EU AI Act

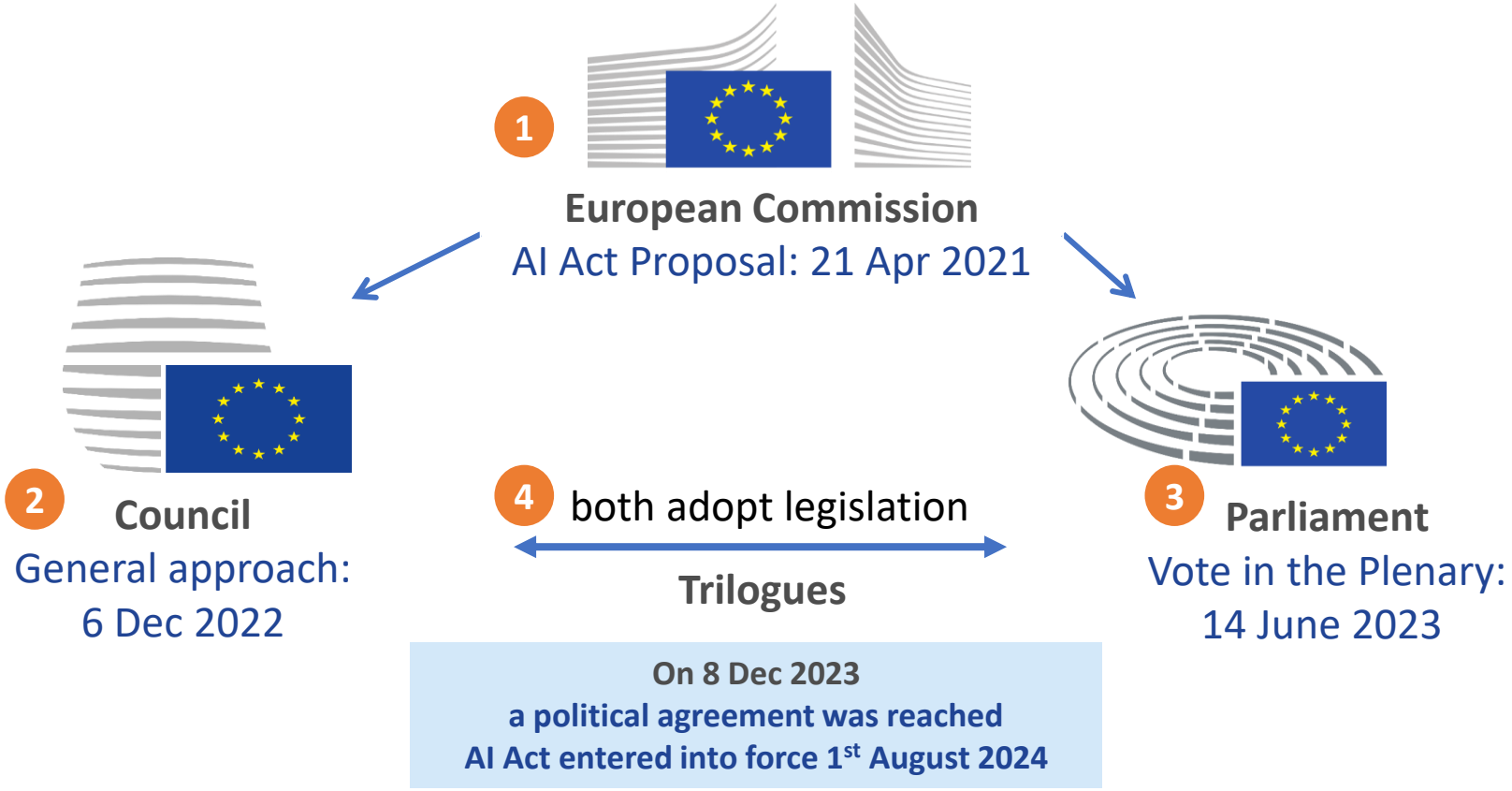
13-14 November 2024

Impact of AI on economy/finance/supervision

European Commission,
DG FISMA
Ana-Maria Fimin, 13/11/2024

European Commission

