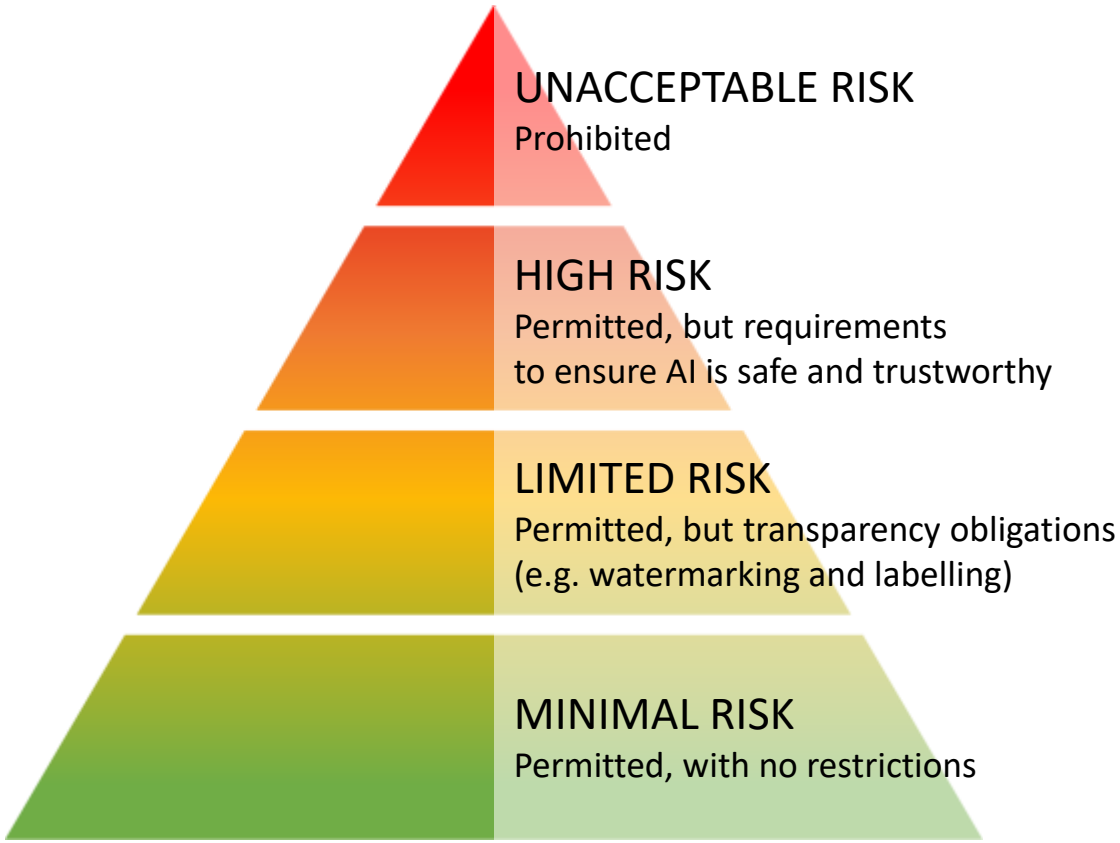
Relevance of the AI Act for the security and border management

Yordanka Ivanova
Head of Sector ‘Legal oversight of AI Act implementation’
European AI Office
European Commission (DG CNECT)

The EU AI Act:
A risk-based legislation for Trustworthy AI systems



- Entered into force 1 August 2024
- Address risks to health, safety and fundamental rights
- Promote innovation and uptake
- Complementary and coherent with other Union law (e.g. on migration)

Unacceptable AI practices will be banned

Manipulation or exploitation of vulnerabilities	to manipulate people and thereby cause significant harms
Social Scoring	for public and private purposes
Biometric categorisation	to deduce or infer for example race, political opinions, religious or philosophical beliefs or sexual orientation, exceptions for labelling in the area of law enforcement
Real-time remote biometric identification	for the purpose of law enforcement, 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 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 databases

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

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 systems 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 **‘Stand-alone’ AI systems used in specific high-risk use cases**

8 areas which are sensitive for health, safety and fundamental rights (Annex III) with **concrete use cases listed for each area that are identified as ‘high-risk’**

„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

Relevant high-risk AI systems in the security and border management

1. Biometrics (Annex III point 1):

- *Remote biometric identification*
- *Biometric categorisation to infer sensitive data*
- *Emotion recognition*

2. Law enforcement (Annex III point 6):

- *AI systems to assess the risk of a natural person becoming the victim of criminal offences;*
- *Polygraphs or similar tools;*
- *AI systems to evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences;*
- *AI systems to assess the risk of a natural person offending or re-offending not solely on the basis of the profiling, or to assess personality traits and characteristics or past criminal behaviour*
- *AI systems for profiling in the course of the detection, investigation or prosecution of criminal offences.*

3. Migration, asylum and border control management (Annex III point 7):

- *Polygraphs or similar tools;*
- *AI systems to assess a risk, including a security risk, a risk of irregular migration, or a health risk, posed by a natural person who intends to enter or who has entered into the territory of a Member State;*
- *AI systems for the examination of applications for asylum, visa or residence permits and for associated complaints with regard to the eligibility of the natural persons applying for a status*
- *AI systems in the context of migration, asylum or border control management, for the purpose of detecting, recognising or identifying natural persons, with the exception of the verification of travel documents.*

Relevant acts and special provision for migration

Entry into force for Annex III high-risk: 2 August 2026

Special rules for systems already placed on the market before that date (Article 111(1))

AI systems which are components of the large-scale IT systems established by the legal acts listed in Annex X that have been placed on the market or put into service before 2 August 2027 shall be brought into compliance with this Regulation by 31 December 2030.

