



The EU AI Act and its relevance for financial services

Actuarial Association in Europe AI Webinar on 24 June

Julian Frohnecke
Legal and Policy Officer
European AI Office – DG CONNECT

General introduction to the AI Act

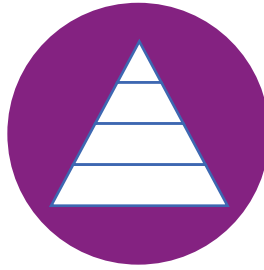
The AI Act: single EU rules for trustworthy AI



Product safety regulation: protection of health, safety and fundamental rights



Horizontal in scope covering all sectors with an integrated governance system



Proportionality with a **risk-based approach**



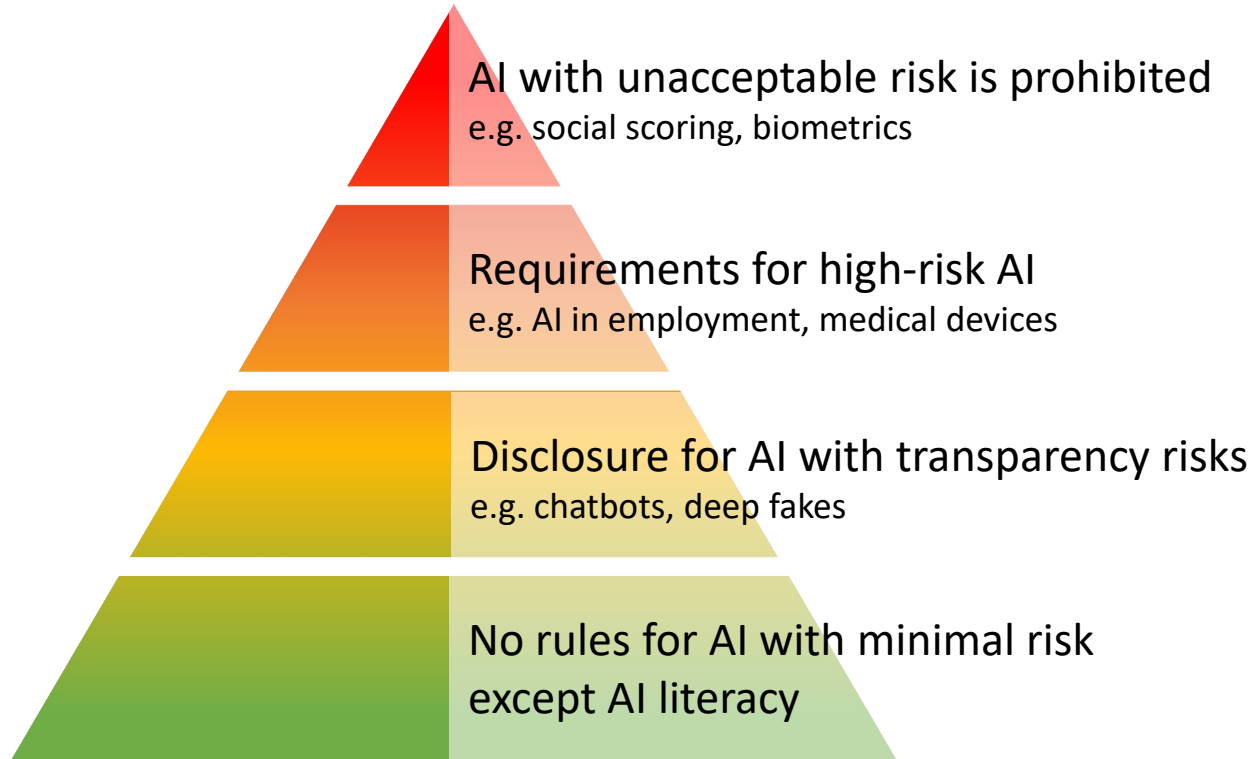
Trust along the value chain and the whole AI lifecycle



