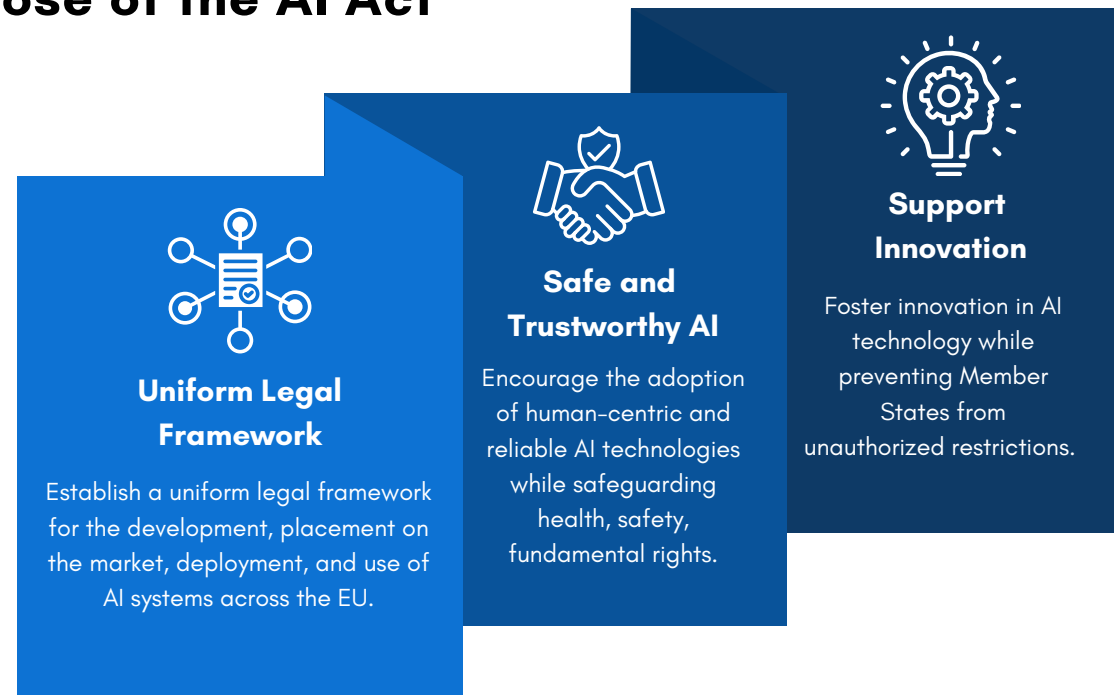
AddTrust | AI Act Compliance

EU AI ACT CHEAT SHEET

Purpose of the AI Act [1]



Organizations within Scope [2]

1 Provider

A natural or legal person, public authority, agency or other body that..

- Develops an AI system or a general-purpose AI model.
- Places an AI system on the market or puts into service in EU/EEA.

2 Importer

A natural or legal person that is..

- Located or established in the EU that places an AI system on the EU market.

3 Distributor

A natural or legal person in the supply chain, other than provider or importer that..

- Makes an AI system available on the Union market, as part of the supply chain.

4 Deployer

A natural or legal person, public authority, agency or other body that..

- Uses an AI system under its authority.

Implementation Timeline [3]

2 Feb. 2025

Prohibitions and general provisions of the regulation on unacceptable-risk AI are applied.

2 Aug. 2025

Obligations for general-purpose AI (GPAI) models will come into effect.

2 Aug. 2026

Main body of the regulation will be effective, except for certain provisions related to high-risk AI systems.

