The EU AI Act and cybersecurity

Kilian Gross

Deputy Director

European AI Office – DG CONNECT

Artificial intelligence – the EU vision

“ ever more powerful AI models have been released. Some expect models that will approach human reasoning within a year's time. […]

Together, we built a shared consensus that AI will be safe, and that it will promote our values and benefit humanity. […]

The time has come for us to formulate a vision of where we want AI to take us, as society and as humanity. […]
We want Europe to be one of the leading AI continents.

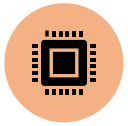
Ursula von der Leyen, President of the European Commission
11 February 2025, AI Action Summit in Paris

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

Artificial intelligence – the changing landscape

AI is now a core part of many products and services

AI is transforming cybersecurity – new opportunities but also new threats and challenges



Cybersecurity threats: Advanced GPAI can, for example, exploit vulnerabilities, create adaptive malware, and automate cyber-attacks or phishing

The EU is responding: The EU AI Act is the world's first comprehensive AI regulation to promote uptake and innovation in **TRUSTWORTHY AI.**

EUROPEAN **ARTIFICIAL INTELLIGENCE** OFFICE

The AI Act – a strategic asset

Horizontal product safety legislation

- “Classic” EU internal market rules
- Coherence with EU acquis on product safety

Technology neutral

- Focus on AI systems
- No regulation of technology, but of use cases

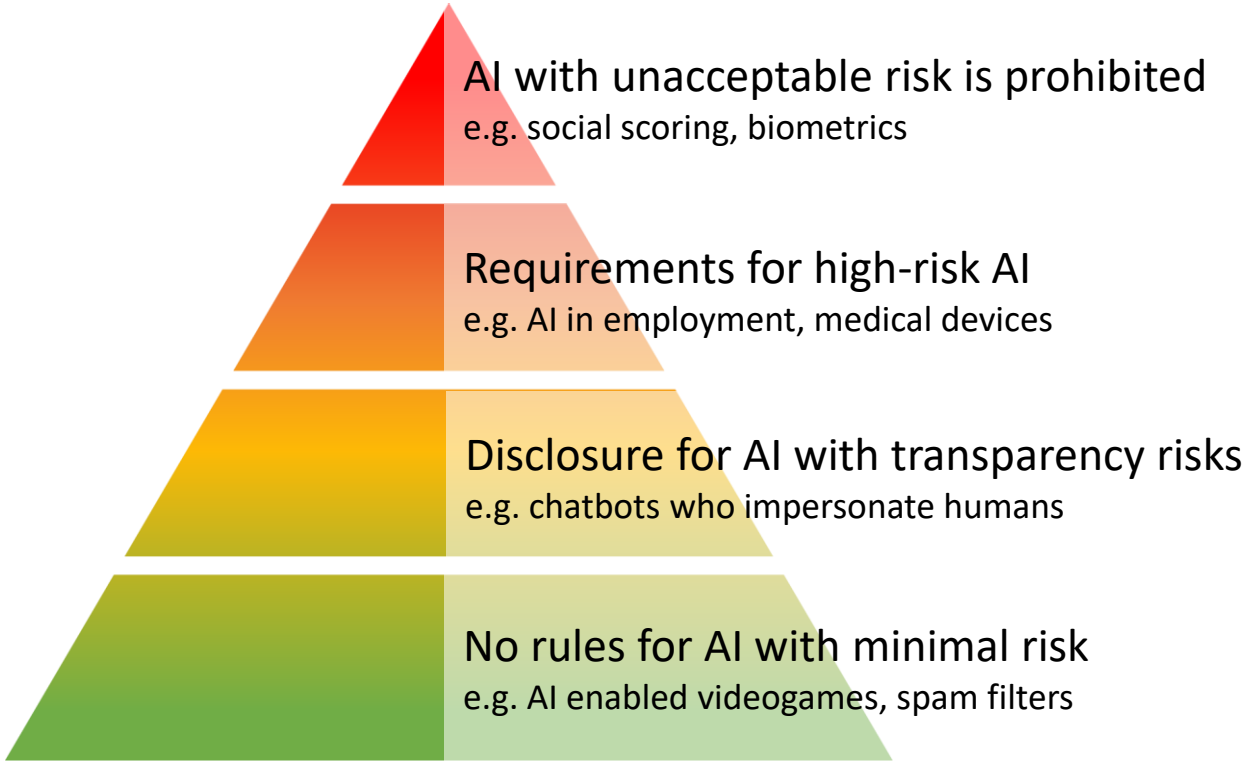
Risk-based approach

- Applying rules commensurate to risk
- Covers risks to health, safety & fundamental rights

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

AI Act – risk-based approach

Risk-based rules for AI systems:



Transparency and risk management for **general-purpose AI models** that can be components of AI systems