A political agreement on the EU AI Act was reached



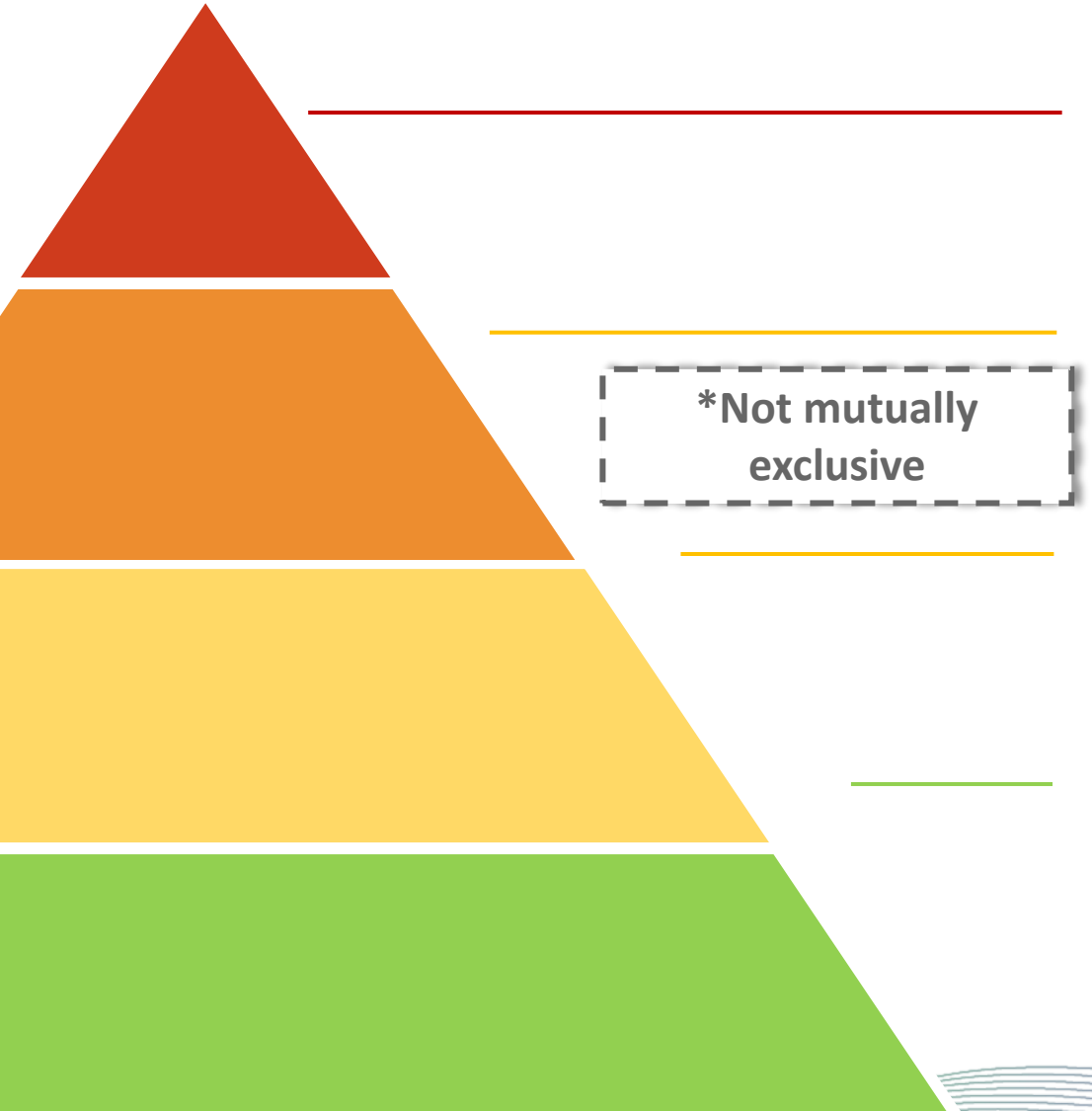
The first comprehensive legislative framework for AI in the world.
It ensures that Europeans can trust what AI has to offer.

