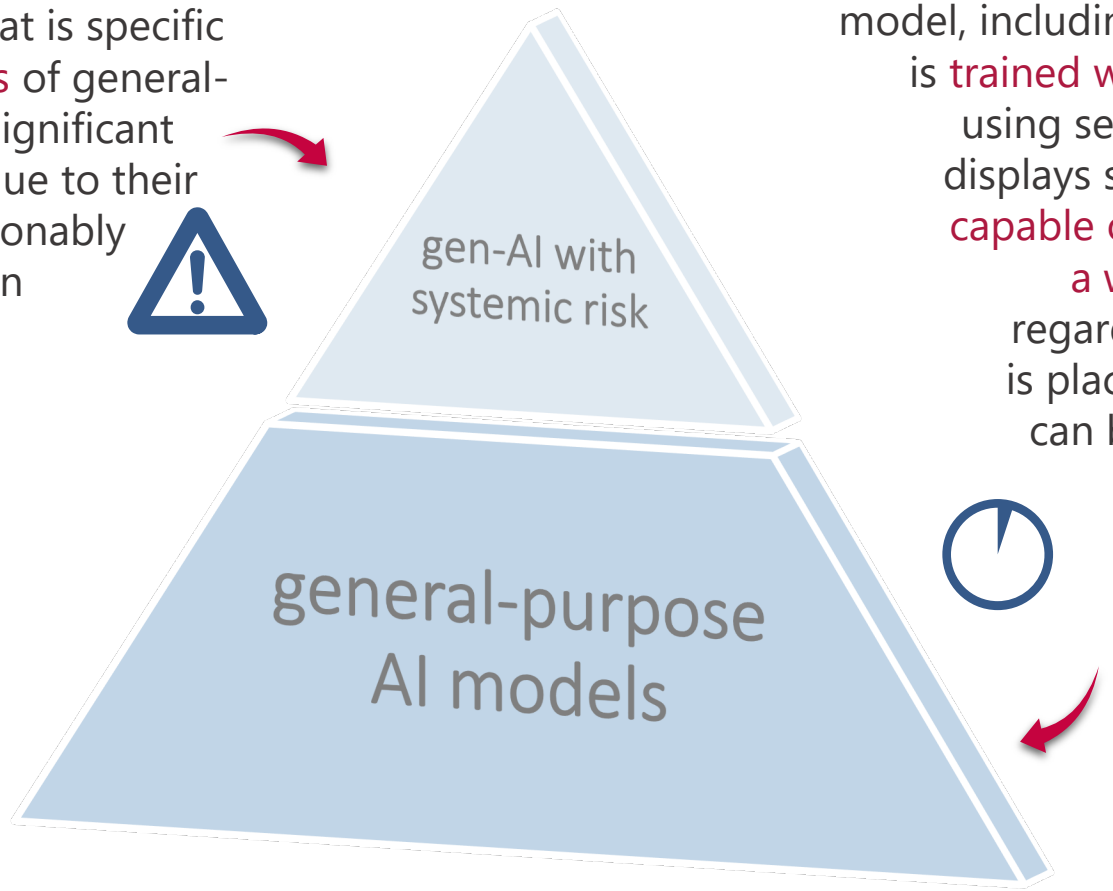
NELSON MULLINS

Pinsent Masons

Two concepts in One Regulation

Risk-based Categories and General-purpose Models

'systemic risk' means a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain; see criteria set out in Annex XIII



