EU AI Act

The complete reference guide to Regulation (EU) 2024/1689

Table des matières

1. Introduction

1.1 Context: Why the European Union Regulates AI

Artificial intelligence is profoundly transforming our societies, economies, and ways of life. Faced with this technological revolution, the European Union has chosen to establish a harmonized regulatory framework rather than leaving each Member State to legislate individually.

This approach is consistent with the European digital strategy, which includes the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), and the Digital Markets Act (DMA).

The main motivations for this regulation are:

- **Protection of fundamental rights**: Preventing algorithmic discrimination and protecting human dignity
- **Safety of persons**: Ensuring that AI systems integrated into products do not endanger health and safety
- **Internal market harmonization**: Creating a uniform framework for the 27 Member States, avoiding regulatory fragmentation
- **European competitiveness**: Establishing a global standard that the EU can export (the "Brussels Effect")

1.2 Objectives of the Regulation

The AI Act pursues several complementary objectives, explicitly stated in its recitals:

1.3 Geographic and Extraterritorial Scope

The AI Act has a **significant extraterritorial scope**. It applies to:

1. **Providers** established in the EU or in a third country, who place on the market or put into service AI systems in the Union

2. **Deployers** of AI systems located in the Union

3. **Providers and deployers** located in a third country, when the output produced by the AI system is used in the Union

4. **Importers and distributors** of AI systems

5. **Product manufacturers** who place on the market or put into service an AI system with their product under their own name or trademark

> *"Any company, regardless of its location, that markets AI systems intended for the European market or whose outputs are used in the EU must comply with the AI Act."*

2. Timeline and Legal Framework

2.1 Genesis of the Regulation (2021-2024)

The development of the AI Act was a multi-year legislative process:

2.2 Phased Implementation Timeline

The regulation adopts a **staggered implementation** over three years, allowing stakeholders to adapt progressively:

DATE	TIMEFRAME	APPLICABLE PROVISIONS
February 2, 2025	6 months	**Prohibited practices** (Article 5) **AI literacy** (Article 4)
August 2, 2025	12 months	**GPAI obligations** (Chapter V) **Governance**: Designation of national authorities Codes of practice for GPAI models
August 2, 2026	24 months	**High-risk systems** (Annex III) **Provider and deployer obligations** **Penalty regime** (Article 99) Majority of provisions
August 2, 2027	36 months	**High-risk systems in regulated products** (Annex I) Medical devices, machinery, vehicles, aircraft Full GPAI compliance (models predating August 2025)
Dec. 31, 2030	6+ years	**Large-scale IT systems** (Annex X) Existing systems placed on the market before this date

3. Risk Classification

The AI Act introduces a **risk-based pyramid approach**. Four levels are defined, each with proportionate obligations:

> Unacceptable Risk
> PROHIBITED

High Risk
REGULATED
Limited Risk
TRANSPARENCY

> Minimal Risk
> UNREGULATED

3.1 Unacceptable Risk – Prohibited Practices (Article 5)

The regulation **prohibits** eight categories of AI systems considered to infringe on fundamental rights or human dignity. These prohibitions have been **effective since February 2, 2025**.

3.2 High Risk – Regulated Systems (Articles 6-49)

High-risk AI systems represent the core of the regulation. They are subject to **strict obligations** before being placed on the market and throughout their lifecycle.

CATEGORY 1: SAFETY COMPONENTS OF REGULATED PRODUCTS (ANNEX I)

AI systems constituting a **safety component** of a product covered by Union harmonization legislation, including:

- Machinery and industrial equipment
- Toys
- Lifts
- Pressure equipment
- Medical devices and in vitro diagnostic medical devices
- Vehicles (type approval)
- Aircraft and air traffic management systems
- Marine equipment
- Railway equipment

CATEGORY 2: SENSITIVE AREAS (ANNEX III)

AI systems deployed in **high-impact areas** on fundamental rights:

3.3 Limited Risk – Transparency Obligations (Article 50)

Certain AI systems present a **risk of deception** but are not considered high-risk. They are subject to **transparency obligations**:

- **Chatbots and conversational agents**: Users must be informed that they are interacting with an AI (unless obvious from the circumstances)
- **Emotion recognition systems**: Information to affected persons (except prohibited cases)
- **Biometric categorization systems**: Information to persons (except prohibited cases)
- **Deepfakes and generated content**: Clear marking that content (image, audio, video, text) has been generated or manipulated by AI

3.4 Minimal Risk – Unregulated

The vast majority of AI systems fall into this category and are **not specifically regulated** by the AI Act. Examples:

- AI-powered video games
- Spam filters
- Content recommendation systems
- Translation assistants
- Industrial optimization tools

4. General-Purpose AI Models (GPAI)

General-Purpose AI models (GPAI) are covered by a dedicated chapter (Chapter V), added during final negotiations to address the emergence of systems like ChatGPT, Claude, Gemini, or DALL-E.