‘

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

https://digital-strategy.ec.europa.eu/en/news/commission-launches-consultation-ai-act-prohibitions-and-ai-system-definition

The AI Act follows a risk-based approach



Unacceptable risk
e.g. social scoring, untargeted scraping

Prohibited

High risk
e.g. recruitment, medical devices

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

*Not mutually exclusive

'Transparency' risk
'Impersonation' (chatbots), deep fakes

Permitted but subject to information/transparency obligations

Minimal or no risk

Permitted with no restrictions, voluntary codes of conduct possible

European Commission

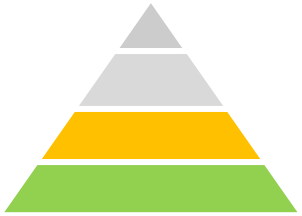
A limited set of particularly harmful AI practices are banned

Unacceptable risk

Subliminal, manipulative techniques or exploitation of vulnerabilities	to manipulate people in harmful ways
Social Scoring	for public and private purposes leading to detrimental or unfavourable treatment
Biometric categorisation	to deduce or infer race, political opinions, religious or philosophical beliefs or sexual orientation, exceptions for labelling in the area of law enforcement
Real-time remote biometric identification	In publicly accessible spaces for law enforcement purposes, -with narrow exceptions and with prior authorisation by a judicial or independent administrative authority
Individual predictive policing	assessing or predicting the risks of a natural person to commit a criminal offence based solely on this profiling without objective facts
Emotion recognition	in the workplace and education institutions, unless for medical or safety reasons
Untargeted scraping of the internet	or CCTV for facial images to build-up or expand biometric databases

Rules for AI systems which are not high-risk:

https://www.whitecase.com/insight-alert/pre-final-text-eus-ai-act-leaked-online



Transparency obligations for certain AI systems (Art. 52)

- **Notify humans** that they are **interacting with an AI system** unless this is evident
- Design **generative AI** so that synthetic audio, image, video or text content **is marked in a machine readable format and detectable as artificially generated**
- Deployers to **label as artificially generated:**
  - **deep fakes** (audio, image or video unauthentic content)
  - **text** if published with the purpose of informing the public on matters of public interest
- Notify humans that **emotion recognition or biometric categorisation systems** are applied to them

Possible voluntary codes of conduct (Art. 69)

- No mandatory obligations, but possibility for voluntary application of the AI Act requirements to non-high-risk
- Possibility for voluntary application of other requirements (e.g. environmental and social sustainability)

High-risk AI systems will have to comply with certain rules

1. High-risk systems embedded in products covered by Annex II

2. High-risk (stand-alone) use cases listed in Annex III:

- **Biometrics:** Remote biometric identification, categorization, emotion recognition;
- **Critical infrastructures**: e.g. safety components of digital infrastructure, road traffic
- **Education**: e.g. to evaluate learning outcomes, assign students in educational institutions
- **Employment:** e.g. to analyse job applications or evaluate candidates, promote or fire workers
- **Essential private and public services**: determining eligibility to essential public benefits and services; credit-scoring and creditworthiness assessment, risk assessment and pricing in health and life insurance
- **Law enforcement:**
- **Border management:**
- **Administration of justice and democratic processes**

Filter mechanism: Excludes systems from the high-risk list that:

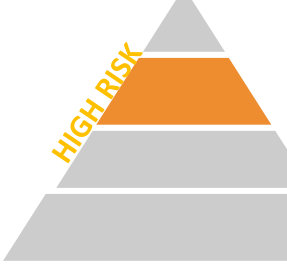
- perform narrow procedural tasks,
- improve the result of previous human activities,
- do not influence human decisions or
- do purely preparatory tasks,

NB. Profiling of natural persons always high-risk

DIGITAL COMMISSION ESSENTIALS

European Commission

Obligations of providers and deployers of high-risk AI



Provider obligations

- **Risk management system** to minimise risks for deployers and affected persons
- **Trustworthy AI requirements:** data quality and management, documentation and traceability, transparency and information to deployers, human oversight, accuracy, cybersecurity and robustness
- **Conformity assessment** to demonstrate compliance prior to placing on the market
- **Quality management system**
- **Register** standalone AI system in EU database (listed in Annex III)
- Conduct **post-market monitoring** and report **serious incidents**
- Non-EU providers to appoint **authorized representative in the EU**

Deployer obligations

- Operate high-risk AI system in accordance with **instructions of use**
- Ensure **human oversight**: persons assigned must have the necessary competence, training and authority
- **Monitor** for possible risks and **report problems and any serious incident** to the provider or distributor
- Public authorities to **register the use in the EU database**
- **Inform affected workers** and their representatives
- **Inform people** subjected to decisions taken or informed by a high risk AI system and, upon request, provide them with **an explanation**

How will it work for the financial sector?