'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 released on the market

AI Models

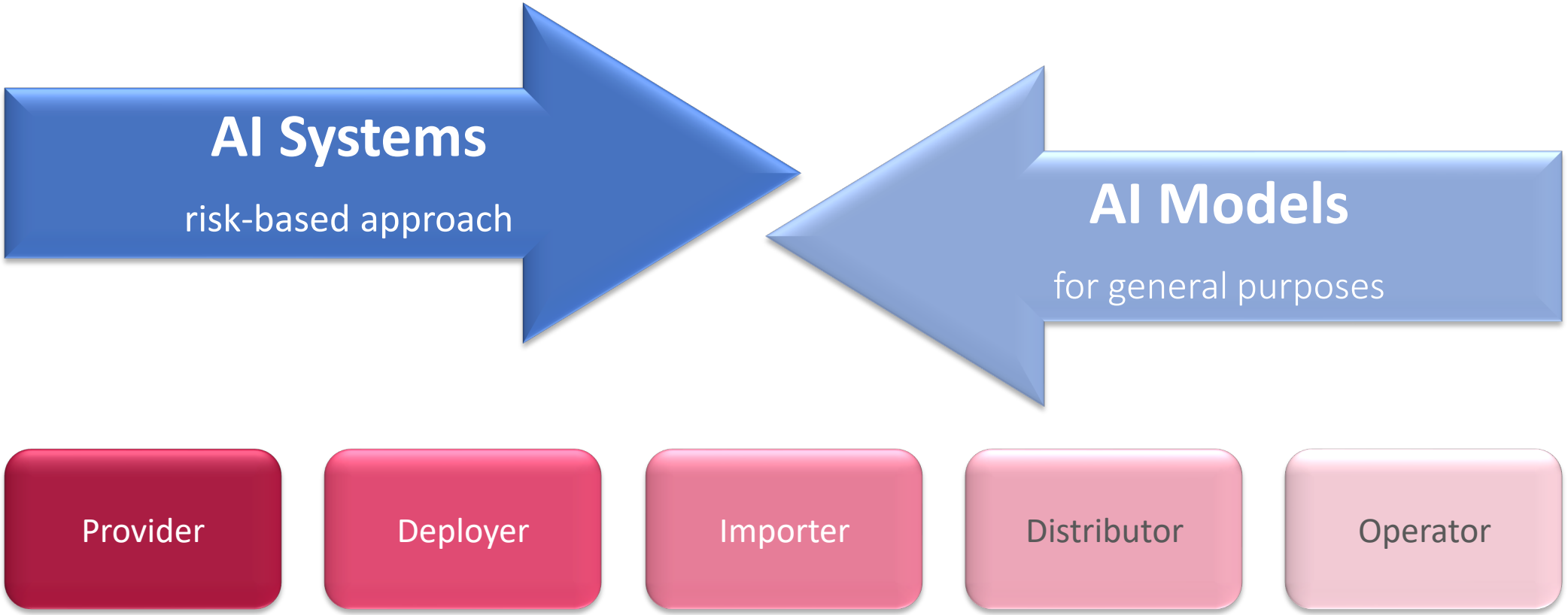
with general purpose

NELSON MULLINS

Pinsent Masons

Two concepts in One Regulation

Risk-based Categories and General-purpose Models



Prohibited AI

- **Social credit scoring** systems
- **Emotion recognition** systems at work and in education
- AI used to **exploit people's vulnerabilities** (e.g., children, the elderly, persons with disabilities)
- **Behavioral manipulation** and circumvention of free will
- **Untargeted scraping of facial images** for facial recognition
- **Biometric categorization systems** used to infer sensitive data, such as race, religion, or sexual orientation
- Specific **predictive policing** applications
- **Law enforcement use of real-time biometric identification in public** (except in limited, preauthorized situations)

High-Risk AI - Explicitly Defined in the AI Act

- Certain **critical infrastructures** for instance in the fields of road traffic and the supply of water, gas, heating and electricity;
- **Education** and vocational training, e.g. to evaluate learning outcomes and steer the learning process and monitoring of cheating;
- **Employment**, workers management and access to self-employment, e.g. to place targeted job advertisements, to analyze and filter job applications, and to evaluate candidates;
- Access to **essential private and public services** and benefits (e.g. healthcare), creditworthiness evaluation of natural persons, and risk assessment and pricing in relation to life and health insurance;
- Certain systems used in the fields of **law enforcement**, **border control**, administration of justice and democratic processes;
- Evaluation and classification of **emergency calls**;
- **Biometric identification**, categorization and emotion recognition systems (outside the prohibited categories) but this shall not include AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be.