2 Aug. 2027

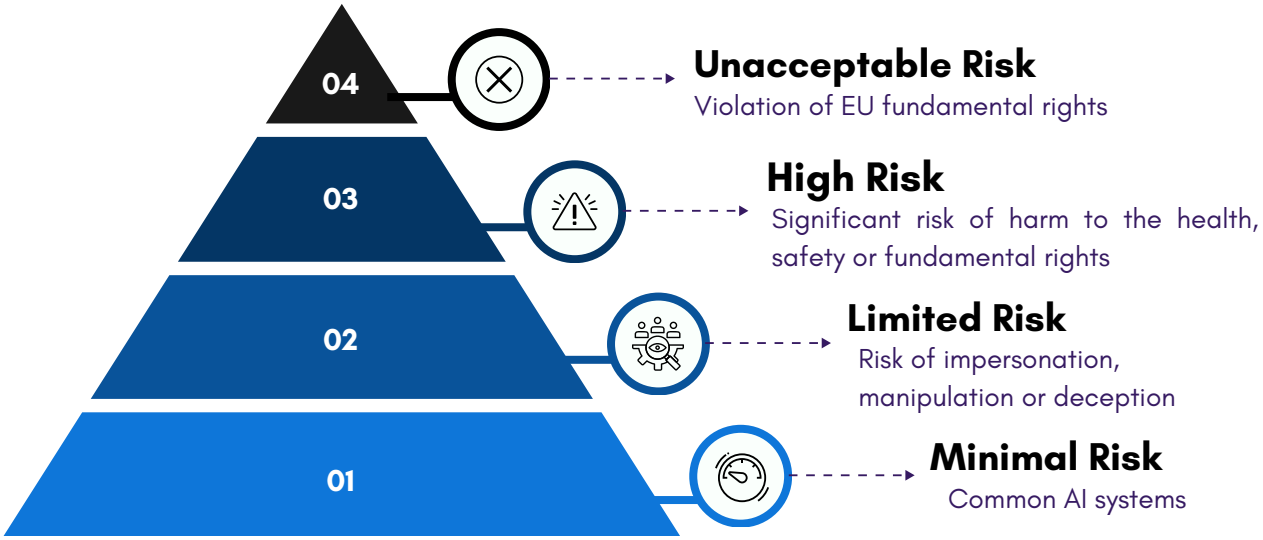
Obligations imposed on high-risk AI systems become applicable.

1. EU AI Act, Article 1. 2. EU AI Act, Article 3 (3), (4), (6), (7). 3. EU AI Act, Article 113.

Updated January 2025

AddTrust disclaims all warranties, expressed or implied, with respect to the contents of this material, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.

Artificial Intelligence System Risk Hierarchy [1]

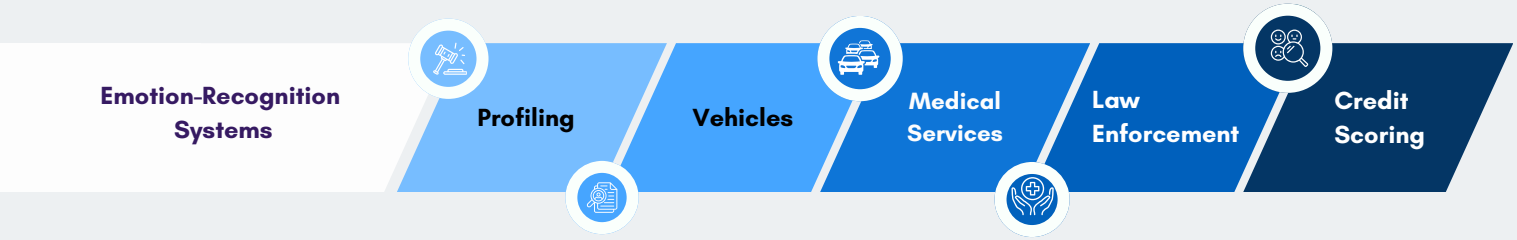


High-Risk AI System [2]

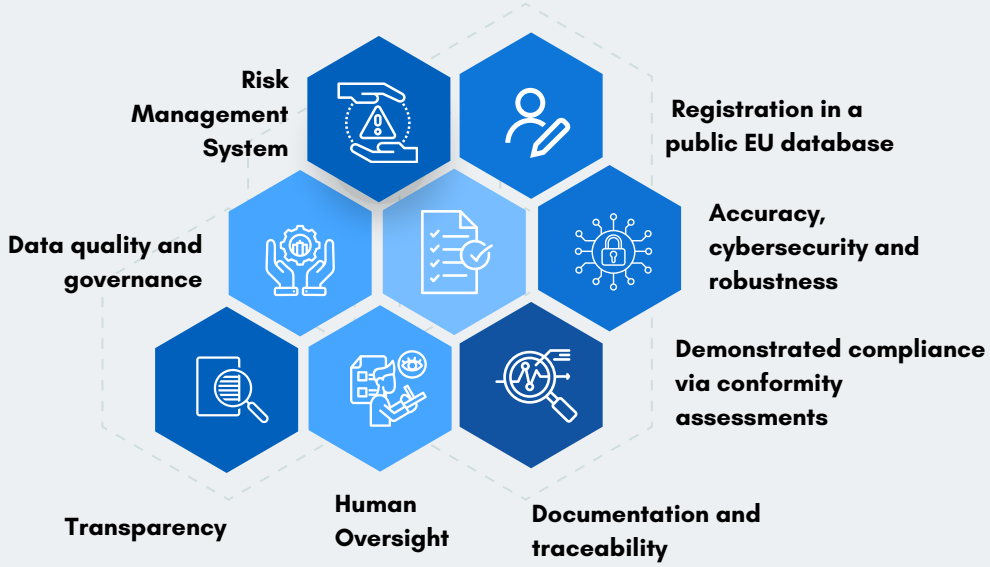
What is High-Risk AI System?

