

The EU approach to AI regulation

Gabriele Mazzini

Architect & Lead Author AI Act

MIT Fellow

The 14th GIO Roundtable
Mandarin Oriental, Shanghai
September 20 , 2024

EU Institutional architecture/process

LEGISLATION



OpenAI ChatGPT launched on **November 30, 2022**



Call to pause AI training/research on systems more powerful than GPT-4 on **March 22, 2023**



Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence on **October 30, 2023**

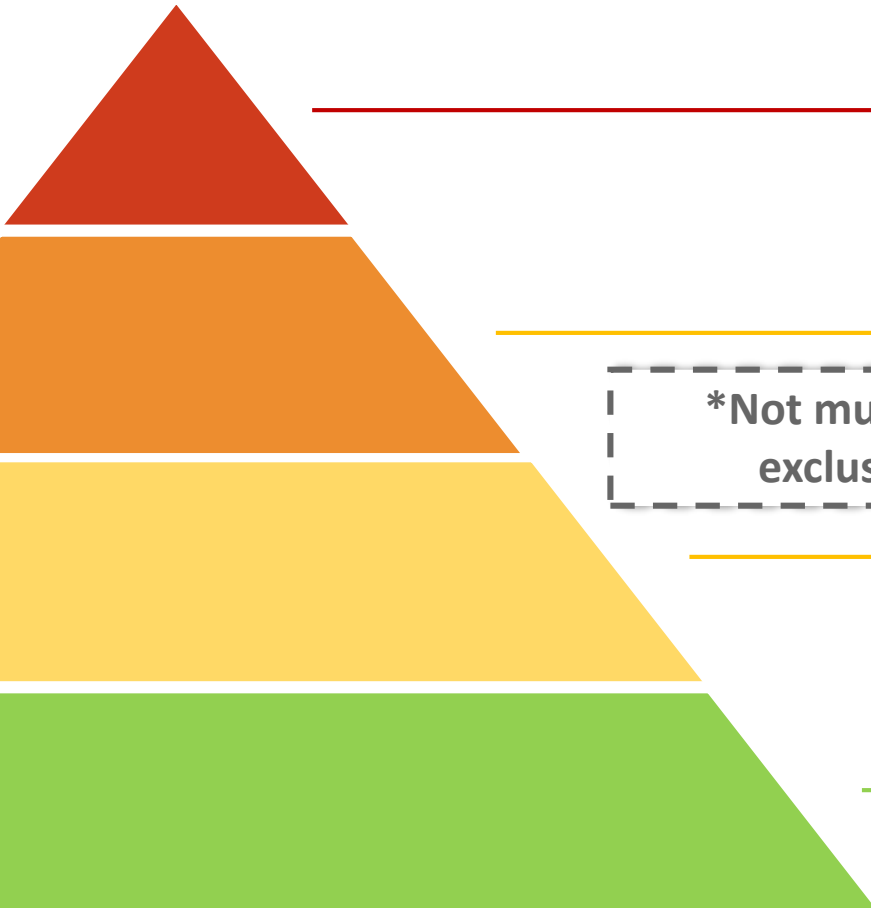
IMPLEMENTATION



The 'nature' of the AI Act

- ▶ **“Classic” internal market rules for the placing on the market and putting into service of AI systems (CE mark)**
- ▶ **Ensure high-level of protection of health & safety and fundamental rights** as legally protected interests
- ▶ **Horizontal approach**: across sectors within EU competence. No national security, military, defense.
 - ▶ Sectorial specificities/needs considered (law enforcement, finance, product legislation acquis)
 - ▶ Without prejudice to other relevant EU acquis (e.g. data protection, consumer protection, equality law, platforms legislation): *AI Act is not the only EU law applicable to AI*

Risk-based approach



The higher the risk the stricter the rules

No regulation of the technology as such

***Not mutually exclusive**

Unacceptable risk
e.g. social scoring

Prohibited

High risk
e.g. recruitment, medical devices

Permitted subject to compliance with AI requirements and ex-ante conformity assessment