NELSON MULLINS Pinsent Masons

High-Risk AI - Analysis

- **The EU AI Act defines high-risk AI based on potential for harm.** Here's how we assess risk:
  - **Intended Use & Impact:** What is the AI designed to do? How widespread will its use be?
  - **Data Dependence:** What type and amount of data does it use? Does it involve sensitive personal data?
  - **Autonomy & Control:** Can the AI make decisions independently? Can humans override harmful outputs?
  - **Harm Assessment:** Has the AI caused harm (health, safety, rights) already? What's the potential for future harm (severity, affected groups, fairness)?
  - **Human Dependence & Vulnerability:** How reliant are people on the AI's output? Can they opt-out? Are impacted individuals vulnerable or is there an imbalance of power?
  - **Reversibility & Solutions:** Can AI mistakes be easily corrected? Are there technical solutions to mitigate risk?
  - **Balancing Benefits & Risks:** What are the potential benefits of the AI? Do existing safeguards adequately prevent or address potential harm?

NELSON MULLINS Pinsent Masons

High-Risk AI – Corrigendum Update

- The corrigendum clarifies that some AI systems previously thought to be high-risk are not necessarily high-risk. AI systems Shall not be considered as high risk if it does not pose a "significant risk of harm, to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making"
- These include AI systems used for:
  - Narrow procedural tasks
  - To improve previous human activity
  - Used to analyze, not replace, human review
  - Perform a preparatory task
- Does the Provider CONSIDER that the AI system poses significant risk? If not Annex III allows the Provider to register and have documentation available upon request.

- The Commission is empowered to adopt delegated acts in accordance with Article 97 to amend the list in Annex III by removing high-risk AI systems where both of the following conditions are fulfilled:

  - (a) the high-risk AI system concerned no longer poses any significant risks to fundamental rights, health or safety, taking into account the criteria listed in paragraph 2 (analysis points);

  - (b) the deletion does not decrease the overall level of protection of health, safety and fundamental rights under Union law.

NELSON MULLINS Pinsent Masons

Key Provider Requirements: High-Risk AI

- **Fundamental rights impact assessment** and **conformity assessment**
- Registration in **public EU database** for high-risk AI systems
- **Implement risk management** and **quality management** system
- **Data governance** (e.g., bias mitigation, representative training data, etc.)
- **Transparency** (e.g., Instructions for Use, technical documentation, etc.)
  - Providers must ensure that AI outputs (e.g., audio, image, video or text) are detectable as AI generated.
  - Providers must develop the AI system in a way which informs end users that they are interacting with an AI system, subject to exceptions.
- **Human oversight** (e.g., explainability, auditable logs, human-in-the-loop, etc.)
- **Accuracy, robustness and cyber security** (e.g., testing and monitoring)

NELSON MULLINS Pinsent Masons

Key Deployer Requirements: High-Risk AI

- **Human Oversight:** Deployers must assign qualified individuals to oversee the AI system, ensuring it's used according to instructions and potential risks are addressed.
- **Instructions & Use:** Follow the provider's instructions for using the AI system and ensure you have the necessary data to operate it effectively.
- **Monitoring & Adjustment:** Actively monitor the AI system's performance, identify potential issues, and make adjustments as needed to maintain accuracy, security, and fairness.
- **Fundamental Rights Impact Assessment**: must be completed by deployers that are bodies governed by public law, private entities providing public services, AI systems used to evaluate credit worthiness/scores or risk assessment/pricing for health and life insurance.
- **Transparency:** Provide clear information to users about the AI system's capabilities and limitations, especially for high-risk systems with significant impact.
    - Deployers must inform individuals about the use of the AI system (exception: AI systems used to detect, prevent or investigate criminal offences, subject to appropriate safeguards.)
    - Deployers must disclose that 'deep fake' content (i.e., image, audio, video) is AI generated . Limited exceptions apply.
    - Deployers must disclose that AI generated text, on matters of public interest, is AI generated, unless there is human review.
- **Data Management:** Comply with relevant data privacy regulations regarding the data used by the AI system. This includes minimizing bias and ensuring data security.
- **Risk Management:** Implement measures to mitigate potential risks identified during the risk assessment process. This may involve technical safeguards, training procedures, or adjustments to the AI system itself.
- **Record Keeping:** Maintain records of the AI system's performance, including incidents and corrective actions taken. This is crucial for demonstrating compliance and ensuring accountability.