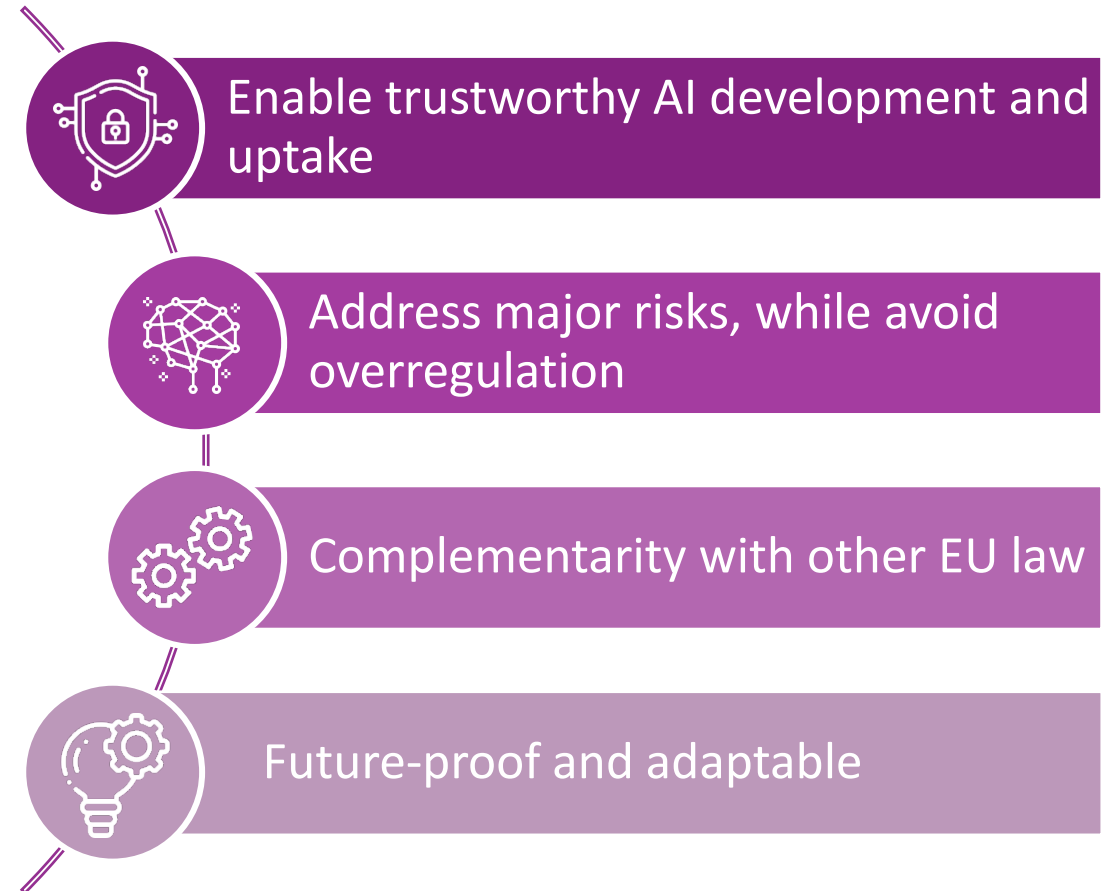
Foster responsible innovation

AI Act – risk-based rules across the AI lifecycle

Risk-based rules for AI systems:



Transparency and risk management for general purpose AI models



EUROPEAN ARTIFICIAL
INTELLIGENCE OFFICE

AI systems presenting an unacceptable risk



Prohibited since 2 February 2025!

CHAPTER II

Article 5

Prohibited AI practices

- ✗ Significantly harmful subliminal, manipulative and deceptive AI techniques
- ✗ Significantly harmful exploitation of vulnerabilities due to age,
- ✗ Social scoring leading to detrimental or unfavourable treatment
- ✗ Individual crime risk assessments solely based on profiling or assessment of personal characteristics
- ✗ Untargeted scraping of the internet
- ✗ Emotion inference in the workplace and education institutions
- ✗ Biometric categorization on sensitive characteristics
- ✗ Real-time remote biometric identification for law enforcement purposes in public spaces

The Commission published **Guidelines on prohibited AI practices** on 4 February 2025.

