



EU AI Act

Conformity requirements for high risk systems

Lecture 2: Overview of the Act

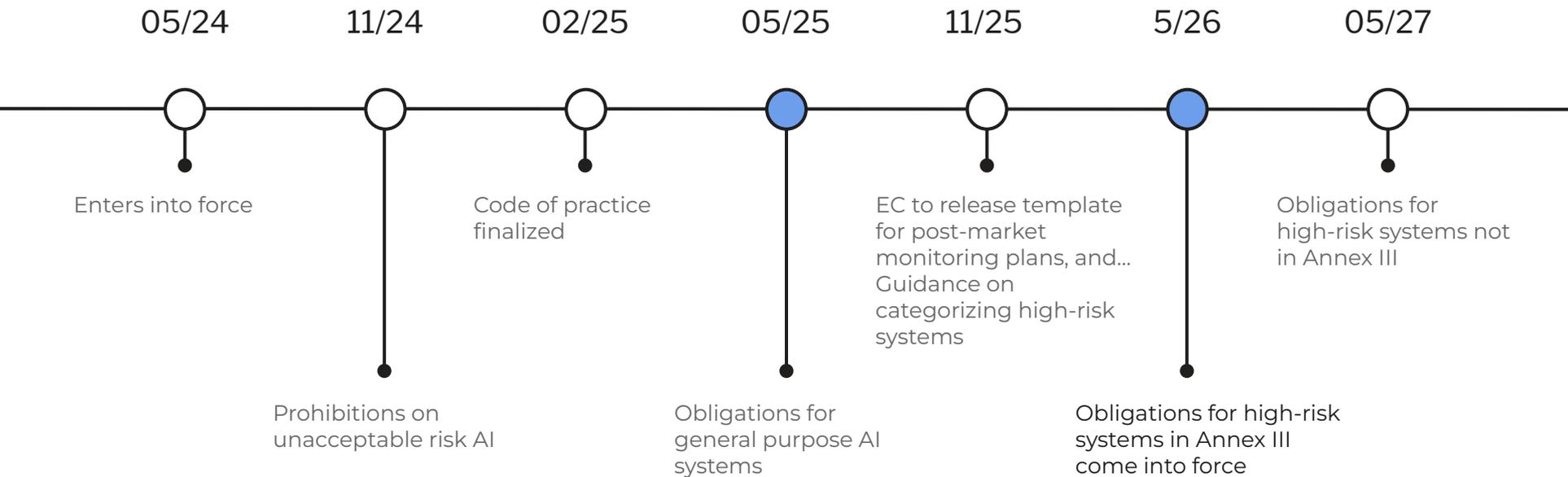
THE
ALGORITHMIC
BIAS LAB

babl

Overview

- Comprehensive regulation aimed at ensuring the safe and ethical development and deployment of AI within the EU.
- Risk-based approach
 - Unacceptable risk,
 - High risk
 - Limited risk (unofficial)
 - Minimal risk (unofficial)
- Requirements on high-risk AI
- General Purpose AI (GPAI) also subject to transparency and reporting requirements

EU AI Act Timeline

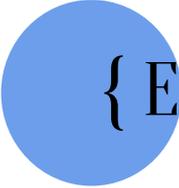


Scope of the Act

Article	Term	Definition
3.1	AI system	'AI system' means a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;
3.2	Provider	'Provider' means a natural or legal person, public authority, agency or other body that develops an AI system or a general purpose AI model or that has an AI system or a general purpose AI model developed and places them on the market or puts the system into service under its own name or trademark, whether for payment or free of charge;
3.3	Deployer	'Deployer means any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity;
3.44.b	General Purpose AI	'General purpose AI model' means an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications. This does not cover AI models that are used before release on the market for research, development and prototyping activities.

Risk Categorisation

Article	Category	Criteria
5	Prohibited AI Practices:	<ul style="list-style-type: none"> • Deploying subliminal techniques beyond a person's consciousness. • Exploiting vulnerabilities due to age, physical or mental disability, or social status. • Creating or expanding facial recognition databases through untargeted scraping • Providing social scoring of individuals s. • Predictive policing
6, Annex III	High-Risk AI Systems	<ul style="list-style-type: none"> • Intended as safety components of products or are themselves products undergoing third-party conformity assessment. • Used in predefined areas specified in the regulation (e.g., biometric identification, management of critical infrastructure, education, employment, essential private and public services, law enforcement, etc.).
52	Limited Risk AI Systems	<ul style="list-style-type: none"> • Does not qualify as high-risk but still pose requires disclosures.
Recital 81	Minimal Risk AI System	<ul style="list-style-type: none"> • All other AI systems that do not fall under the prohibited or high-risk categories. • Allowed to be developed and used according to the discretion of the provider, as long as they comply with the Act's provisions.



{ EU AI Act }

There are a large number of requirements for providers (developers) and deployers (users) of high-risk AI systems

- Quality Management System
 - Risk Management System
- Data Governance
- Technical Documentation
- Record Keeping
- Transparency
- Oversight
- Accuracy & Robustness
- Post Market Monitoring



The goal of this course is NOT to present a full legal reading of the Act, but rather to prepare risk, legal, and compliance professionals to develop and oversee critical compliance efforts required for high-risk AI systems.

The focus will be on practical implementation strategies.



Next: Risk Categorization

THE
ALGORITHMIC
BIAS LAB

babl