EU AI Act

CHEAT SEET

🔍 Basics

Definition of AI: Aligned to the OECD definition

Extraterritorial: Applies to organizations outside the EU

Exemptions: National security, military and defense; R&D; open source (partially)

Compliance Grace Periods: Between 6-24 months

Risk-Based: Prohibited AI >> High-Risk AI >> Limited Risk AI >> Minimal Risk AI

Generative AI: Specific transparency and disclosure requirements

Synthetic risk: undefined

🤖 General Purpose AI (GPAI)

Encompasses AI models used across various applications, subjected to strict oversight due to their wide-reaching impact.

- **Distinct requirements** for General Purpose AI and Foundation Models
- **Adaptability**
- **Wide application range**
- **Large-scale impact potential**

🌐 Open Source AI

Addresses the unique context of AI developed in open-source environments, with specific exemptions and risk considerations.

- Pre-trained AI models under an **open-source license** exempted from minimum standards
- **Systemic Risk Coverage:** Inclusion of open-source models in systemic risk provisions for General Purpose AI (GPAI)

🚫 Prohibited AI

Practices banned due to their high potential for abuse, privacy infringement, or societal harm.

- **Social credit scoring**
- **Emotion recognition** in workplaces and educational institutions
- AI **exploiting vulnerabilities** (e.g., age, disability)
- **Behavioural manipulation** and circumvention of free will
- Untargeted **scraping of facial images** for facial recognition and **Biometric categorisation**
- Specific **predictive policing** applications
- **/ Limited use** of real-time biometric identification in law enforcement in public spaces

⚙️ Systemic risks - lacks clear definition

Models that could globally impact society or economies, typically very large and interconnected systems.

- Widespread **impact**
- **Interconnectedness**
- **Data privacy** and security
- **Bias** and discrimination
- **Dependence** on AI
- **Lack of transparency**
- **Governance** challenges
- **Economic a**nd Labor market disruption
- **Ethical** and Societal Concerns
- **Global reach and compliance**

Key requirements

- **Model evaluations**
- **Systemic risk assessments**
- **Adversarial testing**
- **Comprehensive impact assessments**
- **Incident reporting**

⚠️ High risk AI

Significant implications for individual rights and safety, particularly in sensitive sectors.

- **Medical devices**
- **Vehicles**
- **Recruitment**, HR, and worker management
- **Education** and vocational training
- **Election** and voter influence
- **Access to services** (insurance, banking, credit, benefits, etc.)
- **Critical infrastructure management** (water, gas, electricity, etc.)
- **Emotion recognition**
- **Biometric identification**
- **Law enforcement, border control, migration, and asylum**
- **Administration of justice**
- **/ Specific products** and safety components

Key requirements

- **Fundamental rights** impact assessment and conformity assessment
- **Registration in a public EU database**
- **Risk management and quality management systems**
- **Data governance** (bias mitigation, representative training data, etc.)
- **Transparency** (Instructions for Use, technical documentation, etc.)
- **Human oversight** (explainability, auditable logs, human-in-the-loop, etc.)
- **Accuracy, robustness, and cybersecurity**

💰 Penalties & Enforcement

- Fines up to 7% of global annual turnover or €35m for prohibited AI violations
- Fines up to 3% of global turnover or €15m for most other violations
- Fines up to 1.5% of global turnover or €7.5m for providing incorrect information
- Caps on fines for SMEs and startups
- Establishment of a European AI Office and AI Board at the EU level
- Market surveillance authorities in EU countries to enforce the AI Act
- Provision for individual complaints about non-compliance

📅 Status - 12/12/23

- **Not yet enacted**
- **Political agreement reached on 8 December 2023**

✏️ Made by

Balazs Nemethi - @nembal