a) AI systems that pose a significant risk of harm to the fundamental rights of natural persons, covering six areas below.

b) Required to undergo third-party conformity assessment.



Key Requirements for High-Risk AI System [3]



1. KPMG, Decoding the EU AI Act, p. 13. 2. EU AI Act, Article 6 (3) & IAPP EU AI Act 101 Overview, p. 2.
3. IAPP EU AI Act 101 Overview, p. 3.

Updated January 2025

AddTrust disclaims all warranties, expressed or implied, with respect to the contents of this material, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.

Prohibited AI Practices [1]

Manipulative and Subliminal AI

AI systems that manipulate or deceive individuals beyond their conscious awareness.

Exploitation of Vulnerabilities

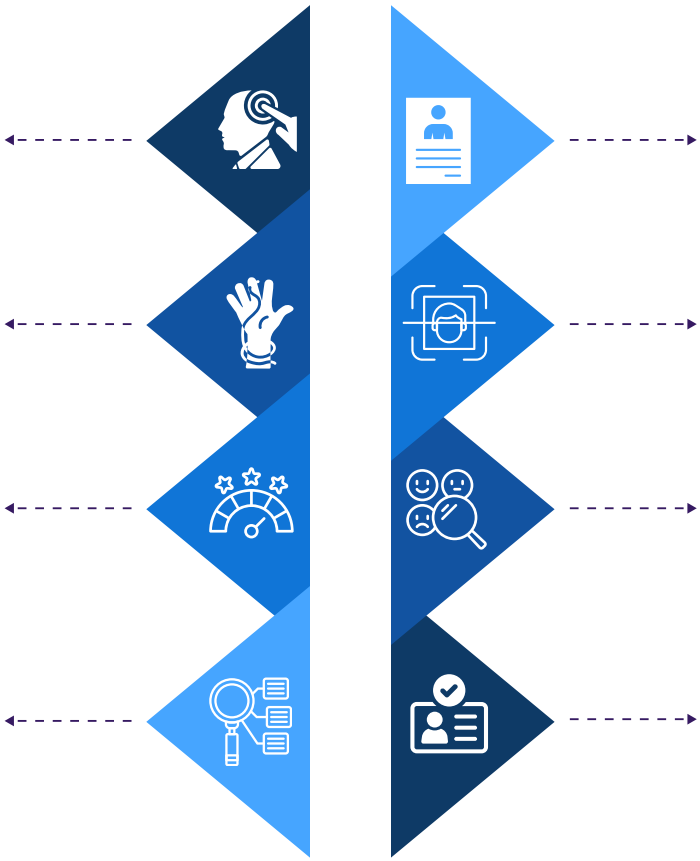
AI systems exploiting vulnerabilities due to age, disability, or socio-economic situations to distort behavior.

Social Scoring AI

AI systems classifying individuals based on social behavior, causing unrelated negative treatment.

Biometric Categorization

AI systems categorizing individuals based on biometric data to deduce sensitive attributes.



Predictive Criminal Profiling

AI systems solely profiling individuals to predict criminal behavior.

Facial Recognition Database Expansion

AI systems expanding facial recognition databases via untargeted image scraping.

Emotion Recognition in Workplace and Education

AI systems inferring emotions in workplaces or educational institutions.

Real-Time Remote Biometric Identification in Public Spaces

Transparency Requirements [2]

Transparency requirements are the requirements for "limited risk" classified AI systems.

