EU AI Act Risk Classification Decision Tree

Type: Decision Tree

Target Audience: AI Developers, Compliance Officers, Product Managers

This decision tree helps determine which of the four EU AI Act risk tiers your AI system falls into. Work through each step sequentially to identify your compliance obligations.

Step 1: Check Against Prohibited Practices (Article 5)

If your system performs any of these functions, it is **BANNED** in the EU:

☐ Social scoring by governments
☐ Subliminal manipulation causing harm
☐ Exploitation of vulnerabilities (age, disability)
☐ Real-time remote biometric ID in public spaces (limited exceptions)
☐ Emotion recognition in workplace/education (with exceptions)
☐ Biometric categorization inferring sensitive attributes
☐ Untargeted scraping for facial recognition databases

Result: If ANY box is checked → **PROHIBITED** (Cannot be deployed in EU)

Step 2: Check Annex I - Safety Components

Is your AI a safety component of, or itself a regulated product under EU harmonization legislation?

Product Category	Examples
Medical Devices	AI-assisted diagnostics, surgical robots
Vehicles	Autonomous driving systems, ADAS
Aviation	Air traffic management AI, drone systems
Machinery	Industrial robots, automated equipment
Toys	AI-enabled interactive toys
Marine Equipment	Navigation AI, safety systems

Result: If YES → **HIGH-RISK** (Articles 9-15 requirements apply)

Step 3: Check Annex III - High-Risk Use Cases

Does your AI system fall into any of these high-risk categories?

Category	Specific Uses	Check
Biometric ID	Remote biometric identification systems	[ ]
Critical Infrastructure	Safety components in water, gas, electricity, traffic	[ ]
Education	Admissions, assessment, proctoring, learning analytics	[ ]
Employment	Recruitment, screening, evaluation, termination	[ ]
Essential Services	Credit scoring, insurance pricing, emergency dispatch	[ ]
Law Enforcement	Risk assessment, lie detection, evidence evaluation	[ ]
Migration/Border	Visa processing, asylum applications, border control	[ ]
Justice/Democracy	Sentencing assistance, election influence	[ ]

Result: If ANY box is checked → **HIGH-RISK**

Step 4: Check Transparency Obligations (Limited Risk)

Does your system require transparency disclosures?

- □ Chatbots or conversational AI (must disclose AI nature)
- □ Deepfakes/synthetic media (must label as AI-generated)
- □ Emotion recognition systems (must inform subjects)
- □ Biometric categorization (must inform subjects)
- □ AI-generated text on public interest matters (must label)

Result: If ANY box is checked → **LIMITED RISK** (Disclosure/labeling required)

Step 5: Default Classification

If your system does not fall into any of the above categories:

Result: **MINIMAL RISK** - No specific obligations, voluntary codes of conduct encouraged

Classification Summary

Risk Level	Obligations	Examples
PROHIBITED	Cannot be deployed in EU	Social scoring, manipulation
HIGH-RISK	Full compliance (Articles 9-15)	Hiring AI, credit scoring
LIMITED RISK	Transparency requirements	Chatbots, deepfakes
MINIMAL RISK	No requirements (voluntary)	Spam filters, games

AI System Name: ________________________________

Classification Result: [ ] Prohibited [ ] High-Risk [ ] Limited Risk [ ] Minimal Risk

Assessed By: _________________________ **Date:** ______________