Navigating the EU AI Act

Seminar AI and Standards - Building a Trusted Future for Europe
14 May 2025, Stavanger

Dr. Tatjana Evas
Legal and Policy Officer
European AI Office

Fundamentals of the EU AI Act

The rationale

Complexity — **Opacity**
Unpredictability — **Safety**
Autonomy — **Data**
Fundamental rights and values

TRUST

Solid framework of EU legislation already in place at EU and national level

HOWEVER

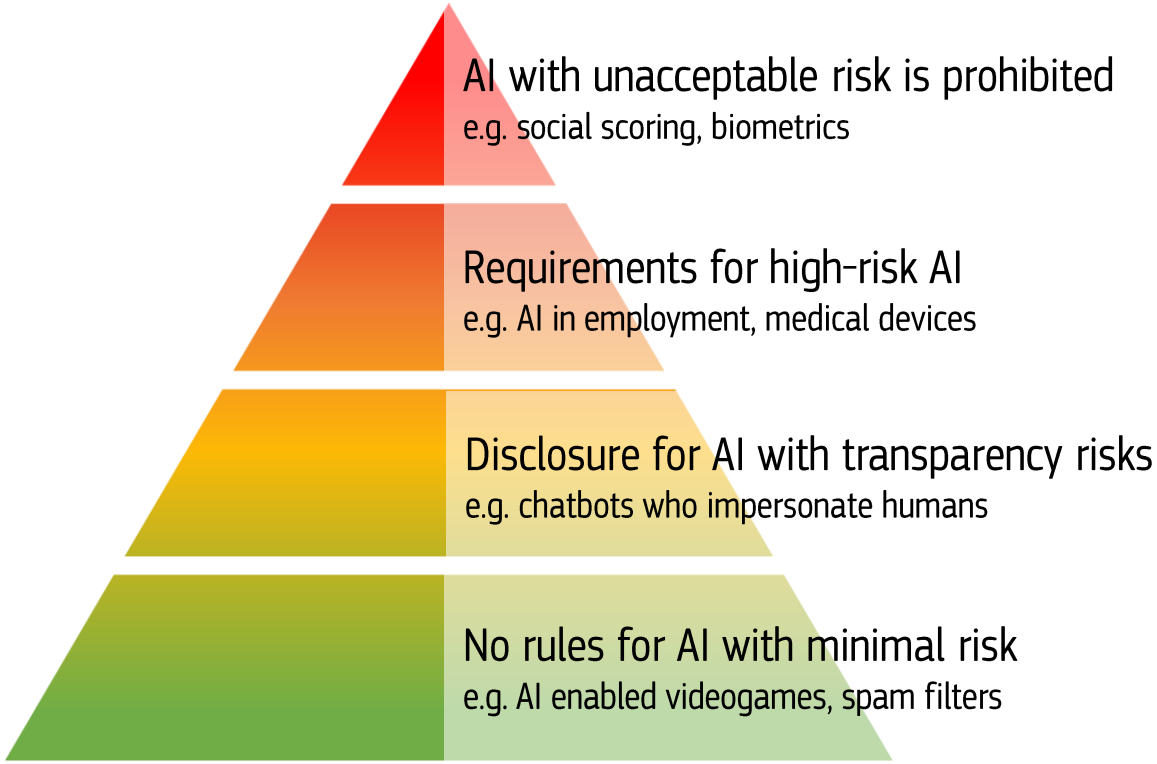
Certain **specific features of AI** can make application and enforcement of the existing rules more challenging and generate **risks to safety and fundamental rights**

Artificial Intelligence Act

A **tailored regulatory response** needed

EU AI Act – rules for trustworthy AI in Europe

Risk-based rules for AI systems:



Transparency and risk management for powerful AI models that can be components of AI systems

- Enhanced Product Safety legislation + Lifecycle approach
- Coordinated governance system – based on well established logic
- Fostering responsible innovation through AI regulatory sandboxes and real-world testing
- Future-proof legislation through use of standards, codes of practice and delegations

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

A holistic governance structure

Rules for AI systems

National level:
EU Member States to designate supervisors

Rules for general-purpose AI models

EU level:
AI Office within Commission

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

Deep-dive into the AI Act’s rules on high-risk AI systems

When is an AI system ‘high-risk’ under the AI Act?

The AI Act classifies AI systems as ‘high-risk’ in two ways:

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

Concerns 22 product regulations (Annex I).
Examples: *Machinery Regulation, Radio Equipment Directive, Toy Safety Regulation*

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 **AI system is intended to be used in a high-risk use case**

8 areas which are sensitive for health, safety and fundamental rights (Annex III) with concrete use cases listed for each area.

AI system classifies as high-risk if it is **intended to be used for one of these use cases**.

„Filter“: AI systems can be excluded from the high-risk use cases in four cases, e.g. if they perform only a narrow procedural task.

