

# Provisional Agreement on the Artificial Intelligence Act

*Ana Maria Correa  
Ku Leuven - CiTiP*

# Artificial Intelligence Act (AIA)

---

European Union

The image features a stylized representation of the European Union flag. The background is a vibrant blue, overlaid with expressive, white brushstroke-like patterns that create a textured, artistic effect. In the center, twelve golden-yellow five-pointed stars are arranged in a circular pattern, mimicking the flag's design. The overall aesthetic is modern and creative.

# European Union

On 8 December 2023, members of the European Parliament and Council negotiators reached a **provisional agreement** on the Artificial Intelligence Act.

At this Stage  
Dec 2023

# Scope of Application

In

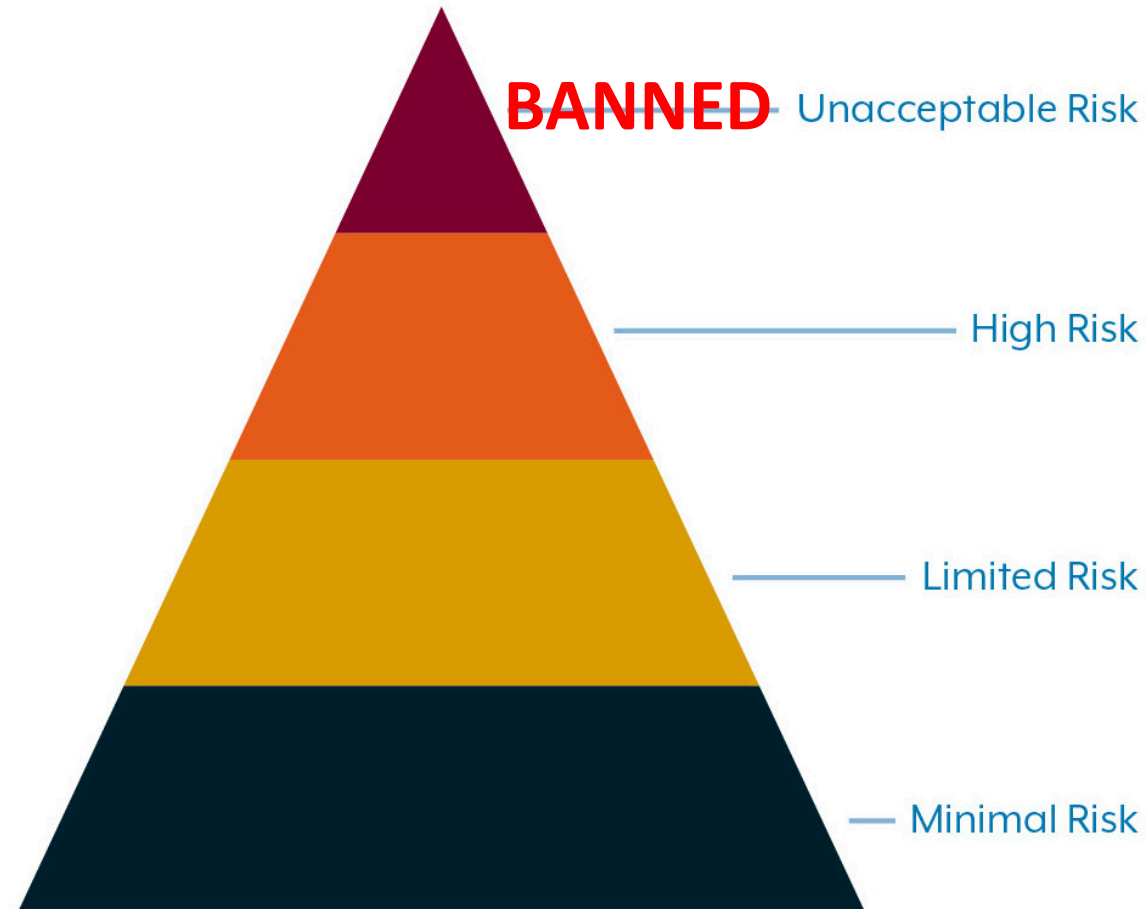
1. The AIA **will apply** to both **public and private** actors inside and outside the EU as long as the AI system is placed on the Union market or its use affects people located in the EU.
2. The act concerns both **providers** (e.g. a developer of an AI predictive systems) and **deployers of AI systems** (e.g. credit agency buying the AI predictive tool).