The Guidelines provide practical use cases and helps entities to better comply with the AI Act.



EUROPEAN ARTIFICIAL
INTELLIGENCE OFFICE

Deep-dive prohibitions:

Social scoring – Art. 5(1)(c)



Main components (cumulative)

1. AI system for the **evaluation or classification of natural persons** over a **certain period of time** based on
 - (i) their **social behaviour**; or
 - (ii) known, inferred or predicted **personal or personality characteristics**;
2. Social score leads to the **detrimental or unfavourable treatment** of persons
 - (i) in **social contexts unrelated** to those in which the data was originally collected; and/or
 - (ii) that is **unjustified or disproportionate to the behaviour**.

Example: A bank uses an AI system to determine the creditworthiness of people and to decide whether an individual should obtain a loan based on social behaviour from unrelated context e.g. internet connections and social media.

Out of scope: lawful evaluations practices in compliance with Union law (which regulates what data is related and ensures fair treatment)

Example: *Financial credit scoring systems used by banks to assess a customer's financial creditworthiness or outstanding debts, providing a credit score or determining their creditworthiness assessment, which are based on the customer's income and expenses and other financial and economic circumstances, if they are relevant for the legitimate purpose of the credit scoring and if they comply with consumer protection laws, specifying the type of data and the necessary safeguards to ensure the fair treatment of consumers in*

When is an AI system high-risk?



1

AI system is embedded into a regulated product or is itself a regulated product

Relevant product legislation is listed in Annex I of the AI Act.

Two conditions:

- AI system is intended as a safety component of a product or is itself a product
- Product in question is subject to a third party conformity assessment

2

‘Stand-alone’ AI systems intended to be used in a high-risk use case in 8 areas (Annex III) :

- Biometrics
- Critical infrastructure
- Employment
- Education
- Essential services
- Law enforcement
- Migration, asylum and border control
- Administration of justice and democratic processes



Only the concrete use cases listed for each area according to their intended purpose

„Filter“: AI systems can be excluded in four cases, if the system

- Performs a narrow procedural task
- Improves the result of a previously completed human activity
- Detects decision-making patterns or deviations and does not replace or influence a human decision or
- Performs a preparatory task

High-risk AI in the financial sector



Annex III, point 5 Access and enjoyment of essential public and private services

Two high risk use cases in the financial area:

- AI systems intended to be used to **evaluate the creditworthiness of natural persons or establish their credit score**, with the exception of AI systems used for the purpose of detecting financial fraud;
- AI systems intended to be used for **risk assessment and pricing in relation to natural persons in the case of life and health insurance**

Recital 58: AI systems provided for by Union law for the purpose of detecting fraud in the offering of financial services and for prudential purposes to calculate credit institutions' and insurances undertakings' capital requirements should not be considered as high-risk

Entities not regulated and supervised under EU financial service law (for example credit bureaus), subject to full set of rules under the AI Act

Financial institutions regulated by EU law subject to a special regime



High-risk systems allowed **subject** to requirements



Mandatory Requirements for high-risk AI system before they can be used on the EU market

Provider is responsible for EU declaration of conformity + CE marking



(Harmonized) Standards:



- Operational tools to support regulatory compliance with requirements
- Provide 'presumption of conformity'
- Ongoing work in ISO/IEC SC-42 and CEN/CENELC JTC-21. The main principle 'international first' i.e. build on IEC/ISO work as much as possible, however, as long as the international standards are aligned with the AIA Objectives and approach and cover same type of risks

Obligations for providers and deployers of high-risk AI systems



Providers



Compliance with Requirements for the AI system, operationalised through harmonised standards



Conformity assessment before placing the system on the market and **post-market monitoring** (incl. serious incident reporting)



Quality and risk management to minimize the risk for deployers and affected persons