NELSON MULLINS Pinsent Masons

Key Requirements: High-Risk AI

- Any distributor, importer, deployer or other third-party shall be considered a provider of a high-risk AI system in the following circumstances:
  - **Rebranding** - If you place your name or trademark on a pre-existing high-risk AI system.
  - **Modification** - If you make substantial modifications to a high-risk AI system.
  - **Purpose Change** - If you change the intended purpose of an AI system in a way that makes it high-risk
- Distributors and importers of high-risk AI systems must verify that a high-risk AI system comply with the AI Act's requirements.

Limited-Risk AI

- **Compliance** with transparency obligations
- Obligation to **inform** natural persons that they are interacting with an AI system
- Required **disclosure** that content has been generated by an artificial intelligence.
- Development of **voluntary codes of conduct**.

general-purpose AI Models

with systemic risks

- **Article 51** – systemic risks
  - high impact capabilities;
  - capabilities or impact equivalent to criteria set out in Annex XIII
  - high impact capabilities presumed, when the cumulative amount of computation used for its training measured in floating point operations is greater than 10^{25}
- **Annex XIII** – Criteria for systemic risks being involved

a) the **number of parameters** of the model;

b) the quality or size of the **data set**, for example measured through tokens;

c) the **amount of computation** used for training the model, measured in floating point operations or indicated by a combination of other variables such as estimated cost of training, estimated time required for the training, or estimated energy consumption for the training;

d) the **input and output mod**alities of the model, such as text to text (large language models), text to image, multi-modality, and the state of the art thresholds for determining high-impact capabilities for each modality, and the specific type of inputs and outputs (e.g. biological sequences);

e) the benchmarks and evaluations of capabilities of the model, including considering the **number of tasks** without additional training, adaptability to learn new, distinct tasks, its level of autonomy and scalability, the tools it has access to;

f) whether it has a high impact on the internal market due to its reach, which shall be presumed when it has been made available to at least **10,000 registered business users** established in the Union;

g) the **number of registered end-users**

NELSON MULLINS

Pinsent Masons

general-purpose AI Models

with systemic risks

- **Article 52** – notification obligation
  - within two weeks after that requirement is met or it becomes known that it will be met
- **Article 53** – obligations for all GPAI providers
  - Technical documentation, including training and testing process
  - AI policy ensuring compliance notably with applicable IP law
  - Summary of training sets
  - Compliance with codes of practice (see Article 56)
- **Article 54** – authorised representatives
- **Article 55** – obligations for GPAI providers offering models with systemic risks
  - Evaluation schemes
  - Assessing and mitigating of possible systemic risks
  - Recording relevant information about serious incidents and possible corrective measures to address them
  - Ensuring an adequate level of cybersecurity protection
  - Compliance with codes of practice (see Article 56)

Open Source – Corrigendum Updates

- Exempts certain open-source AI models used for research and development from some regulations; however open-source models put into service may still be subject to the AI Act, especially if considered GPAI with system risks.
  - "Third parties making accessible to the public tools, services, processes, or AI components other than general-purpose AI models, should not be mandated to comply with requirements targeting the responsibilities along the AI value chain, in particular towards the provider that has used or integrated them, when those tools, services, processes, or AI components are made accessible under a free and open-source licence. Developers of free and open-source tools, services, processes, or AI components other than general-purpose AI models should be encouraged to implement widely adopted documentation practices, such as model cards and data sheets, as a way to accelerate information sharing along the AI value chain, allowing the promotion of trustworthy AI systems in the Union"