The requirements laid down in this Regulation shall be taken into account in the evaluation of each large-scale IT system established by the legal acts listed in Annex X to be undertaken as provided for in those legal acts and where those legal acts are replaced or amended.

Relevant union legislative acts on large-scale IT systems in the area of Freedom, Security and Justice (Annex X)

1. *Schengen Information System - Regulation (EU) 2018/1860, Regulation (EU) 2018/1861 and Regulation (EU) 2018/1862*
2. *Visa Information System - Regulation (EU) 2021/1133 and Regulation (EU) 2021/1134*
3. *Eurodac - Regulation (EU) 2024/1358*
4. *Entry/Exit System - Regulation (EU) 2017/2226,*
5. *European Travel Information and Authorisation System - Regulation (EU) 2018/1240 and Regulation (EU) 2018/1241*
6. *European Criminal Records Information System on third-country nationals and stateless persons - Regulation (EU) 2019/816 (ECRIS-TCN)*
7. *Interoperability - Regulation (EU) 2019/817 (borders and visa) and Regulation (EU) 2019/818 (police and judicial cooperation, asylum and migration)*

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

What are high-risk requirements and obligations?

Providers

- **Requirements for the AI system,** e.g. data governance, human oversight, accuracy & robustness, operationalised through **harmonised standards**
- **Conformity assessment** before placing the system on the market and **post-market monitoring**
- **Quality and risk management** to minimize the risk for deployers and affected persons
- **Registration** in the **EU database**

Deployers

- **Correct deployment**, training of employees, use of **representative data** and **keeping of logs**
- Possible **information obligations** vis-a-vis affected persons
- Possible **fundamental rights impact assessment** (applies only to some deployers, incl. public sector)
- Public sector also has to **register the deployment** of high-risk AI in EU database

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

‘Transparency’ obligations for certain AI systems

Trust through disclosure

AI systems interacting with people:

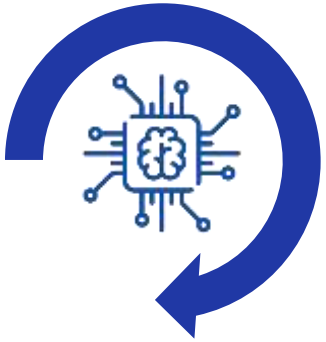
- Humans have to be informed if they interact with an AI and this is not obvious
- Deployers have to inform people if they use emotion recognition or biometric categorisation (with some exceptions for law enforcement)

AI-generated content:

- AI systems that generate output need to include machine readable marks
- Visible labelling of deep fakes (audio, image and video content) and certain text that is intended to inform the public on matters of public interest

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

The EU AI Act:
Rules for powerful AI models



General-purpose AI models

= highly capable AI models used at the basis of AI systems such as ChatGPT and numerous downstream AI applications

Transparency for all general-purpose AI models

+

Risk management for GPAI models with systemic risks

Codes of practice developed together with stakeholders will detail out rules

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

The EU AI Act:
A robust governance structure

Rules for AI systems

National level:
EU Member States to designate national supervisors

EU level:
The European Data Protection Supervisor oversees systems used by EU institutions, bodies and agencies

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

AI Act – priorities for implementation

- **Setting up the governance structure**
  (AI Office, AI Board, Scientific Panel and Advisory forum)
- **Coordinating drawing up of Code of practice on General-Purpose AI**
- **Preparation of standards for high-risk requirements** (CEN/CENELEC)
- **Preparing guidelines, implementing and delegated acts**
  (e.g. on definition of AI system, prohibitions, high-risk use cases, transparency)
- **Support for the establishment of AI regulatory sandboxes**
  to promote innovation and regulatory learning

Entry into force: 1 Aug. 2024

Prohibitions	2 Feb. 2025
Governance & GPAI	2 Aug. 2025
All other rules (incl. High-risk Annex III)	2 Aug. 2026
High-risk AI in products (Annex I)	2 Aug. 2027