Registration in the EU database

Deployers



Correct deployment, human oversight (incl. training and staff competence), use of **representative data**, **monitoring and incident reporting**



Possible **information obligations** vis-a-vis affected persons affected by AI supported decisions and **a right to an explanation**



Possible **fundamental rights impact assessment** (applies only to some deployers, incl. for credit-scoring and insurance risk assessment)



Public authorities also have to **register the deployment** of high-risk AI in EU database

Financial institutions regulated by EU law subject to a special regime



1. Integration of some procedural obligations into existing internal governance

processes: risk management (e.g. Art. 9(10)), technical documentation and records keeping (Art. 18(3), 19(2) and 26(5)), post market monitoring (Art. 72(4)), reporting of serious incidents (Art. 73(10))

2. Targeted derogations from certain obligations:

quality management (Art. 17(4)) and deployers' monitoring obligations (Art. 26(5))

3. Supervision under the AI Act integrated into the existing financial supervisory system:

Art. 74(6): same **national** financial supervisory authorities in so far as the placement on the market, putting into service or the use of the AI system is in direct connection with the provision of those financial services

- ▶ *Exception:* Member States may decide to designate another authority to fulfill these market surveillance tasks in justified circumstances and provided that coordination is ensured.
- ▶ National market surveillance authorities part of the Single Supervisory Mechanism to inform ECB in case they identify risks to the financial stability of relevance for the ECB tasks

AI systems presenting a limited risk – transparency requirements in Art. 50



Trust through
disclosure



When interacting with an AI:

- Humans have to be informed if they interact with an AI in case this is not obvious, e.g. interaction with a chatbot or an AI agent
- Deployers must inform individuals subjected to emotion recognition and biometric categorization systems

AI-generated content:

- AI systems that generate synthetic outputs need to include machine readable marks and be detectable
- Visible labelling of 'deep fakes' and text publications intended to inform the public on matters of public interest unless reviewed by humans

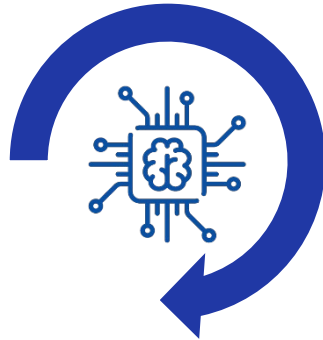


The transparency obligations do not affect the transparency obligations for high-risk AI systems and are cumulatively applicable.



EUROPEAN ARTIFICIAL
INTELLIGENCE OFFICE

Rules for general-purpose AI models



General-purpose AI models

= highly capable AI models used at the basis of AI systems such as ChatGPT

Transparency for all general-purpose AI models



Risk management for models with systemic risk

Art. 53

- Technical documentation
- Information to downstream providers
- Policy to comply with EU copyright law
- Public summary of training data

Art. 55

- Systemic risks assessment and mitigation
- Adversarial testing and model evaluation
- Incidents monitoring
- Cybersecurity protection



Code of practice developed together with stakeholders will detail out rules



EUROPEAN ARTIFICIAL
INTELLIGENCE OFFICE

The AI Act governance structure

Rules for AI systems
(i.e. prohibitions, high-risk, transparency)



Market surveillance authorities

- National authorities with procedures for EU coordination and uniform decisions in cross-border cases
- EDPS for EU institutions, bodies and agencies

Rules for general-purpose AI models



Commission Office) (AI



AI Board

with EU Member States to coordinate at EU level



Scientific Panel

supports with independent technical advice



Advisory Forum

supports with stakeholder input



EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

Introducing the European AI Office

360 degrees vision on AI:



