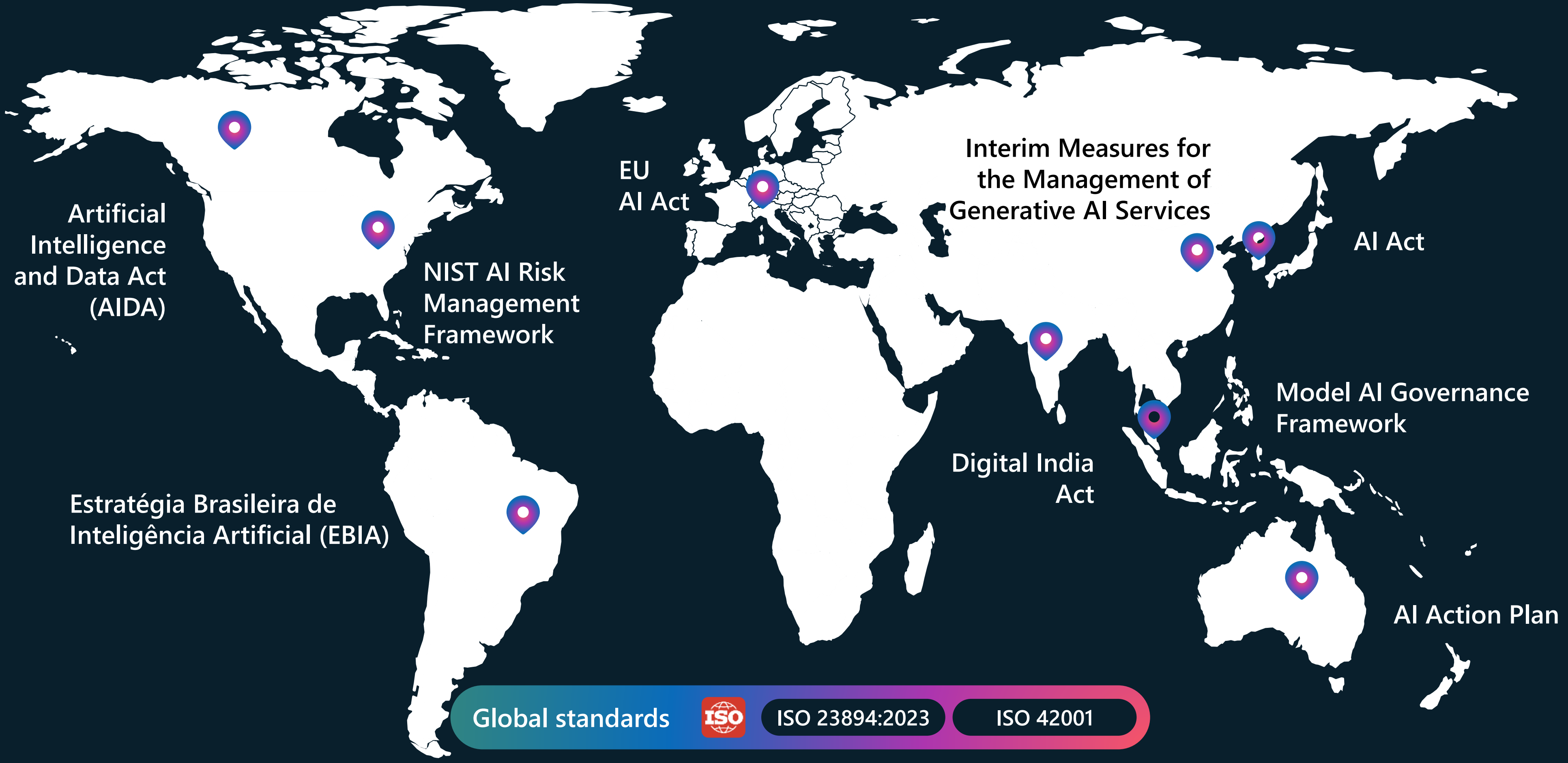
EU AI Act – Overview

Author: Ioana Tanase

AI Legislation landscape



Artificial Intelligence and Data Act (AIDA)

