

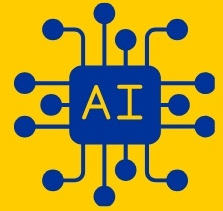


EU AI ACT Cheat Sheet



Understand the world's first comprehensive AI law

THE BASICS



- **Definition of AI:** aligned to the recently updated OECD definition
- **Extraterritorial:** applies to organisations outside the EU
- **Exemptions:** national security, military and defence; R&D; open source (partial)
- **Compliance grace periods** of between 6-24 months
- **Risk-based:** Prohibited AI >> High-Risk AI >> Limited Risk AI >> Minimal Risk AI
- **Extensive requirements** for 'Providers' and 'Users' of High-Risk AI
- **Generative AI:** Specific transparency and disclosure requirements

PROHIBITED AI



- **Social credit scoring** systems
- **Emotion recognition** systems at work and in education
- AI used to **exploit people's vulnerabilities** (e.g., age, disability)
- **Behavioural manipulation** and circumvention of free will
- **Untargeted scraping of facial images** for facial recognition
- **Biometric categorisation systems** using sensitive characteristics
- Specific **predictive policing** applications
- **Law enforcement use of real-time biometric identification in public** (apart from in limited, pre-authorised situations)

HIGH-RISK AI



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

KEY REQUIREMENTS: HIGH-RISK AI



- **Fundamental rights impact assessment** and **conformity assessment**
- Registration in **public EU database** for high-risk AI systems
- **Implement risk management** and **quality management** system
- **Data governance** (e.g., bias mitigation, representative training data etc.)
- **Transparency** (e.g., Instructions for Use, technical documentation etc.)
- **Human oversight** (e.g., explainability, auditable logs, human-in-the-loop etc.)
- **Accuracy, robustness and cyber security** (e.g., testing and monitoring)

GENERAL PURPOSE AI



- Distinct requirements for **General Purpose AI** (GPAI) and **Foundation Models**
- **Transparency** for all GPAI (e.g., technical documentation, training data summaries, copyright and IP safeguards etc.)
- Additional requirements for **high-impact models with systemic risk**: model evaluations, risk assessments, adversarial testing, incident reporting etc.
- **Generative AI**: individuals must be informed when interacting with AI (e.g., chatbots); AI content must be labelled and detectable (e.g., deepfakes)

PENALTIES & ENFORCEMENT



- Up to **7% of global annual turnover** or €35m for prohibited AI violations
- Up to **3% of global annual turnover** or €15m for most other violations
- Up to **1.5% of global annual turnover** or €7.5m for supplying incorrect info
- **Caps on fines for SMEs and startups**
- **European 'AI Office' and 'AI Board'** established centrally at the EU level
- **Market surveillance authorities** in EU countries to enforce the AI Act
- **Any individual can make complaints** about non-compliance

Based on publicly-available information following the political agreement reached by the EU institutions on 8 December 2023

Created by Oliver Patel, CIPP/E

Learn more about our [AI Governance Center](#) and find out latest AI resources on this [topic page](#).