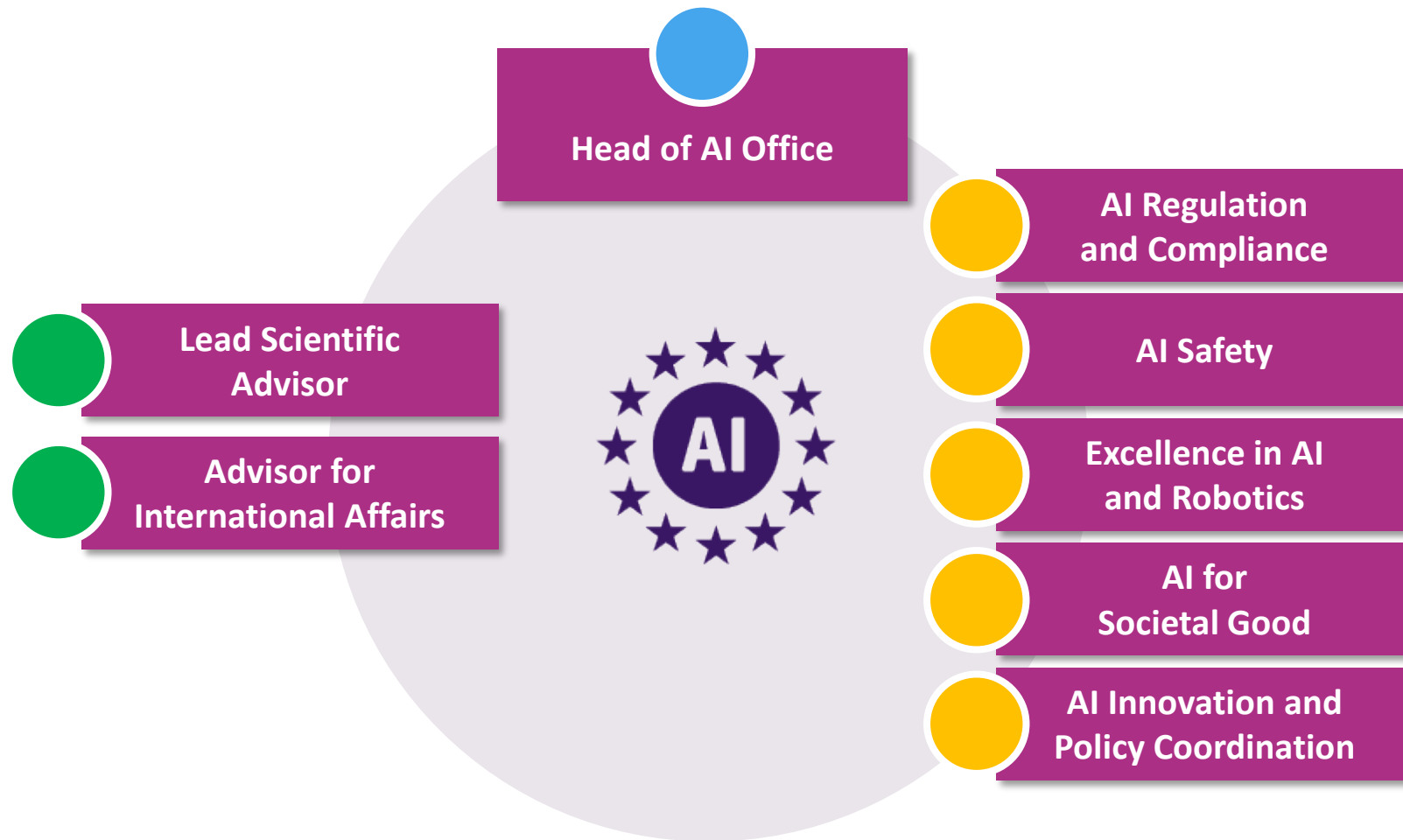
Key regulatory and coordination role in the implementation of the AI Act



Sole enforcer of the rules for general-purpose AI models



Fosters research and innovation in trustworthy AI



EUROPEAN ARTIFICIAL
INTELLIGENCE OFFICE

AI Board set-up and subgroups



AI Board

- High-level representatives & experts from Member States
- Chaired by Member States (following Council Presidency) with AI Office as a Secretariat
- Advising and steering on matters of AI policy and AI Act implementation