NIST AI Risk Management Framework

EU AI Act

Interim Measures for the Management of Generative AI Services

AI Act

Model AI Governance Framework

Digital India Act

Estratégia Brasileira de Inteligência Artificial (EBIA)

AI Action Plan

Global standards ISO ISO 23894:2023 ISO 42001

EU AI Act

EU AI Act applies to (TL/DR: *all*):

- Deployers within the EU
- Providers selling AI systems or general-purpose AI models in the EU, regardless of their location
- Importers and distributors in the EU market
- Product manufacturers for AI systems under their name or trademark in the EU
- Providers and deployers whose AI system outputs are used in the EU
- Persons in the EU affected by AI systems

Timeline:

- February 2, 2025: Obligations for prohibited AI systems
- August 2, 2025: Obligations for general-purpose AI models
- August 2, 2026: Most obligations (including high-risk AI systems)
- August 2, 2027: Other obligations for high-risk systems

Risk based approach to AI systems:

Unacceptable systems that are banned

High with strict regulations

Limited with lighter transparency obligations

Minimal and mostly unregulated

Prohibited AI Systems

Exploitation of vulnerable persons

Social scoring

Emotion inference in sensitive areas

Biometric data misuse

Untargeted facial recognition

Real-time remote biometric identification in public spaces for law enforcement (generally prohibited)

High risk AI Systems

Cat 1: AI used in machinery, toys, lifts, medical devices, and vehicles.

Cat 2:

- Biometrics
- Critical infrastructure
- Education
- Employment
- Essential services
- Credit evaluation
- Additionally, certain AI systems used in law enforcement, migration, asylum, border management, justice administration, and democratic processes

High risk systems obligations

Providers

- Implementing a risk management and quality management system
- Data governance and bias mitigation
- Maintaining technical documentation
- Record-keeping and traceability
- Ensuring human oversight and system accuracy
- Complying with registration and conformity assessment
- Providing contact information and affixing the "CE marking"

Deployers

- Assigning trained human oversight
- Ensuring relevant input data
- Informing impacted individuals and workers
- Conducting fundamental rights impact assessments for specific uses
- Providing explanations of AI's role in decision-making

Systems with transparency requirements

AI systems that may mislead end-users:

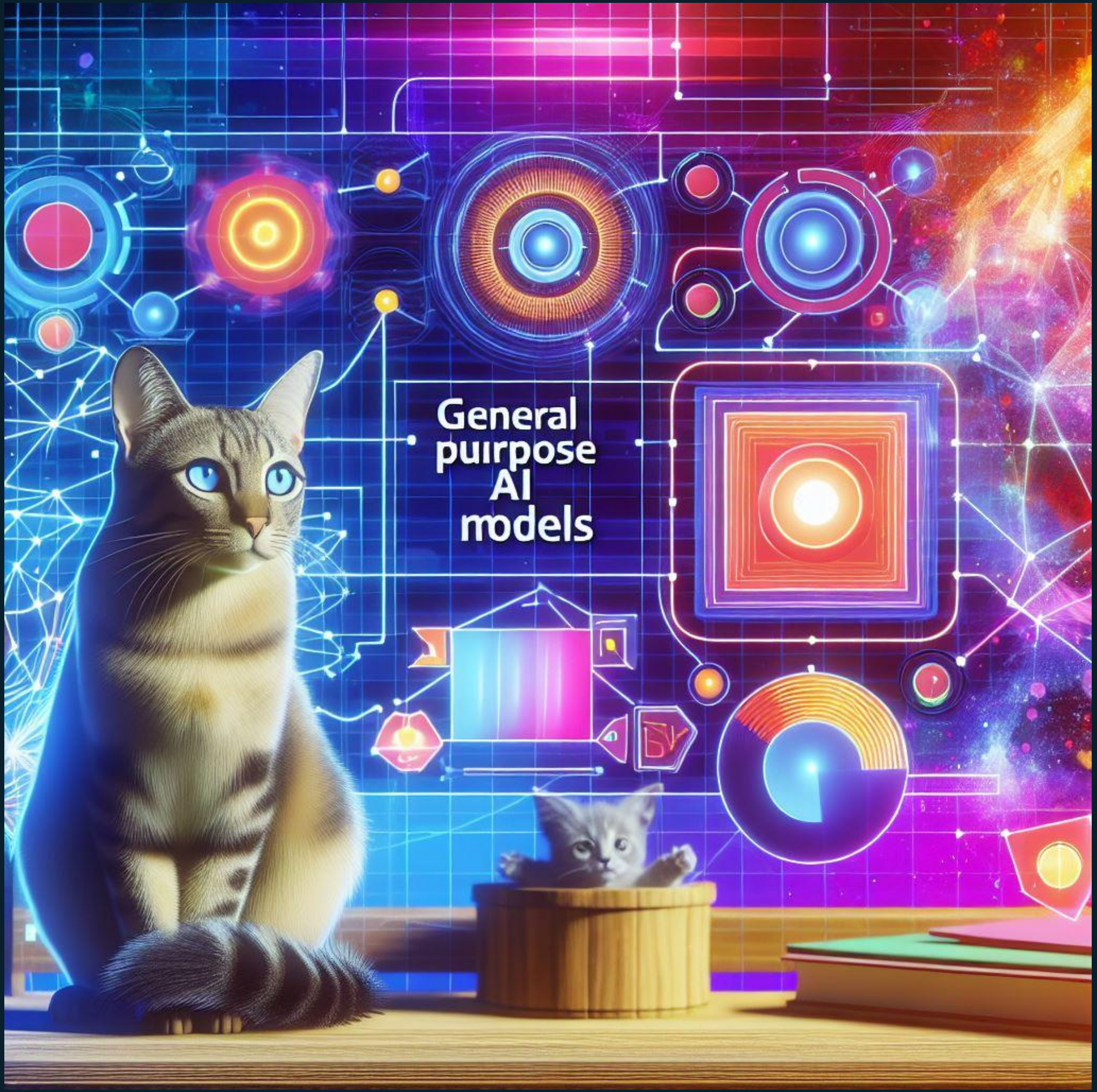
- AI systems interacting with individuals
- AI systems generating synthetic content
- Emotion recognition systems
- Biometric categorization systems
- Deep fake content generators
- Text generators informing the public

Obligations depending on system may include: disclosure requirements, labelling requirements, and transparency requirements with respect to the user