## Out

1. It does not apply to research, development and prototyping activities preceding the release on the market.
2. It does not apply to AI systems that are exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.

# AIA → Risk-Based Approach





---

## Banned AI



Several  
Exceptions

1. **Social Scoring** for public and private
2. **Exploitation of vulnerabilities of persons**, use of subliminal techniques
3. **Real-time remote biometric identification in publicly accessible spaces by law enforcement** (narrow exceptions allowed)
4. **Biometric categorization of natural persons** on biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs or sexual orientation, unless used to identify victims
5. **Individual predictive policing**
6. **Emotion recognition** in the **workplace** and **education institutions**, unless for medical or safety reasons (i.e. monitoring the “tiredness levels of a pilot”)
7. Untargeted scraping of **internet or CCTV for facial images to build-up or expand databases.**



# High-Risk AI (Annex III)

Certain AI systems with "significant potential harm to":

1. health,
2. safety,
3. fundamental rights,
4. environment,
5. democracy and
6. the rule of law",

# Medical Devices



# Systems to determine access to educational institutions or for recruiting people



Certain critical infrastructures - for instance -  
in the fields of water, gas and electricity







---

## High-Risk AI → Mandatory Compliance Obligations

---

1. Risk mitigation
2. Data governance
3. Documentation
4. Human oversight
5. Transparency
6. Robustness
7. Accuracy
8. Cybersecurity


*Ps. Before placing a high-risk AI system on the EU market providers must subject it to a conformity assessment.*

# Extra

High-risk AI systems that are **deployed by public authorities or entities acting on their behalf** will have to be registered in a public database, **unless those systems are used for law enforcement and migration.**

In these last cases, they will have to be registered in **a non-public** part of the database that will be only accessible to relevant supervisory authorities.