AI Regulatory Sandboxes

Getting to a market-ready tool

- **Article 57** – Prospective providers will, within 24 months of the entry into force of the AI Act, have access to regulatory sandboxes to facilitate the development, training, testing and validation of innovative AI systems for a limited time before their being placed on the market or put into service.
  - Set up at national level, but possibly also at regional, local or transnational level.
  - Free-of-charge access for SMEs and start-ups (but competent authorities may recover exceptional costs in a fair and proportionate manner, Art. 58(2)(d)), and SMEs established in the EU have prioritised access (Art. 62(1)(a))
  - Guidance, supervision and support to identify risks to fundamental rights, health and safety, testing, mitigation measures, and their effectiveness.
  - Written proof of the activities successfully carried out in the sandbox, as well as an exit report, which can be used as proof of compliance for the purpose of conformity assessment. (Art. 57(6)-(7))
- **Article 57 (11) -** Significant risks to health and safety and fundamental rights identified during the development and testing have to be adequately mitigated. In the impossibility of an effective mitigation, the testing will be suspended or terminated.

NELSON MULLINS

Pinsent Masons

AI Regulatory Sandboxes

Getting to a market-ready tool

- **Article 57(12) –** Prospective providers remain liable for damage to third parties resulting from experimentation in the sandbox; however, no fine will be levied against them for an infringement of the Act as long as they followed the guidance of their supervisory authority in good faith.
- **Article 58(1) –** The detailed functioning of the sandboxes (eligibility and selection, application, participation, monitoring, exit form, termination, and T&Cs) will be specified by the Commission.
- **Article 59** – As an exception to the GDPR, personal data collected for other purposes may be processed in the regulatory sandbox for training and testing if a series of strict conditions are met (AI system developed for a listed sector, monitoring mechanisms in place, siloed data, …).
- **Article 60 –** Prospective providers of high-risk AI may test their systems in **real world conditions outside regulatory sandboxes**, if they comply with a strict list of requirements (such as having a real-world testing plan approved by the responsible market surveillance authority, …) and abide by a tighter monitoring regime.

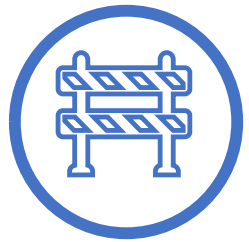
NELSON MULLINS


Pinsent Masons

Regulatory Bodies & Enforcement

Regulatory Bodies

- **Article 64** – AI Office (Commission Decision Establishing the European AI Office)
- **Article 65 –** European Artificial Intelligence Board
  - tasks set out in Article 66
  - advising and assisting the Commission and the Member States
- **Article 67 –** Advisory Forum
- **Article 68 –** Scientific Panel of independent experts
- **Article 70 –** National Notifying Authorities
- **Article 70 –** National market surveillance authorities



NELSON MULLINS Pinsent Masons

Regulatory Bodies & Enforcement

Fines

- Member States define penalties, including warnings, enforcement measures and fines. The penalties must be effective, proportionate and dissuasive.
- Maximum fine for infringement of prohibited AI practices (Art. 5): **€ 35m or 7% of worldwide turnover**, whichever is higher.
- Maximum fine for non-compliance with any of their obligations by a provider, an authorised representative, an importer, a distributor, a deployer, a notified body or transparency obligations for providers and users: **€ 15m or 3% of worldwide turnover**, whichever is higher.
- Maximum fine for the supply of incorrect, incomplete or misleading information to notified bodies or national competent authorities in reply to a request: **€ 7.5m or 1% of worldwide turnover**, whichever is higher.
- Maximum fines for EU institutions: **€ 1.5m** for an infringement of the prohibitions in Art. 5, or **€750,000** for the infringement of any other provision.
- Maximum fine for providers of GPAI models: **€ 15m or 3% of worldwide turnover**, whichever is higher.