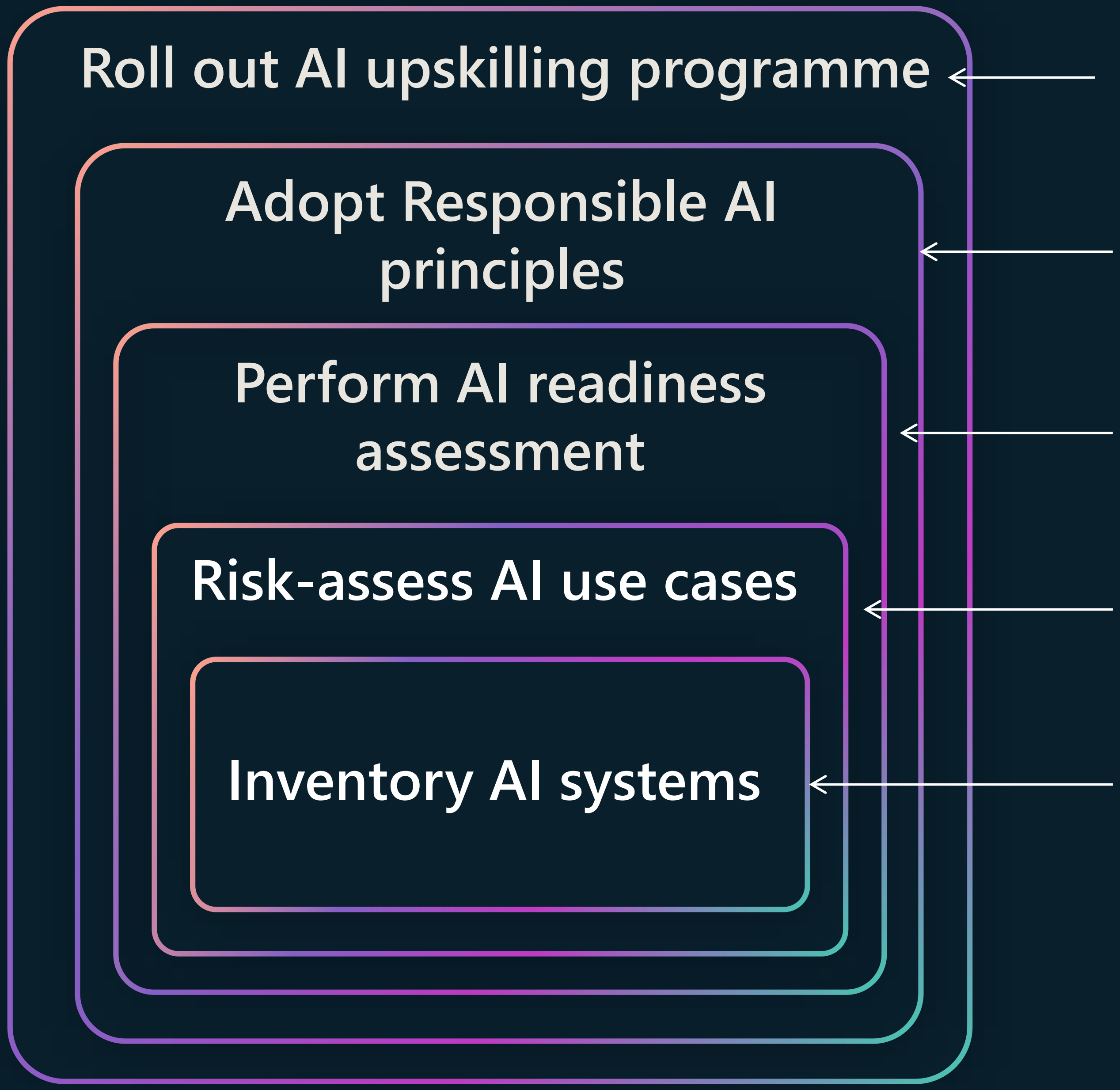
General purpose AI models

Obligations on providers:

- Keeping updated technical documentation, detailing training and testing processes, and providing it to authorities on request
- Providing up-to-date information for AI system providers who use these models
- Complying with EU copyright laws.
- Publishing a summary of the content used for model training.
- Models posing systemic risks face stricter requirements, such as ensuring cybersecurity and assessing risks at an EU level. Currently, only the most advanced models are considered potentially systemic risks.



Holistic measures to consider



Roll out AI upskilling programme

Educate your workforce on EU AI Act requirements and responsible AI principles to promote compliance and ethical practices.

Adopt Responsible AI principles

Apply ethical guidelines to ensure responsible AI development and use, aligned with laws and societal expectations.

Perform AI readiness assessment

Identify governance gaps and improvement areas by assessing AI capabilities and practices.

Risk-assess AI use cases

Evaluate each AI use case for compliance with the EU AI Act, focusing on risks and ethics.

Inventory AI systems

List all AI systems used in your organisation.

Penalties

Market Surveillance Authorities can impose significant fines under the AI Act for non-compliance:

- Up to €35 million or 7% of worldwide annual turnover for prohibited AI systems.
- Up to €15 million or 3% of worldwide annual turnover for most other obligations.
- Up to €7.5 million or 1% of worldwide annual turnover for supplying incorrect information.
- Additionally, the European Commission can fine providers of general-purpose AI models up to €15 million or 3% of worldwide annual turnover.

Complaints regarding AI Act infringements can be submitted to a Market Surveillance Authority.

Terminology

AI System == a machine-based system designed to operate with autonomy and adaptiveness, generating outputs like predictions, recommendations, or decisions based on the input it receives.

General-Purpose AI Mode -= performs various tasks competently, is integrated into different systems or applications, and is not limited to research or prototyping activities.

Provider == An entity that develops or markets an AI system or model, placing it on the market or putting it into service under its own name or trademark.

Deployer == An entity using an AI system under its authority, except when used for personal non-professional activities.