- Ensuring safe and trustworthy AI
- Fostering responsible innovation
- Complementarity with other EU law
- Future-proof and adaptable

EUROPEAN **ARTIFICIAL INTELLIGENCE** OFFICE

The AI Act – key provisions on cybersecurity

- **Cybersecurity is an important element of the requirements to ensure that high-risk AI systems and GPAI models with systemic risks are trustworthy!**
- **High-risk AI systems:** Article 15 (requirements), Article 42 (2) (presumption of conformity) + Recitals 76, 77, 78 and 122
- **General-purpose AI models with systemic risks:** Article 55 (1) d) (obligation) + Recitals 114 and 115

AI Act – a unified approach to safety and security

The EU AI Act leads a paradigm shift:

- **AI cybersecurity** is one of the essential requirements of **AI system safety**
- Cybersecure-by-design is not optional—**it's legally mandated**
- Organizations must treat cybersecurity as an **integral feature** of AI system development, not a separate domain
- Cybersecurity is **not just security of IT infrastructure**

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

AI Act – requirements and standards

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

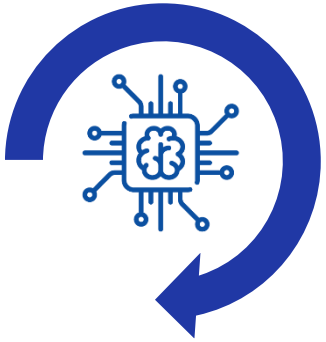
Provider is responsible for EU declaration of conformity + CE marking

(Harmonized) Standards – in preparation

- → **Operational tools to support regulatory compliance with the requirements under the AI Act**
- → 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

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

Disclosure obligations and risk management for GPAI 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 those with systemic risk

Code of practice developed together with stakeholders will detail out rules

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

AI Act interplay with the Cyber Resilience Act

- CRA sets horizontal cybersecurity rules for all digital products
- AIA sets AI specific cybersecurity rules
- Both AIA and CRA are part of EU ‘New Legislative Framework’ safety acquis’
- **Standards will play a key role**
- Presumption of conformity + One conformity assessment procedure for AI enabled products (default rule the AI Act)

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

Recap: The AI Act – the changing paradigm

Cybersecurity is a core part of AI Act product safety approach

→ The Act **explicitly includes cybersecurity** as one of the essential requirement of high-risk AI system safety. That means: High-risk AI system that is **not cybersecure is, by definition, not safe under the EU AI Act**.

Requirements for high-risk AI systems in the Act:

- Implement **technical measures to manage and mitigate risks** including cybersecurity risks **– RMS & QMS**
- Prevent **data manipulation and data vulnerabilities**
- Maintain **logging** and comply with **transparency and human oversight**
- Ensure **resilience against adversarial attacks**
- Comply with **state-of-the-art cybersecurity practice**

Standards – compliance tools

EUROPEAN **ARTIFICIAL INTELLIGENCE** OFFICE

The AI Act's governance structure

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

Market surveillance authorities

Rules for general-purpose AI models

Commission (AI Office)

