



Acting as the voice of the security industry

Confederation of European Security Services

The EU AI Act in Practice

AI use cases in private security





Objectives of today's meeting

- help CoESS members understand the regulatory logic and risk-based approach underlying the AI Act.
- Introduction of the legal concept of high-risk AI.
- Business realities meet the EU AI Act: AI use cases in security and classification.

What can companies do now to drive responsible AI uptake?





Irina Orssich

Head of AI Act Governance and Regulatory Policy

European Commission's EU AI Office

Private security services in Europe





High-potential AI use cases in security services





AI in private security services: *Opportunities and risks*

Opportunities in private security services



Performance



**Occupational
Safety**



New Jobs

Risks in private security services



**Fundamental
right risks**



Security risks



Secondary effects

Four pillars for responsible AI deployment

1. AI governance and accountability
2. AI literacy and human oversight
3. Secure and resilient operations
4. Due diligence



Acting as the voice of the security industry

Confederation of European Security Services



Charter

on the ethical and responsible use of Artificial Intelligence in the European private security services

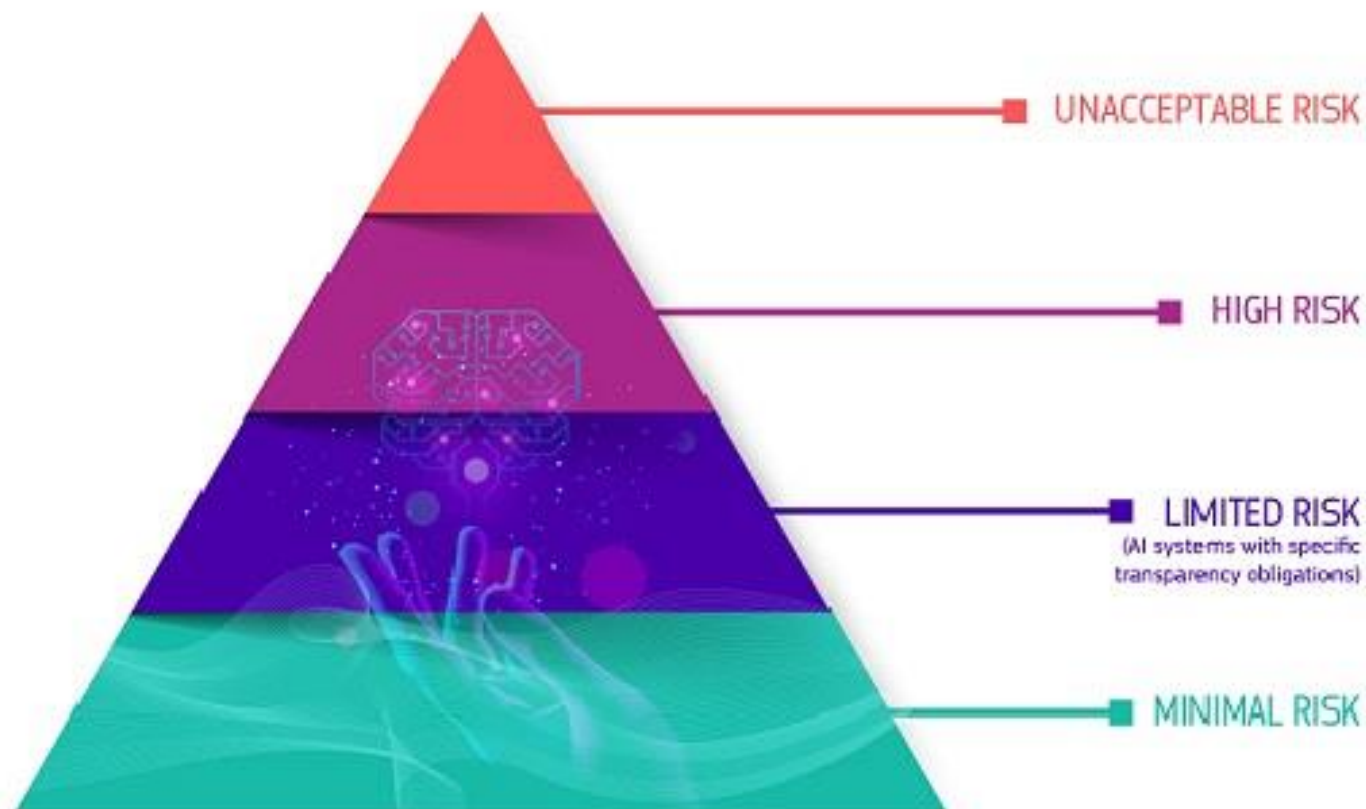




Introduction into the EU AI Act

EU AI Act

- since August 2024 in force.
- applies since February 2025 in stepped approach.
- Risk-based approach.





AI use cases in private security services

Low risk



Risk analysis



Crowd surveillance



Biometric verification

High risk



Airport security (APIDS)



RBI



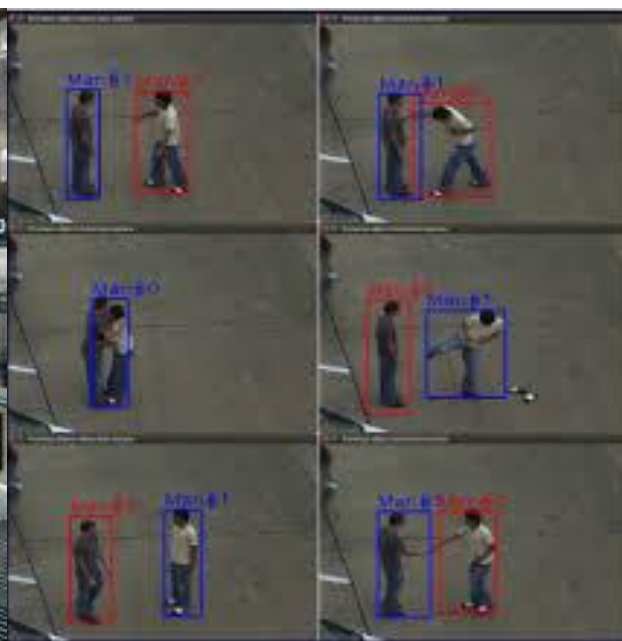
HR management



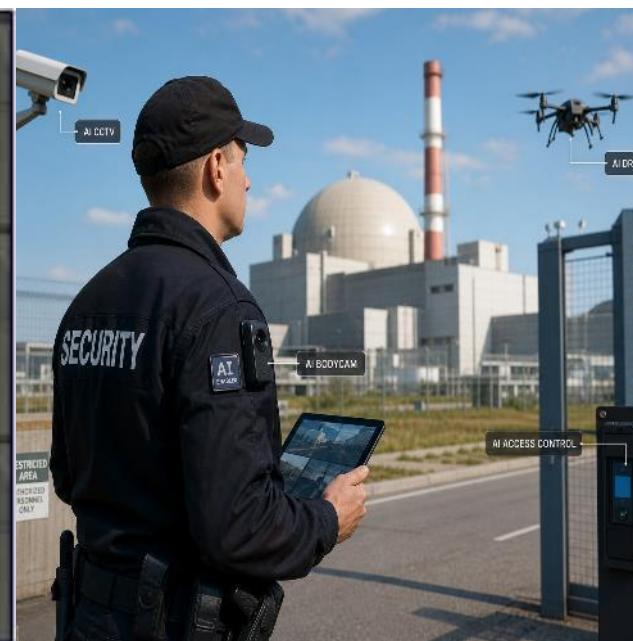
Examples for cases of uncertain classification



Biometric
identification



Behaviour
detection



Critical
Infrastructure
Protection



Alarm dispatch



Key questions for discussion

1. When do the uncertain AI use cases classify as high-risk AI?
2. What should companies prepare for now in terms of AI governance and compliance?
3. What are key documents and stakeholders that can help?