(key role for coordination of enforcement)

AI Board subgroups:

PHASE 1 (second half of 2024)

- Innovation ecosystem
- AI regulatory sandboxes
- Interplay with MDR and IVDR
- Prohibitions
- Standards
- Steering Group on GPAI

➤ Established and regular

PHASE 2 (first half of 2025)

- AI Act interplay with other Union legislation
- Annex III High-risk
- Law enforcement and security
- Financial services

➤ Currently being established, first meetings end of February/beginning of

PHASE 3 (second half of 2025)

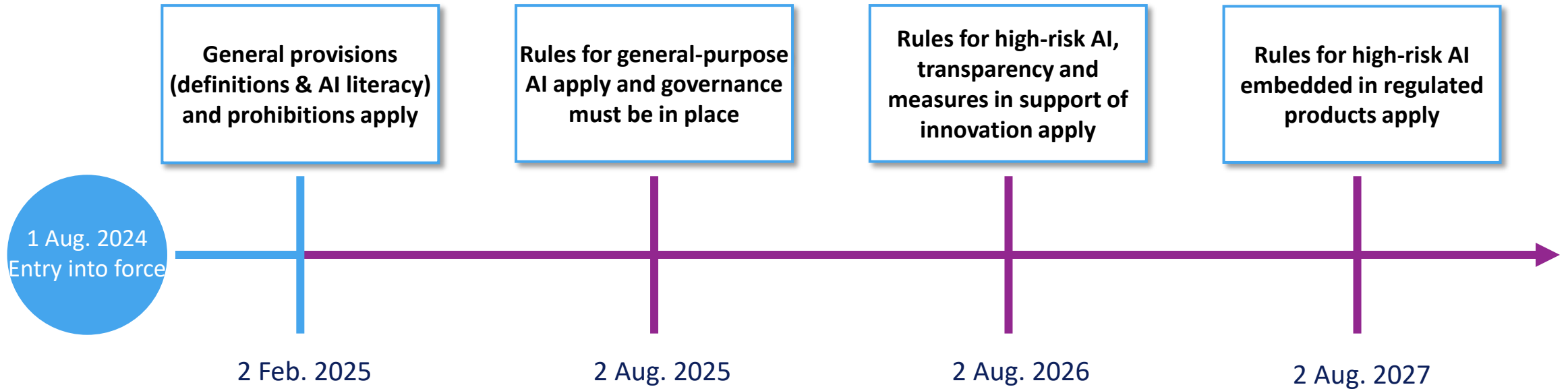
- Market surveillance authorities (AdCo)

➤ Will be established in Q3/2025



EUROPEAN ARTIFICIAL
INTELLIGENCE OFFICE

The AI Act timeline



Recent activities

Publication of a [repository of good practices for AI literacy](#).

Publication of guidelines on the [AI system definition](#) and [prohibitions](#).

Ongoing iterative drafting of [Code of practice on general-purpose AI](#).

Our [AI Pact webinars](#) for an in-depth look into the AI Act.

Explore all our activities online:



EUROPEAN ARTIFICIAL
INTELLIGENCE OFFICE

Next relevant deliverables

Report on the need to amend Article 5 prohibitions and Annex III (see Article 112)

Guidelines on the classification of high-risk AI systems (Article 6 and Annexes)

Standards for the requirements for high-risk AI systems (CEN/CENELEC)

Guidelines on requirements and obligations for high-risk AI systems, template for the fundamental right Impact assessment

Guidelines on the interplay between Union law and other relevant sectoral laws

Guidelines on the transparency obligations in Article 50 AI Act + Code of Practice on transparency of AI-generated content