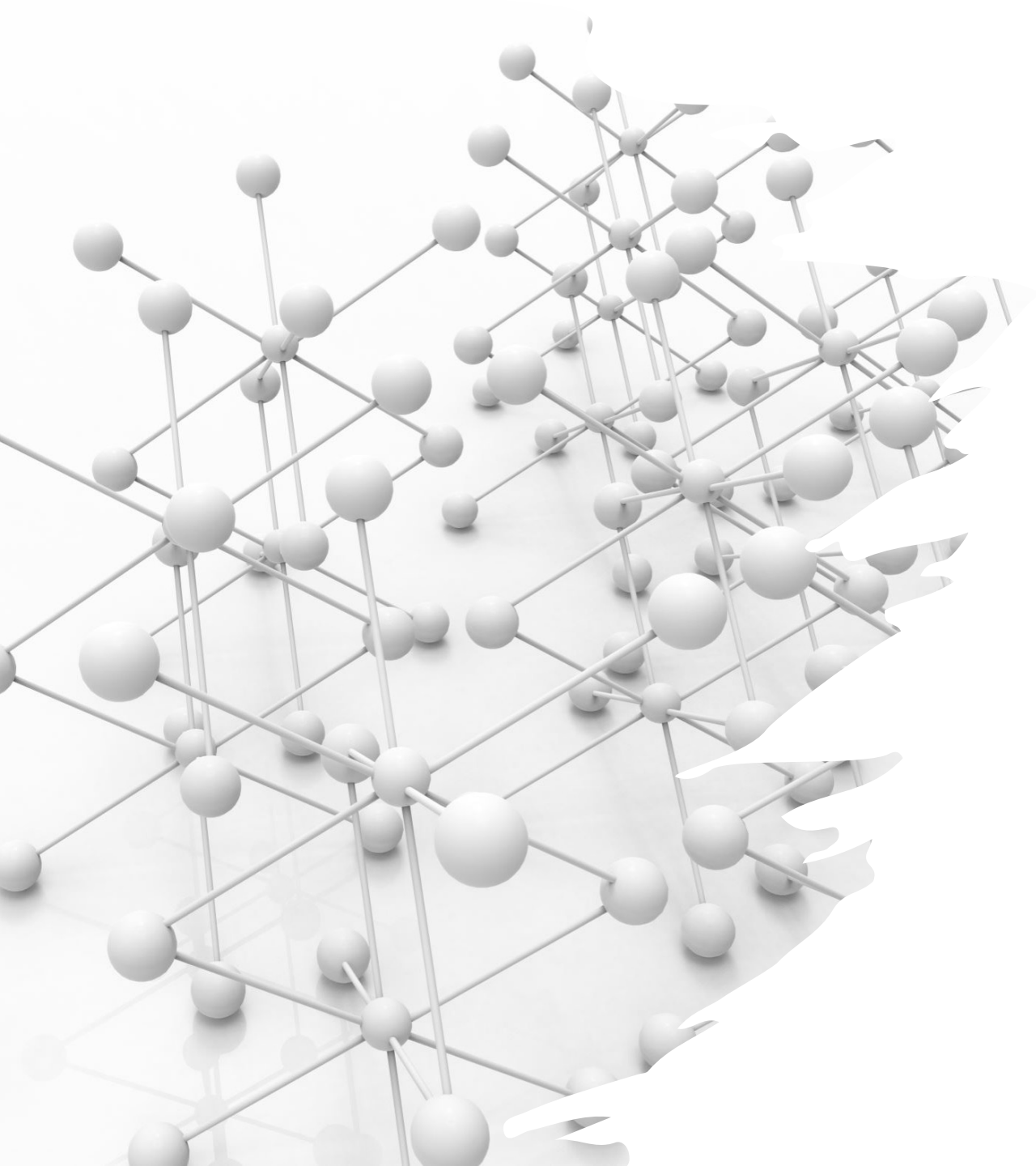
## Limited-risk AI

→ Minimal transparency obligations.

E.g. Informing users that they are interacting with an AI system.

→ E.g. limited-risks: (certain) chat bots.





# Minimal Risk

→ AI systems not falling under one of the three main risk classes, such as AI-enabled recommender systems or spam filters, are classified as minimal/no-risk.

→ The EU AI Act allows the free use of minimal-risk AI systems, while voluntary codes of conduct are encouraged.

# General Purpose AI



According to the press release:

1. Transparency requirements initially suggested.
2. GPAI models with systemic risks:  
Extra transparency requirements:  
documentation.

GPAI models that have been classified as systemic risk will be subject to more stringent obligations, which include "conduct[ing] model evaluations, assess[ing] and mitigat[ing] systemic risks, conduct[ing] adversarial testing, report[ing] to the Commission on serious incidents, ensur[ing] cybersecurity and report[ing] on their energy efficiency".

# Penalties

Fines for violations of the EU AI Act will depend on the type of AI system, size of company and severity of infringement and will range from:

- 7.5 million euros or 1.5% of a company's total worldwide annual turnover (whichever is higher) for the supply of **incorrect information**;
- 15 million euros or 3% of a company's total worldwide annual turnover (whichever is higher) for **violations** of the EU AI Act's obligations;
- 35 million euros or 7% of a company's total worldwide annual turnover (whichever is higher) **for violations of the banned AI applications**.

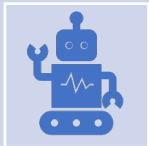
# When would the AI Act be fully applicable?



6 months: MS shall face out prohibit systems



12 months: obligations for general purpose AI become applicable



24 months: all rules of the AI act become applicable, including obligations for high-risk AI

Thank you



Ana Maria Corrêa (PhD)

CiTiP, KU Leuven.  
Belgium.

[ana.correa@kuleuven.be](mailto:ana.correa@kuleuven.be)

