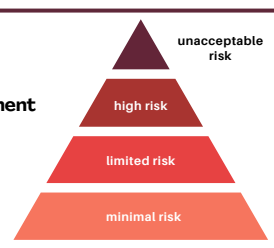
AI Act: key takeaways

1 Applicability
the basics

- **AI**: OECD definition
- **Scope**: organisation within and outside of the EU
- **Exempted**: national security, militrary and defence, R&D and open source
- **Compliance due**: within 6-24 months

2 Risk based approach
unacceptable > high > limited > minimal

- **Prohibited**
- Conformity **assesment**
- **Transparency**
- **No** obligations



3 When is the AI prohibited?
unacceptable risk

- **Social credit scoring**
- Exploitation of **vulnerabilities** (including age or disability)
- Behavioural **manipulation** or manipulation of free will
- **Emotion detection** at the workplace or educational settings
- Untargeted **scraping** of facial images for facial recognition purposes
- Applications for **predictive policing** (some excluded)
- **Biometric categorisation** systems using sensitive characteristics
- Law and enforcement use of real-time **biometric identification in public**

4 When is the AI high risk?
conformity assesment needed

- **Emotion recognition** applications (excluding workplace and educational settings)
- **Biometric identification technologies**
- **Vehicles** and transportation systems
- **Medical devices**
- Recruitment, **human resource** and workforce management
- Education and vocational **training** systems
- **Law enforcement**, **border** security, **migration** and **asylum**
- Access to **specific services** (including insurance, banking, credit, and other (public) benefits)
- Administration of **justice**
- Specific products and their **safety components**

5 Key requirements HRAI
high risk AI conformity assesment

- Assessment of impact on **fundamental rights** and conformity evaluation
- Register in a public **EU-database** for HRAI
- Establishment of **risk and quality management** systems
- **Data governance measures**, including bias reduction and representative training data
- Enhanced **transparency**, including usage instructions, system limitations, and technical documentation
- **Human supervision**, encompassing explainability, auditable logs, and human-in-the-loop
- Ensuring **accuracy**, **robustness**, and **cybersecurity**, including system testing and continuous monitoring

6 General purpose AI
also called 'GPAI'

- **Specific** requirements for GPAI and foundation models
- Full **transparency** for **all** GPAI implementations: e.g. with technical documentation, executive summaries, and safeguards for intellectual propertyrights
- **Extra requirements for high-impact models with systemic risks**: such as model evaluations, comprehensive risk assessments, adversarial testing, and mandatory incident reporting
- For **generative AI**: **mandatory disclosure** making sure that individuals know when they are interacting with AI systems (such as chatbots). AI-content must be clearly **labeled** and made **detectable** (e.g. in the case of deepfakes)

7 Fines and enforcement
in case of non-compliance

- **Prohibited** AI violations: up to 7 % of global annual turnover or €35 million
- **Other** violations: up to 3% of global annual turnover or €15 million
- Spreading **incorrect information**: up to 1.5% of global annual turnover or €7.5 million
- **Limit** on fines for SMEs and startups
- **European** AI Office and AI Board (at central EU level)
- Market surveillance **authorities** in EU countries
- **Any individual** can make complaints about non-compliance