AI Board
with EU Member States to coordinate at EU level

Scientific Panel
supports with independent technical advice

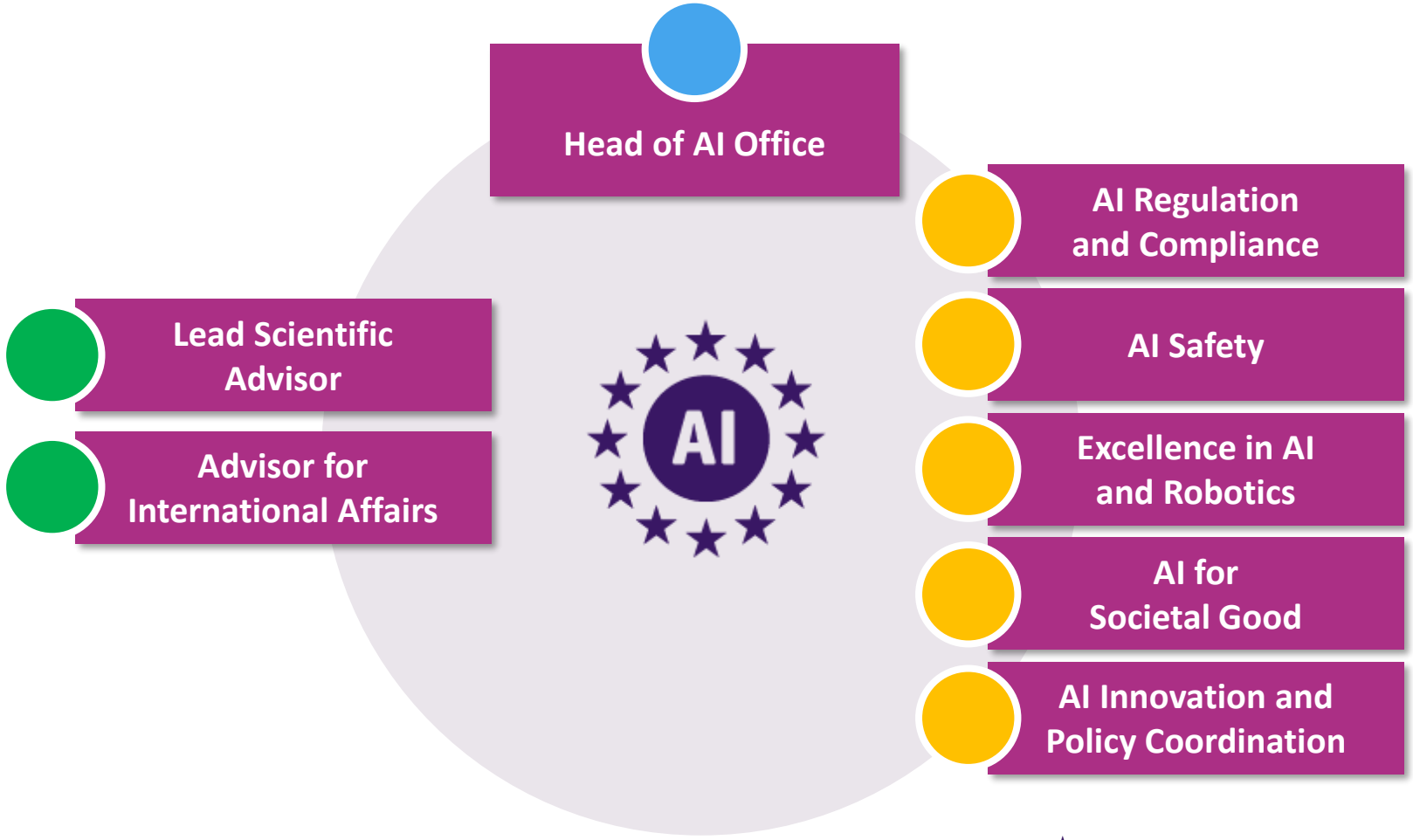
Advisory Forum
supports with stakeholder input

EUROPEAN **ARTIFICIAL INTELLIGENCE** OFFICE

Introducing the European AI Office

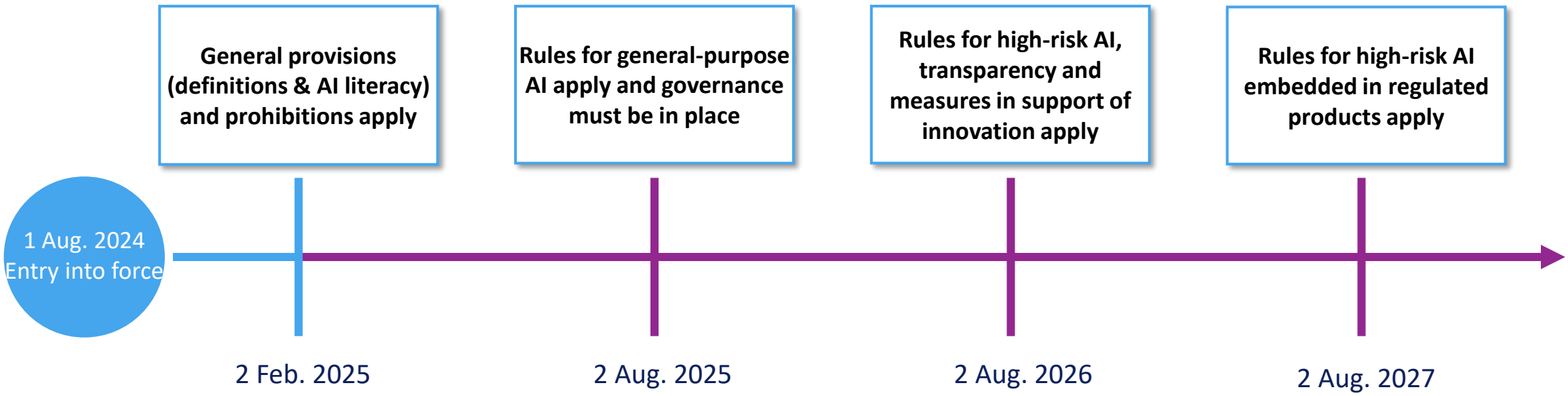
360 degrees vision on AI:

- key role in the implementation of the AI Act, especially in relation to general-purpose AI models
- fosters research and innovation in trustworthy AI
- positions the EU as a leader in international discussions and contributor to AI for good



EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

The AI Act timeline



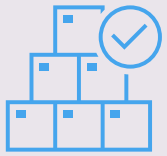
EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

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



- In-depth **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, webinar and workshops
- 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.