4.1 Definition

A GPAI model is defined as:

> *"An AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing 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."*

Examples: GPT-4, Claude, Gemini, LLaMA, Mistral, DALL-E, Midjourney, Stable Diffusion.

4.2 Obligations for GPAI Model Providers

All GPAI model providers must, **as of August 2, 2025**:

1. **Prepare and maintain technical documentation** of the model and its training process
2. **Establish and document a compliance policy** with EU copyright law
3. **Publish a detailed summary** of the content used for model training
4. **Provide information and documentation** to downstream providers integrating the model
5. **Designate a representative** in the Union (for non-EU providers)

4.3 GPAI Models with Systemic Risk

A GPAI model presents **systemic risk** when:

Providers of GPAI models with systemic risk must, **in addition to** general obligations:

- **Perform model evaluations** according to standardized protocols and tools
- **Conduct adversarial testing** to identify and mitigate systemic risks
- **Track, document, and report** serious incidents to the AI Office and national authorities
- **Ensure adequate cybersecurity** for the model and its infrastructure
- **Notify the Commission** within 2 weeks if their model reaches the systemic risk threshold

5. Obligations by Actor

The AI Act distinguishes several categories of actors in the AI value chain, each with specific obligations.

5.1 Providers (Developers)

Providers are natural or legal persons who develop or have an AI system developed with a view to placing it on the market or putting it into service under their own name or trademark.

OBLIGATIONS FOR HIGH-RISK SYSTEMS:

1 **Risk management system (Article 9)**
Establish, implement, document, and maintain a risk management system throughout the AI system lifecycle.

2 **Data governance (Article 10)**
Ensure that training, validation, and testing datasets are relevant, representative, error-free, and complete.

3 **Technical documentation (Article 11)**
Prepare technical documentation demonstrating system compliance before placing it on the market.

4 **Logging (Article 12)**
Design the system to enable automatic recording of events (logs) throughout its operation.

5 **Transparency (Article 13)**
Design the system to allow deployers to understand its operation and interpret its outputs.

6 **Human oversight (Article 14)**
Design the system to enable effective human oversight during its use.

7 **Accuracy, robustness, and cybersecurity (Article 15)**
Ensure that the system achieves an appropriate level of accuracy, robustness, and cybersecurity.

5.2 Deployers (Users)

Deployers are natural or legal persons using an AI system under their own authority (excluding personal non-professional use).

MAIN OBLIGATIONS:

- **Compliant use**: Use the system in accordance with the instructions provided by the provider
- **Human oversight**: Ensure that human oversight is exercised by competent and authorized persons
- **Input data**: Ensure that input data is relevant to the system's purpose
- **Operational monitoring**: Monitor system operation and suspend use in case of malfunction
- **Log retention**: Retain automatically generated logs (minimum 6 months)

- **Information to individuals**: Inform affected persons that they are subject to a decision made by a high-risk system
- **Fundamental rights impact assessment**: Conduct an impact assessment before deployment (for certain deployers)

5.3 Cross-Cutting Obligation: AI Literacy (Article 4)

Effective since February 2, 2025, the AI literacy obligation applies to all providers and deployers:

6. Governance and Enforcement

The AI Act establishes a **multi-level governance architecture** combining European and national oversight.

6.1 At the European Level

THE AI OFFICE

Established within the European Commission, the AI Office is responsible for:

- Supervising GPAI models and models with systemic risk
- Developing guidelines and codes of practice
- Coordinating with national authorities
- Enforcing rules on GPAI model providers

THE EUROPEAN ARTIFICIAL INTELLIGENCE BOARD (AI BOARD)

Composed of Member State representatives, it:

- Advises and assists the Commission
- Contributes to consistent application of the regulation
- Coordinates national authorities
- Issues recommendations and opinions

6.2 At the National Level

Each Member State was required to **designate at least one competent authority** by August 2, 2025:

- **Notifying authority**: Responsible for designating and monitoring notified bodies
- **Market surveillance authority**: Responsible for market monitoring and regulation enforcement

7. Penalties and Sanctions

The AI Act provides for a **tiered administrative penalty regime** (Article 99), applicable from August 2, 2025.

7.1 Fine Structure

7.2 Other Consequences

Beyond fines, authorities may:

- **Order withdrawal from the market** or recall of a non-compliant system
- **Prohibit the deployment** of an AI system
- **Require corrective measures** within a set timeframe
- **Publish non-compliance decisions** (name and shame)

8. Sectoral Impact

The AI Act has differentiated implications across industry sectors. This section analyzes the four most impacted sectors.