EUROPEAN **ARTIFICIAL INTELLIGENCE** OFFICE

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**
- → 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

Specific obligations for the public sector

Specific obligations for deployers of high-risk AI systems apply only to the public sector:

Bodies governed by public law have to carry out a **fundamental rights impact assessment**

Public authorities, agencies and other bodies have to **register the deployment** of high-risk AI in EU database

EUROPEAN **ARTIFICIAL INTELLIGENCE** OFFICE

AI Act & sectoral product safety legislation

Key principle: **complementarity**

- **New Legislative Framework** (Annex I A) + Cyber Resilience Act → high-risk requirements apply immediately
- **Old Legislative Framework** (Annex I B):
  → high-risk requirements apply through the amendments into sectoral legislation

AI Act and EU Data protection law are complementary and mutually reinforcing

AI Act

Sets harmonised rules for the marketing and use of AI systems, irrespective of whether personal data is processed

- Market-based and product safety approach aiming to address risks to health, safety and fundamental rights across the whole AI lifecycle and value chain, while fostering innovation
- Risk-based with targeted rules (prohibitions, high-risk, transparency) complementing EU data protection law
- For example, Article 5(1)h) AIA lex specialis for the EU law enforcement directive
- AI Act does not create a legal basis for personal data processing, except Art. 10(5) and Art. 59

EU data protection law

Sets rules for processing of personal data

- GDPR, LED and EUDPR
- Fundamental rights and technology neutral approach
- Sets general principles and obligations for controllers/processors and rights of data subjects
- Relevant rules continue to apply when personal data is processed for training or using AI systems/AI models

Clarity needed how rules interplay and cooperation between supervisory authorities

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

AI as the touchpoint: how the digital rulebook applies

DSA, DMA and AI Act are designed to be complementary and mutually reinforcing.

The DSA

AI can be used within online platforms and search engines

- Disclosure obligations for recommender, advertising and content moderation systems
- Providers of very large online platforms and search engines must analyse and mitigate systemic risks of algorithmic systems in their services

The DMA

DMA covers AI if it is part of core platform services

- For example, a virtual assistant, a search engine or an operating system.
- DMA requirements may include limiting the use of data accumulated through services (e.g. for training AI), ensuring that users have access to their data and requiring fair ranking in search results.

The AI Act

AI Act applies to AI integrated into online services or if the AI is an online service

- Prohibition of harmful manipulative or exploitative AI
- Transparency obligations for generative AI, e.g. watermarking and labelling of deep fakes
- Transparency and risk management for general-purpose AI models (synergy with DSA – reflected in AIA)

Interplay of DSA and AI Act in addressing harmful AI-enabled practices of online platforms

DSA addresses societal and systemic harms of online services. AI Act adds additional protection by prohibiting unacceptable cases resulting in significant harm.

DSA allows **targeted advertising and recommender systems**, but mandates transparency and gives opt-out from profiling

AI Act prohibits **AI-enabled manipulation and social scoring** resulting in significant harm

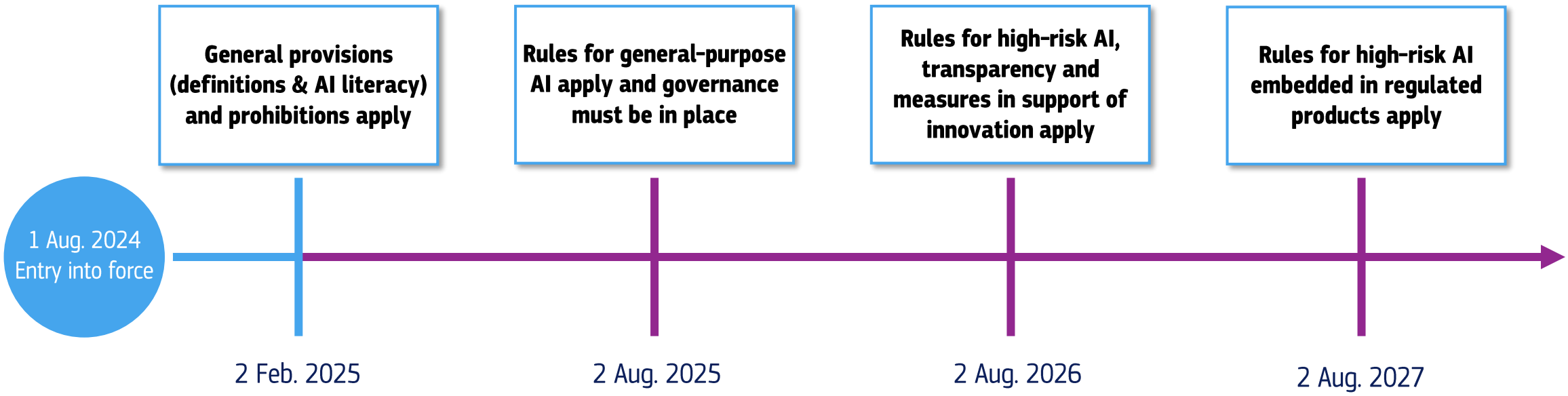
DSA provides a **high-level of privacy, safety and security to minors**

AI Act prohibits AI-enabled **exploitation of children's vulnerabilities** resulting in significant harm

EUROPEAN **ARTIFICIAL INTELLIGENCE** OFFICE

Update on the AI Act’s implementation

The AI Act timeline



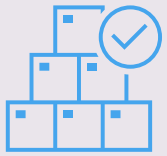
EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

Implementation priorities for the AI Act

Set-up of governance structure

- Growing the **AI Office**
- Collaboration with **Member States** in the AI Board
- Establishing the **Scientific Panel** and **Advisory Forum**

Providing guidance on the practical AI Act application



- Publication of **guidance documents & guidelines**
- Coordinating the development of stakeholder-driven instruments like **standards** and the **code of practice** on general-purpose AI

Stakeholder outreach and support in compliance

- **AI Pact** network with more than 3000 stakeholders
- Actions under **Digital Europe Programme**
- Upcoming **AI Act Service Desk**

EUROPEAN **ARTIFICIAL INTELLIGENCE** OFFICE

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

Thank you for your attention.

Tatjana.Evas@ec.Europa.eu