European Union Artificial Intelligence Act

September 2021

Timeline and Background

Timeline

- **April 21** – EU Commission published draft AI Act
- **August 6** – Public feedback period on draft AI Act closes
- **~Q2 2022** – EU Parliament and Member States finish review/amendment of draft AI Act
- **~2024** – Requirements of draft AI Act begin to apply

Legislative Objectives

- Ensuring AI systems placed on EU market are safe and respect existing law on **fundamental rights**
- Part of crowded digital agenda: *Data Governance Act; Digital Services Act; Digital Markets Act; Data Act*

Scope – Applies To:

- **Providers** of AI systems placed on the EU market (regardless of where the provider is established)
- **Users** of AI systems where the user is located within the EU
- **Providers and Users** of AI systems located in a third country where the output produced by the AI system is used in the EU

Risk-Based Approach

- Draft AI Act distinguishes between AI systems/practices that create:
  1. Unacceptable risk → prohibited
  2. High risk → subject to compliance with various requirements
  3. Limited risk* → subject to information/transparency obligations
  4. Low or minimal risk → permitted with no restrictions

- **"AI system"** is defined as **software** developed with any of the following **techniques** and that can **generate outputs** such as content, predictions, recommendations or decisions:
  1. Machine learning approaches (including supervised, unsupervised and reinforced learning, as well as deep learning);
  2. Logic-and knowledge-based approaches (including knowledge representation, inductive programming, inference and deductive engines);
  3. Statistical approaches, Bayesian estimation, search and optimization methods

Unacceptable Risk

- Draft AI Act **prohibits** certain AI **practices**:
  1. Providing/using AI systems that deploy subliminal techniques or exploit vulnerabilities to distort behavior in a manner likely to cause harm
  2. AI-based general purpose social scoring (*e.g.*, trustworthiness) of natural persons by public authorities
  3. Real-time remote biometric identification systems in public spaces for law enforcement purposes

High-Risk AI Systems

- High-Risk AI systems are those in any of the following areas:
  1. Biometric identification and categorization of natural persons
     - AI systems intended to be used for 'real-time' and 'post' remote biometric identification of natural persons
  2. Management and operation of critical infrastructure (*i.e.*, water, gas, electricity, heating, road traffic)
  3. Education and vocational training
  4. Employment, workers management and access to self-employment
     - AI systems intended to be used for recruitment or selection of natural persons (e.g., advertising vacancies, filtering applications, evaluating candidates)
  5. Access to essential private and public services and benefits
  6. Law enforcement
  7. Migration, asylum and border control management
  8. Administration of justice and democratic processes
- List of high-risk AI systems to be reviewed by EU Commission annually

Requirements for High-Risk AI Systems

- **Risk management system**
  - Identification and analysis of foreseeable risks; adoption of risk management measures
- **Data governance and management**
  - Appropriate data collection practices, data preparation/processing operations, formulations of relevant assumptions and examinations of possible biases
- **Technical documentation**
  - Demonstrating how the system complies with the requirements of the Act
- **Logging capabilities**
  - Ensuring a level of traceability of the AI system's functioning throughout its lifecycle
- **Sufficient transparency**
  - To enable users to interpret the system's output, including instructions for use
- **Human oversight capabilities**
  - Aimed at minimizing risks to health, safety and fundamental rights
- Appropriate levels of **accuracy, robustness and cybersecurity**
  - In light of the AI system's intended purpose

Obligations on Providers of High-Risk AI Systems

- **Ensure the AI system is compliant** with requirements
  - May include "conformity assessment" procedures (form of ex-ante audit sometimes performed by third party "conformity assessment bodies")
  - Includes registration of high-risk AI systems in an EU database
- **Maintain a quality management system** that documents (policies/procedures) the Provider's strategy for compliance with requirements
- **Duty to disclose** to regulators if Provider becomes aware the high-risk AI system presents a risk to health, safety or fundamental rights
  - Providers have post-market monitoring and reporting obligations

Obligations on Users of High-Risk AI Systems

- Use the AI system in accordance with its **instructions for use**
- If controlling **input data**, ensure it is relevant to the intended purpose of the AI system
- **Monitor the operation** of the AI system
  - Inform the provider and suspend use of system if reason to believe use presents risks to health, safety or fundamental rights

Transparency Requirements for Certain AI Systems

- AI systems intended to **interact with natural persons**
  - Providers must ensure system designed such that natural persons are informed they are interacting with an AI system
- **Emotion recognition** or **biometric categorization** systems
  - Users must inform natural persons exposed to the system of the operation of the system
- **"Deep Fakes"**
  - Users must disclose that the content has been artificially generated or manipulated

Low-Risk AI Systems – Voluntary Codes of Conduct

➢ Voluntary Codes of Conduct

- To be "encouraged and facilitated" by the EU Commission, Member States and the European Artificial Intelligence Board

➢ Intended to foster voluntary application of:

- The same requirements applicable to high-risk AI systems
- Commitments related to, *e.g.*, environmental sustainability, accessibility for persons with disabilities, diversity of development teams, etc.

Governance

➢ Establishes a "European Artificial Intelligence Board"

- Expert body providing advice/assistance to the EU Commission and national supervisory authorities
- Contributes to cooperation between and adoption of uniform administrative practices across Member States

➢ National Supervisory Authorities

- Each Member State to designate national supervisory authorit(ies) to implement regulation, act as notifying and market surveillance authority and to serve on European AI Board
- Expected to be existing data protection supervisors

Penalties for Non-Compliance

- Infringement of **prohibited** AI practices:
  - Fines of up to 30,000,000 EUR or 6% of total worldwide annual turnover

- Infringement of **data and data governance** requirements for high-risk AI systems:
  - Fines of up to 30,000,000 EUR or 6% of total worldwide annual turnover

- Non-compliance of AI system with **any other** requirement:
  - Fines of up to 20,000,000 EUR or 4% of total worldwide annual turnover