NELSON MULLINS

Pinsent Masons

U.S. – AI Laws, Orders, & Regulations

- IAPP Global Legislation Tracker: Global AI Law and Policy Tracker (iapp.org)
- Federal Guidance
  - Biden issued Executive Order Regulating AI in US Government : Nelson Mullins - President Joe Biden's Executive Order on Artificial Intelligence
- Nelson Mullins - Recent Trends on AI Regulation by States
  - Many state's have proposed or passed Executive Orders or policy memos directing their agencies to develop policies and procedures on AI, including: Maryland, Virginia, California, Kansas, New Jersey, Oklahoma, Oregon, Wisconsin and Pennsylvania . Each EO has different requirements.
- Trends in Consumer Protection for AI
  - The new Utah Artificial Intelligence Policy Act (AIPA) was signed into law by Governor Spencer Cox and will take effect May 1. Nelson Mullins - Utah Law Makes AI Subject to Consumer Protection Laws
  - Connecticut's SB 2: "AN ACT CONCERNING ARTIFICIAL INTELLIGENCE."
  - Colorado's SB24-205: Consumer Protections for Artificial Intelligence[1]
    - This bill focuses on high-risk AI systems. Developers of high-risk AI systems are required to use reasonable care to avoid algorithmic discrimination. They must:
      - Provide information about the system to deployers.
      - Make impact assessments available.
      - Disclose risks of algorithmic discrimination.
    - Deployers of high-risk systems also have responsibilities, including implementing risk management policies and notifying consumers of consequential decisions made by the system.
    - Additionally, developers of general-purpose AI models must maintain documentation related to copyright compliance and training data.
- We are seeing an influx of required representations addressing responsible AI use with regard to bids for government contracting.

NELSON MULLINS Pinsent Masons

Questions?

NELSON MULLINS

Pinsent Masons

Today's Presenters

Jason Epstein
Partner
Nelson Mullins

T 615.664.5364
jason.epstein@nelsonmullins.com

Dr. Nils Rauer, MJI
Partner
Pinsent Masons

T +49.69.506026.012
nils.rauer@pinsentmasons.com

Mallory Acheson
Of Counsel
Nelson Mullins

T 615.664.5378
mallory.acheson@nelsonmullins.com

Bella Phillips
Associate
Pinsent Masons

T+44.113.368.7671
bella.phillips@pinsentmasons.com

NELSON MULLINS

Pinsent Masons

Additional Resources

- AI - Questions and Answers - European Commission Dec 12, 2023
- EU AI Act: "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised
  - rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts"
  - Draft with all three versions of the EU AI Act in parallel columns Jun 20, 2023
  - European Parliament Version, June 14, 2023 Jun 14, 2023
  - Artificial intelligence act, Council's General Approach Nov 25, 2022
  - Artificial intelligence act, Commission proposal Apr 21, 2022
  - Corrigendum: CO_TA (europa.eu)
- Preparing to implement the EU AI Act, IAPP/LinkedIn recording, March 19, 2024

About this Presentation

- Pinsent Masons Rechtsanwälte Steuerberater Solicitors Partnerschaft mbB is registered in the partnership register of the Munich District Court (PR 1953) with its registered office at Ottostraße 21, 80333 Munich. It has offices in Munich, Düsseldorf and Frankfurt. For a complete list of partners, see www.pinsentmasons.com. Pinsent Masons Rechtsanwälte Steuerberater Solicitors Partnerschaft mbB is the legal successor of Pinsent Masons Germany LLP (a Limited Liability Partnership (LLP) registered in England and Wales under number OC373389, which had a branch registered in the partnership register of the Munich District Court under number PR 1154 with its principal place of business at Ottostraße 21, 80333 Munich. Pinsent Masons Rechtsanwälte Steuerberater Solicitors Partnerschaft mbB is an affiliate of Pinsent Masons LLP and is authorized to use the Pinsent Masons trademark and branding. "Pinsent Masons" refers, as the context requires, the international law firm Pinsent Masons LLP and/or one or more affiliates practicing or doing business under the name "Pinsent Masons". The word "Partner", when used in connection with Pinsent Masons, refers to a member of Pinsent Masons or to an employee or consultant of equivalent status. A list of Pinsent Masons LLP members, non-members referred to as partners, and non-affiliates designated as partners is available for inspection at our offices or can be found at the following link: www.pinsentmasons.comFor a full list of jurisdictions in which we operate, please visit www.pinsentmasons.com

- Nelson Mullins provides this material for informational purposes only.
- The material provided herein is general and is not intended to be legal advice.
- Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues.
- Receipt of this material does not establish an attorney-client relationship.
- Nelson Mullins is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.

NELSON MULLINS Pinsent Masons