Providers

Providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are **informed that they are interacting with an AI system.**

Providers of AI systems, including general-purpose AI systems, shall **ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated.**

Deployers

Deployers of an emotion recognition system or a biometric categorisation system shall **inform the natural persons exposed thereto of the operation of the system.**

Deployers of an AI system that generates or manipulates image, audio or video content constituting a deep fake, shall **disclose that the content has been artificially generated or manipulated.**

1. EU AI Act, Article 6 (1) & Annex III. 2. EU AI Act, Article 50 (1)-(4).

Updated January 2025

AddTrust disclaims all warranties, expressed or implied, with respect to the contents of this material, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.

General-Purpose AI Models (GPAI) [1]

What is GPAI?

AI models that display significant generality and are capable of competently **performing a wide range of distinct tasks**, regardless of how they are placed on the market, and that can be integrated into a variety of downstream systems or applications. **The greater testing and reporting requirements are imposed on GPAI with systemic risk.**

Key Requirements for Providers of GPAI [2]

- Perform * **FRIAs** and conformity assessments.
- Implement **risk management and quality management systems** to continually assess and mitigate systemic risks.
- **Inform individuals** when they interact with AI. AI content must be labelled and detectable.
- **Test and monitor for accuracy**, robustness and cybersecurity.

* FRIAs: Fundamental Rights Impact Assessment

General-Purpose AI Models with Systemic Risks [3]

What is GPAI with Systemic Risks?

GPAI models that pose significant large-scale threats to society or the economy.

GPAI with Systemic Risks should meet either of these conditions:

1. Has high-impact capabilities evaluated using appropriate technical tools and methodologies.
2. It is determined by the European Commission to have capabilities or impact equivalent to those with high-impact capabilities.

Key Requirements for GPAI Models with Systemic Risks [4]

Model Evaluation
Conduct model evaluation using standardized protocols.

Risk Assessment
Assess and mitigate possible systemic risks at Union level.

Cybersecurity Protection
Ensure an adequate level of cybersecurity protection.

Codes of Practice
Rely on codes of practice.

Confidentiality Obligations
Documentation shall be treated in accordance with confidentiality obligations.

Documenta-tion
Promptly report serious incidents and corrective measures.

1. EU AI Act, Article 3 (63). 2. IAPP EU AI Act 101 Overview, p. 3. 3. https://artificialintelligenceact.eu/article/51/ **Updated January 2025**
4. https://artificialintelligenceact.eu/article/55/

AddTrust disclaims all warranties, expressed or implied, with respect to the contents of this material, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.

Regulators

Each Member State must designate at least one notifying authority and one market surveillance authority, which must operate independently and impartially to enforce the Regulation effectively. [1]

For **high-risk AI systems** used by financial institutions, **the relevant national financial supervision authority will act as the market surveillance authority** under this Regulation. [2]

Enforcement Powers & Penalties

The market surveillance authorities shall report annually to the Commission about the use of prohibited practices that occurred during that year and about the measures taken. [3]

Prohibited Practices [4]

(i) The AI system does not comply with the requirements and obligations laid down in this Regulation.

(ii) Although a high-risk AI system complies with this Regulation, it nevertheless presents a risk to the health or safety of persons, to fundamental rights, or to other aspects of public interest protection.

Penalties [5]

Prohibited AI Violation	Misleading Information to Authority	Other Violations
Up to 7%a of global annual turnonver or 35 million euros	Up to 1% of global annual turnonver or 7.5 million euros	Up to 3% of global annual turnover or 15 million euros

Major challenges by the AI Act [6]

- Protecting the fundamental rights to the privacy through sustainable data processing
- Fostering development and innovation of AI ecosystem
- Understanding the relationship between the AI Act and the existing regulations governing AI systems
- Managing the evolving network of stakeholders involved in supervision and enforcement
- Establishing suitable multidisciplin-ary governance frameworks within organizations

1. EU AI Act, Article 70 (1). 2. EU AI Act, Article 74 (6). 3. EU AI Act, Article 74 (2). 4. EU AI Act, Article 79 (2) & 82 (1).
5. EU AI Act, Article 99 (3)-(5). 6. IAPP EU AI Act 101 Overview, p. 1.

Updated January 2025

AddTrust disclaims all warranties, expressed or implied, with respect to the contents of this material, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.