'Transparency' risk
'Impersonation' (bots), deep fake

Permitted but subject to information/transparency obligations

Minimal or no risk

Permitted with no restrictions

General Purpose AI models

All GPAI (lower tier)

- Technical documentation (incl. computational resources & energy consumption)
- Information downstream
- Copyright (policy & detailed summary of content)

GPAI with systemic risks (higher tier)

- Evaluation of high-impact capabilities
 - at least 10^{25} FLOPs
 - designated by the AI Office (e.g. based on certain criteria)
- All obligations from the lower tier PLUS
 - risk assessment and mitigation
 - incident reporting
 - adequate level of cybersecurity

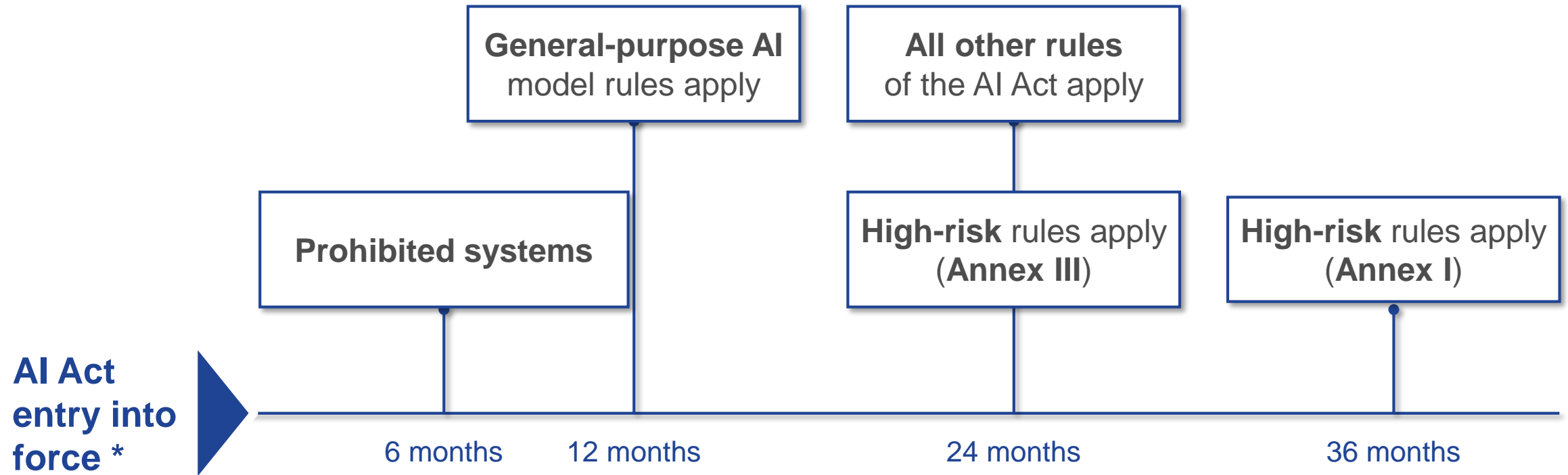
- **Open-source models** in scope, except technical documentation and transparency as regards lower tier
- **Codes of Practice** for demonstrating compliance

AI Office and implementation

Implementation of the AI Act

- enforcement of rules on GPAI (incl. developing evaluation tools/benchmarks, investigate infringements)
- support enforcement by national authorities
- support all COM responsibilities (e.g. guidance, delegated/implementing acts (*around 70 action items*), secretariat to AI Board & its subgroups, admin. support to Advisory Forum & Scientific Panel of Experts)
 - Art. 96 (shall): the application of the **requirements and obligations** referred to in Articles 8 to 15 and in Article 25; the **prohibited practices** referred to in Article 5; the practical implementation of the provisions related to **substantial modification**; the practical implementation of **transparency obligations** laid down in Article 50; detailed information on the **relationship of this Regulation with the Union harmonisation legislation listed in Annex I, as well as with other relevant Union law**, including as regards consistency in their enforcement; the application of the **definition of an AI system** as set out in Article 3, point (1).

Progressive entry into application



Thank you!

gmazzini@llm10.law.harvard.edu