European Commission

SHAPING EUROPE'S DIGITAL FUTURE

The AI Act and its impact on the aviation sector

Antoine-Alexandre André – DG CNECT A.2 (AI Office)

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

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

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

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

- AI system shall be considered to be high-risk where both of the following conditions are fulfilled:

a) the AI system is intended to be used as a **safety component of a product, or the AI system is itself a product, covered by the Union harmonisation legislation** listed in Annex I;

b) the product whose safety component pursuant to point (a) is the AI system, or the AI system itself as a product, is **required to undergo a third-party conformity assessment**, with a view to the placing on the market or the putting into service of that product pursuant to the Union harmonisation legislation listed in Annex I.

Aviation legislation is included in the list!

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

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 II)
- 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**

New special rules for General Purpose AI models (GPAI)

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)

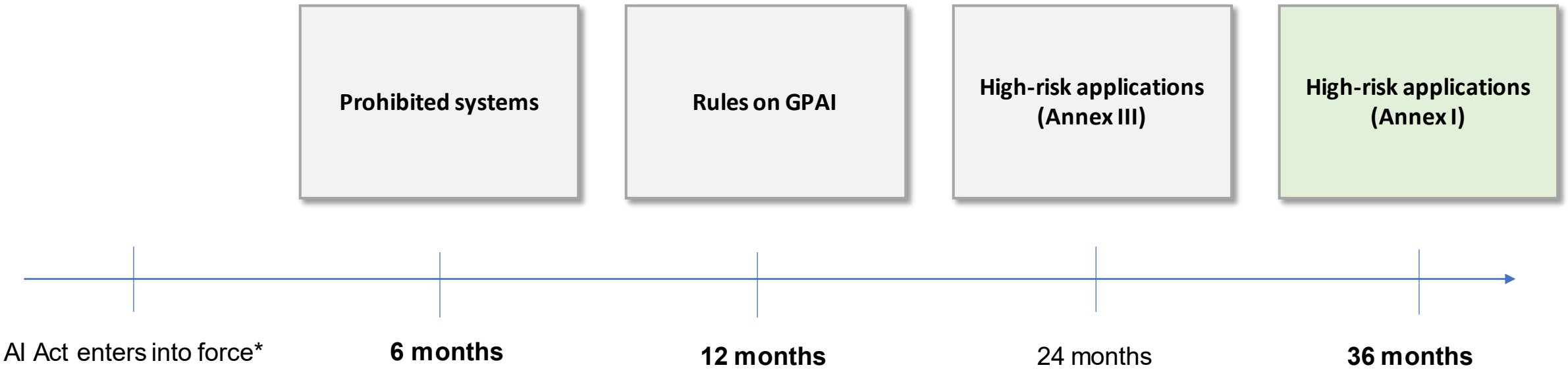
- **at least 10^25 FLOPs** or **designated by the AI Office** (e.g. based on benchmarks for capabilities, user count)
- All obligations from the lower tier **+ state-of-the-art model evaluations** (including red teaming / adversarial testing**), risk assessment and mitigation, incident reporting, cybersecurity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

updateable via delegated acts

DIGITAL COMMISSION ESSENTIALS

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

antoine-alexandre.andre@ec.europa.eu

European Commission