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 37: *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

DIGITAL COMMISSION ESSENTIALS

European Commission

Financial institutions regulated by EU law subject to a special regime

- **Supervision under the AI Act integrated into the existing financial supervisory system**
  Art. 63(4): 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.
- **Integration of some procedural obligations into existing internal governance processes**: risk management (e.g. Art. 9(9)), technical documentation and records keeping (Art. 18(2), 20(2) and 29(5)), post market monitoring (Art. 61(4)), reporting of serious incidents (Art. 62(3))
- **Targeted derogations from certain obligations** : quality management (Art. 17(3)) and deployers' monitoring obligations (Art. 29(4))

The impact on fundamental rights has to be assessed

The use of a high-risk AI system may produce an impact on fundamental rights after deployement
Prior to first use, some deployers must do a **fundamental rights impact assessment for Annex III systems** (except critical infrastructure)

Consisting of an assessment of:

► **Deployers' processes**, in which the high-risk AI system is intended to be used

► **Categories of natural persons and groups** likely to be affected by its use in the specific context

► **Specific risks of harm** likely to impact the affected categories of persons or group of persons

►Description of **human oversight measures**

►Measures to be taken **in case of materialization of the risks**

Carried out by

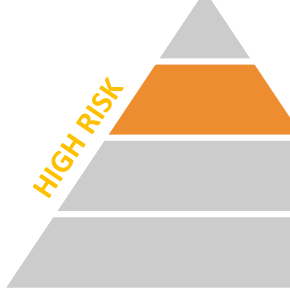
Deployers that are

1. Bodies governed by **public law**
2. Private operators providing **public services**
3. Certain other **private providers** (credit scoring/ credit worthiness assessment of health and life insurances)

DIGITAL COMMISSION ESSENTIALS

European Commission

The compliance and enforcement system



Pre-market – conformity assessment

AI that is safety component of products (regulated by product legislation)

→ **conformity assessment** (already existing under the relevant sectoral legislation)

Other high-risk AI systems ("stand-alone")

→ **Ex ante conformity assessment through internal checks ***

→ **Registration** (EU database)

Post-market

- **Market surveillance** (authorities)
- **Post-market monitoring** (providers)
- **Reporting system** for serious incidents (providers and users)
- **Re-assessment** by the provider in case of substantial changes to AI systems
- **Human oversight and monitoring** (users)

* Exception remote biometric identification

European Commission

New special rules for General Purpose AI models (GPAI)

GPAI models: trained on large data, can competently perform wide range of tasks and be integrated in numerous downstream applications; research, development, and prototyping activities preceding the placement on the market are not covered.

All GPAI
(lower tier)

- Information and documentation requirements, mainly to achieve **transparency for downstream providers**
- Policy to respect copyright and a summary of the content used for training purposes
- **Free and open-source models are exempted** from transparency requirements, when they do not carry systemic risks except from the copyright-related obligations

GPAI with systemic risks
(higher tier)

- **at least 10^25 FLOPs** or **designated by the AI Office** (e.g. based on benchmarks for capabilities, user count)
- All obligations from the lower tier **+ state-of-the-art model evaluations** (including red teaming / adversarial testing**), risk assessment and mitigation, incident reporting, cybersecurity and additional documentation**

updateable via delegated acts

- GPAI providers may rely on **Codes of Practice** to demonstrate compliance
- Codes of practice to be developed by industry under coordination of AI Office, the scientific community civil society and other experts also involved; the codes could be approved by COM through implementing act;
- New standardisation deliverable on GPAI to supersede the codes once EU harmonised standards available