8.1 Human Resources and Recruitment

The HR sector is **particularly affected** by the AI Act, with most AI applications in this area classified as **high-risk**.

HIGH-RISK SYSTEMS:

- CV screening and scoring tools
- Candidate-job matching systems
- Video interview analysis tools
- Performance evaluation systems
- Task and schedule allocation tools
- Promotion or termination decision systems

PROHIBITED PRACTICES IN HR:

- **Emotion recognition** in the workplace (except medical/safety reasons)
- **Social scoring** of employees
- **Invasive biometric surveillance**

8.2 Healthcare and Medical Devices

The healthcare sector combines two regulatory frameworks: the AI Act and the **Medical Devices Regulation** (MDR 2017/745).

HIGH-RISK SYSTEMS:

- Diagnostic assistance systems (medical imaging, pathology)
- Patient triage tools
- Treatment recommendation systems
- Medical devices incorporating AI
- Emergency prioritization systems

8.3 Finance and Insurance

The financial sector extensively uses AI for risk assessment, placing it within the high-risk scope.

HIGH-RISK SYSTEMS:

- **Credit scoring** and creditworthiness assessment
- AI-based **insurance pricing** (except motor insurance)
- Fraud detection systems affecting access to services
- Risk assessment for mortgages

8.4 Education

AI in education is classified as **high-risk** due to its potential impact on learners' life trajectories.

HIGH-RISK SYSTEMS:

- Admission systems (Parcoursup-like algorithms)
- Automated exam grading
- Learning assessment and pathway recommendations
- Exam proctoring systems

- Plagiarism detection with decisional implications

9. International Comparison

The AI Act is part of a **global race to regulate AI**. Approaches vary significantly across jurisdictions.

9.1 The Brussels Effect

Like the GDPR, the AI Act could generate a **Brussels Effect** – the tendency of global companies to align their practices with European standards to access the single market.

10. Practical Recommendations

This section presents a **compliance checklist** for organizations preparing for the AI Act.

10.1 Immediate Actions (Already Applicable)

- [ ] **Audit of prohibited practices**
  Verify that no prohibited AI system (social scoring, emotion recognition at work, etc.) is being used.

- [ ] **AI literacy program**
  Train staff using or overseeing AI systems.

10.2 Short-Term Actions (Before August 2026)

- [ ] **AI system inventory**
  Catalog all AI systems used or developed by the organization.

- [ ] **Risk classification**
  Classify each system according to AI Act categories (prohibited, high-risk, limited, minimal).

- [ ] **Gap analysis**
  Identify gaps between current practices and AI Act requirements.

11. Conclusion

Regulation (EU) 2024/1689 on artificial intelligence represents a **major regulatory advancement** on a global scale. As the first comprehensive legal framework on AI, it strikes a balance between protecting fundamental rights and preserving innovation.

Key Takeaways

1. **Risk-based approach**: Obligations are proportionate to the AI system's risk level
2. **Phased implementation**: From February 2025 (prohibited practices) to December 2030 (large-scale IT systems)

3. **Extraterritorial scope**: Any organization affecting users in the EU is covered
4. **Significant penalties**: Up to €35 million or 7% of global turnover
5. **Multi-level governance**: Coordination between the European AI Office and national authorities

> *"The AI Act is not an end in itself, but the beginning of a process of regulating artificial intelligence that will evolve with technology."*

12. Appendices

Glossary

AI System
A machine-based system designed to operate with varying levels of autonomy, 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.
Provider
A natural or legal person who develops an AI system or a GPAI model, or has an AI system or a GPAI model developed, and places it on the market or puts the AI system into service under its own name or trademark.
Deployer
A natural or legal person using an AI system under its own authority, except where the AI system is used in the course of a personal non-professional activity.
GPAI (General-Purpose AI)
A general-purpose AI model capable of competently performing a wide range of distinct tasks, regardless of the way it is placed on the market.
Systemic Risk
A risk specific to the high-impact capabilities of GPAI models, having a significant effect on the Union market due to their reach, or actual or reasonably foreseeable negative effects on public health, safety, fundamental rights, or society.
Regulatory Sandbox
A controlled framework established by a competent authority enabling the development, training, and validation of innovative AI systems for a limited time before placing them on the market.

Official Resources

- Official text of the Regulation (EUR-Lex)
- EU AI Act Portal (analysis and summaries)
- European Commission - AI Regulatory Framework
- Official Implementation Timeline

Summary Timeline

Document: White Paper – EU AI Act: The Complete Reference Guide

Version: 1.0

Publication date: January 20, 2026

Author: JAIKIN

This document is provided for informational purposes and does not constitute legal advice. For any specific questions regarding AI Act compliance, please consult a qualified legal advisor.