Uncertain AI use cases

“Law Enforcement Authority”



EU AI Act Definition of „Law Enforcement Authority“: *Any body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or (...), including the safeguarding against and the prevention of threats to public security;*

Annex III, Draft Guidelines: *The classification (...) depends not on the formal designation of the body or entity as such, but on whether the tasks it performs, as granted by law, are of a law enforcement nature, i.e. the prevention, investigation, detection, or prosecution of criminal offences (...).*

Question: *private security prevents crime, but does not exercise public law-enforcement powers. Which factors are considered decisive in distinguishing an entity entrusted with public authority and public powers from one that is licensed and regulated to carry out a commercial security activity.*



Uncertain AI use cases

“Remote Biometric Identification”



The EU AI Act classifies in Point 1(a) of Annex III Remote Biometric Identification systems as high-risk.

Para. 129 in the Draft Guidelines continues:

An AI system must fulfil three conditions to be classified as an RBI system:

- (i) its purpose must be biometric identification;*
- (ii) that identification must occur without the active involvement of the person concerned, typically at a distance;*
- (iii) the system must perform a comparison between that person’s biometric data and biometric data contained in a reference database.*

Question : when is active involvement present?



Uncertain AI use cases

“Behavioural Event Detection”



The EU AI Act classifies in Point 1(c) of Annex III Emotion Recognition Systems as high-risk.

Para. 177 in the Draft Guidelines *excludes the detection of a “fighting stance” or of a physical position indicating a concealed weapon, but classifies the flagging of “aggressive posture” - for example via body-worn cameras or crowd-mood screening - as high-risk emotion recognition.*

Question : These describe near-identical sensing operations in standard guarding activity.

Shouldn’t flagging unusual conduct, posture or movement without concluding what a person feels or intends be outside the high-risk AI scope, unless the AI itself infers emotion or intent?



Uncertain AI use cases

“AI security systems in Critical Infrastructure”

Safety vs. security function



Point 2 of Annex III AI Act lists as high-risk six use cases of AI systems intended to be used as a safety component in the management and operation of certain specific cases of critical infrastructure.

Para. 185 clarifies that „Components designed solely to prevent the following types of harm or damage should not be regarded as ‘safety components’:

- a) non-physical harm or immaterial damages;
- b) any damages caused by third parties.”

Para. 206 in the Draft Guidelines continues that “An AI system used in a surveillance and protection for physical perimeter protection such as camera systems, radar systems and drone control systems used to directly protect the physical integrity of the infrastructure” falls into the high-risk AI classification.

Question : shouldn't AI systems that detect externally originating threats, rather than hazards generated by the infrastructure itself, be excluded from high-risk?



Uncertain AI use cases

“AI security systems in Critical Infrastructure”

Autonomy of the system



Point 2 of Annex III AI Act lists as high-risk six use cases of AI systems intended to be used as a safety component in the management and operation of certain specific cases of critical infrastructure.

Para. 184 in the Draft Guidelines adds AI systems intended to be used as a component in CI:

- *to monitor and detect situations which may directly lead to physical harm to natural persons or physical damage to property;*
- *to prevent physical harm to natural persons or physical damage to property (...);*
- *mitigate consequences of possible physical harm (...).*

Question : this would cover a large range of AI security system. Where “detect-and-alert-a-human” configurations sit ?



Uncertain AI use cases

“Alarm monitoring, dispatch and response”



Point 5(d) of Annex III classifies as high-risk AI systems intended to evaluate or classify emergency calls by natural persons or to be used to dispatch or to establish priority in the dispatching of emergency first response services

Para. 330 in the Draft Guidelines clarifies that this includes *e.g. AI systems intended to be used to evaluate and classify emergency calls by natural persons, and to dispatch and prioritise emergency first response services.*

Questions : what about use cases where :

- *humans retain full decision-making authority (system alert one input among others)*
- *and where AI systems to prioritise or dispatch response are used in private Alarm Receiving Centres (ARCs) for private response only - not public emergency response?*



Next steps

1. What should companies prepare for now in terms of AI governance and compliance?
2. What are key documents and stakeholders that can help?