A holistic governance structure for effective enforcement

Enforcement by national competent authorities and the AI Office with a supportive structure for close collaboration with Member States and for additional technical expertise

National competent authorities

- Supervising the application and implementation regarding high-risk conformity and prohibitions
- Carrying out market surveillance, EDPS for Union entities

European AI Office (established within the Commission)

- Developing Union expertise and capabilities in the field of artificial intelligence, implementation body
- Enforcing and supervising the new rules for GPAI models, incl. evaluations, requesting measures

European Artificial Intelligence Board

- High-level representatives of each MS, advising and assisting the Commission and MS

Advisory Forum

- Balanced selection of stakeholders, incl. industry, SMEs, civil society, academia
- Advising and providing technical expertise

Scientific Panel

- Pool of independent experts
- Supporting the implementation and enforcement as regards GPAI models, with access by Member States

COM decision setting up AI Act

- **Commission Decision Establishing the European AI Office**

A European Artificial Intelligence Office will be established within the Commission as part of the administrative structure of the Directorate-General for Communication Networks, Content and Technology and subject to its annual management plan.

The European Artificial Intelligence Office should exercise its tasks, in particular to issue guidance, in a way that does not duplicate activities of relevant bodies, offices and agencies of the Union under sector specific legislation.

https://digital-strategy.ec.europa.eu/en/library/commission-decision-establishing-european-ai-office

Next steps

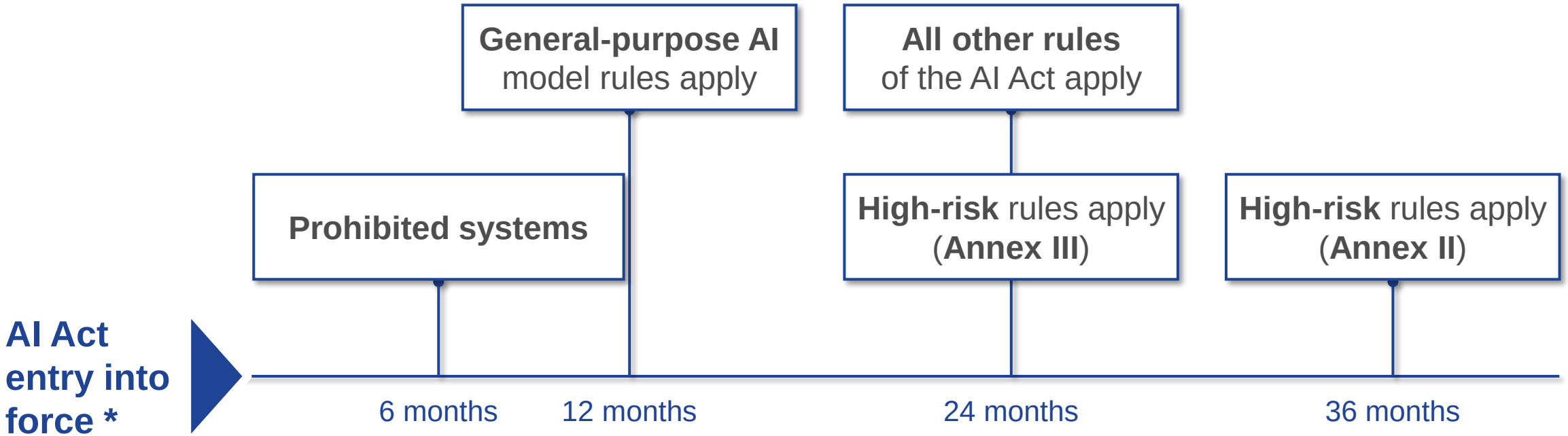
- The European Parliament and the Council as co-legislators need to endorse trilogue agreement

- Once adopted, there will be 2 years of transitional period before the **Regulation becomes directly applicable** across the EU.

- In parallel, **harmonized standards of CEN/CENELEC** should be ready and support operators in the practical implementation of the new rules& conformity assessment procedures

European Commission

The AI Act enters into application in a gradual approach



*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.

DIGITAL COMMISSION ESSENTIALS

European Commission

Thank you

Ana-maria.fimin@ec.europa.eu

European Commission