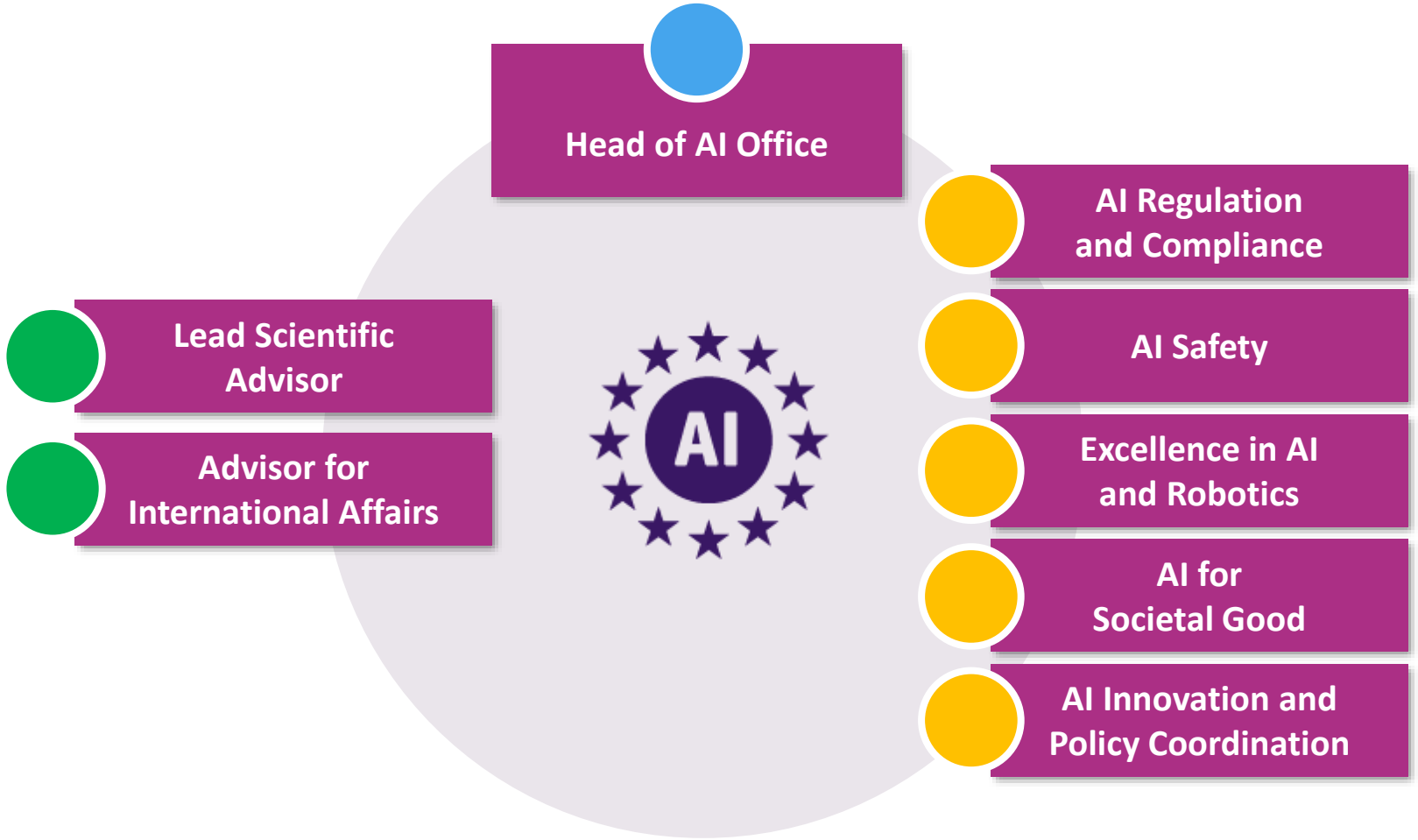
The AI office launched **AI Pact** to support companies and other organisations in the implementation and foster anticipated application of the AI Act

European Commission

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

Advisory governance bodies

AI Board

- High-level representatives & experts from Member States
- Advising and steering on all matters of AI policy

Scientific Panel

- Independent experts with scientific or technical expertise
- Supports in enforcement of AI Act, can issue alerts of risks

Advisory Forum

- Advises AI Office and provides stakeholder input
- Diverse composition, balancing commercial and non-commercial interests

AI Office coordinates set-up of all three and supports the operation by providing the Secretariat

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

Current AI Act priorities:
2. Preparing Commission guidelines

Practical guidance on prohibitions

Practical guidance on AI system definition

To be adopted before rules start to apply on 2 February 2025.

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

Current AI Act priorities:
3. Supporting compliance

Community-building through AI Pact

Network with **1000+ organisations**, including **public sector**.

Outreach and webinars on AI Act, 10 workshops coming up over next months.

Voluntary pledges to anticipate AI Act. Includes Google, OpenAI, Nokia, IBM.

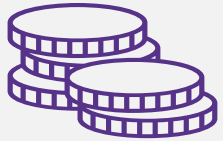
Standards to operationalise AI Act rules

Standards will play a **key role for providers** to facilitate compliance.

CEN and CENELEC are already working on standards for high-risk requirements.

Publication expected for **spring 2025**. Commission to assess and endorse.

Digital Europe Programme support actions



Pilot for **Union Testing Facility** in AI to support authorities in enforcement.

Support action for **EU-level coordination of AI regulatory sandboxes** by public authorities.

AI Innovation Accelerator will provide materials, training courses and tools.

EUROPEAN **ARTIFICIAL INTELLIGENCE** OFFICE

Thank you for your attention!