EU AI ACT Cheat Sheet

Understanding the world's first comprehensive AI law

THE BASICS

- **AI defined in accordance with the newly revised OECD definition.**
- **Extraterritorial application** extends to organizations beyond the EU.
- **Exemptions** include national security, military and defense, R&D, and partial coverage for open source.
- **Grace periods** for compliance range between 6 to 24 months.
- **Categorization based on risk:** Prohibited AI, High-Risk AI, Limited Risk AI, and Minimal Risk AI.
- **Stringent demands** placed on 'Providers' and 'Users' of High-Risk AI.
- **Generative AI** necessitates specific transparency and disclosure criteria.

PROHIBITED AI

- Systems for **social credit scoring**
- Employment and educational **emotion recognition** systems
- AI leveraging **people's vulnerabilities** (e.g., age, disability)
- **Manipulation** of behavior and undermining free will
- **Indiscriminate collection of facial images** for facial recognition
- **Biometric categorization systems** involving sensitive traits
- Particular **predictive policing uses**
- **Law enforcement** employing real-time biometric identification in public (except in restricted, pre-approved scenarios)

HIGH-RISK AI

- **Medical devices & Automobiles**
- **Hiring, human resources, and labor supervision**
- Instruction and **professional education**
- Shaping **political elections and the voting populace**
- **Entry to amenities** (like insurance, banking, credit, benefits, etc.)
- Supervising **crucial infrastructure** (like water, gas, electricity, etc.)
- Systems for **recognizing emotions** and identifying individuals via **biometrics**
- **Policing, regulating borders, migration, and asylum procedures** and conducting **legal affairs**
- Particular **merchandise or safety elements** within particular products

KEY REQUIREMENTS: HIGH-RISK AI

- **Assessment of fundamental rights' impact and conformity**.
- Enrollment in the public **EU database** for high-risk AI systems.
- Establishment of **risk and quality management systems**.
- **Governance of data** (such as bias mitigation and representative training data).
- Enhancement of **transparency** (e.g., Instructions for Use, technical documentation).
- Inclusion of **human oversight** (e.g., explainability, auditable logs, human-in-the-loop).
- **Ensuring accuracy, robustness** and **cybersecurity** (e.g., through testing and monitoring).

GENERAL PURPOSE AI

- Different specifications for **General Purpose AI** (GPAI) and **Foundation Models**
- **Ensuring transparency** across all GPAI (like technical documentation, summaries of training data, copyright and IP protections, etc.)
- Extra prerequisites for **high-impact models carrying systemic risk**: model assessments, risk evaluations, adversarial testing, incident reporting, etc.
- **Generative AI**: notifying individuals during AI interactions (e.g., chatbots); requiring AI-generated content to be labeled and identifiable (e.g., deepfakes)

PENALTIES & ENFORCEMENT

- Penalties of up to **7% of global annual turnover** or €35m for breaches involving prohibited AI.
- Penalties of up to **3% of global annual turnover** or €15m for most other violations.
- Penalties of up to **1.5% of global annual turnover** or €7.5m for providing inaccurate information.
- **Limits on fines for SMEs and startups**.
- Establishment of the **European 'AI Office' and 'AI Board'** centrally within the EU.
- **Market surveillance authorities** in EU nations tasked with enforcing the AI Act.
- Empowerment of **any individual to file complaints** regarding non-compliance.

Not yet enacted. Political agreement reached on December 8th, 2023