EUROPEAN ARTIFICIAL
INTELLIGENCE OFFICE

Stakeholder engagement and outreach

Stakeholder outreach and support in compliance

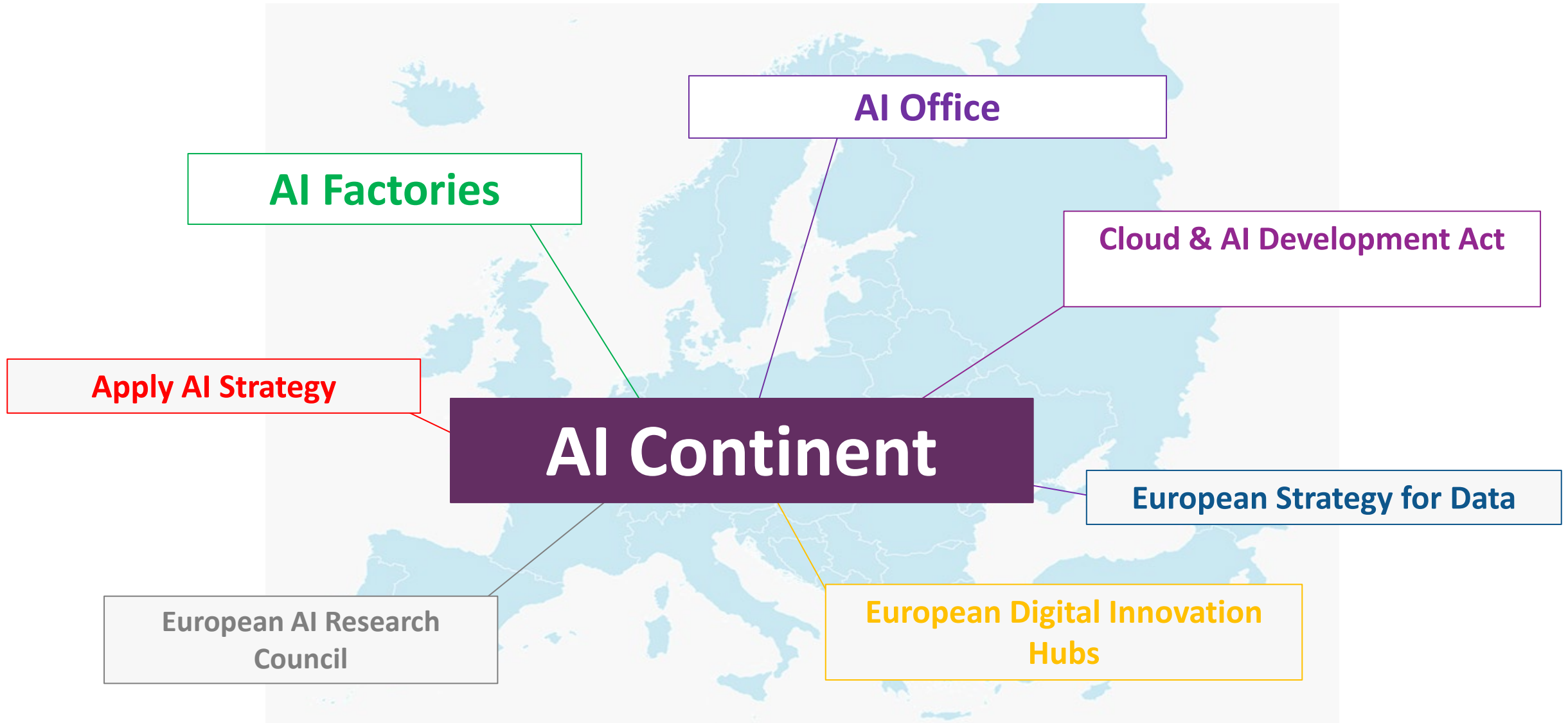
- **Public consultations**
- **AI Pact** network with more than 3000 stakeholders
- Regulatory **sandboxes**
- Support actions under **Digital Europe Programme**
- Upcoming **AI Act Service Desk**
- Upcoming set-up of the **Advisory forum** (incl. all stakeholder groups)
- Set up of the **independent scientific panel**



EUROPEAN ARTIFICIAL
INTELLIGENCE OFFICE

Questions and answers.

The AI Continent: the best place to develop trustworthy and advanced AI



Thank you!