Is Your AI System High-Risk?

Takes 2 minutes. Gives you clarity.

Start at Q1. Your first YES determines your risk category. If the answer is NO, continue to the next question.

1 **Does your AI do any of the 8 prohibited practices?**
e.g. social scoring, facial scraping, emotion recognition at work
Art. 5 | see p.2

YES → **BANNED**
Do not place on the EU market.

NO ↓

2 **Is your AI a safety component AND required to undergo third-party conformity assessment?**
e.g. medical devices, vehicles, machinery under Annex I product legislation
Art. 6(1)(a)+(b)

YES → **HIGH-RISK**
Full compliance required.

NO ↓

3 **Does your AI operate in a sensitive area? (see list below)**
e.g. hiring, credit scoring, policing, education, biometrics, migration
Art. 6(2), Annex III

YES → **HIGH-RISK***
Unless Art. 6(3) exception applies.

NO ↓

4 **Does your AI interact with people or generate content?**
e.g. chatbots, AI-generated images/video/text, deepfakes, voice synthesis
Art. 50

YES → **LIMITED RISK**
Transparency obligations apply.

NO ↓

MINIMAL RISK
No specific obligations under the AI Act.

* **Art. 6(3) exception. Annex III systems may be non-high-risk only if BOTH of these apply:**
(1) the system does NOT pose a significant risk of harm to health, safety, or fundamental rights,
(2) AND one of Art. 6(3)(a)–(d) applies: narrow procedural / improves prior human work / detects patterns without replacing human judgment / preparatory task.
Profiling is always high-risk. Documentation (Art. 6(4)) + EU database registration (Art. 49(2)) still required. See page 2.

THE 8 SENSITIVE AREAS (Question 3, Annex III)

1. **Biometrics**: facial recognition, emotion detection
2. **Critical infrastructure**: power, water, transport safety
3. **Education**: admissions, grading, assessment
4. **Employment**: recruitment, CV screening, monitoring
5. **Essential services**: credit scoring, insurance, benefits
6. **Law enforcement**: risk assessment, evidence evaluation
7. **Migration & borders**: visa risk, document verification
8. **Administration of justice**: research, interpretation, sentencing

WHAT TO DO NEXT

- **BANNED** Stop. Do not place on or use in the EU. Up to €35M or 7% of global turnover (Art. 99(3)).
- **HIGH-RISK** Full Art. 8–17 compliance. Up to €15M or 3% of global turnover (Art. 99(4)). See page 2.
- **LIMITED RISK** Disclose AI use. Label AI-generated content. Inform users of AI interaction (Art. 50).
- **MINIMAL RISK** No AI Act obligations. Voluntary codes of conduct encouraged. Monitor for regulatory changes.

Need templates for all of the above? The Enterprise AI Playbook Starter Pack covers it:
AI Governance Workbook, Decision Tree, Governance Policy, Enterprise Trust Pack, 30-Day Roadmap.

Detailed Reference

The 8 prohibited practices, the full Art. 6(3) exception, and the core high-risk obligations.

A. All 8 Prohibited AI Practices (Art. 5)

If any match your system, it is BANNED in the EU. No exceptions.

ART. 5(1)	PROHIBITED PRACTICE	TYPICAL USE CASE TO WATCH FOR
(a)	**Subliminal / manipulative / deceptive techniques**	dark patterns, hidden persuasion that materially distorts behaviour
(b)	**Exploitation of vulnerabilities**	targeting age, disability, social or economic situation
(c)	**Social scoring**	rating people by behaviour or traits for unrelated decisions
(d)	**Criminal risk assessment by profiling**	predicting offences based solely on personality / profiling
(e)	**Untargeted facial image scraping**	building face databases from internet or CCTV without consent
(f)	**Emotion recognition (workplace / education)**	inferring mood of employees or students (medical/safety exempt)
(g)	**Biometric categorisation by sensitive attributes**	inferring race, politics, religion, union, sexual orientation
(h)	**Real-time remote biometric identification**	live face recognition by law enforcement in public spaces (narrow exceptions)

B. Art. 6(3) Exception in Full

An Annex III system is NOT high-risk only if BOTH of these are true:

(1) The system does NOT pose a significant risk of harm to health, safety, or fundamental rights of natural persons; AND

(2) ONE of the following applies (alternative, not cumulative):

- **(a)** the system performs a narrow procedural task;
- **(b)** the system improves the result of a previously completed human activity;
- **(c)** the system detects decision-making patterns without replacing or influencing prior human assessment;
- **(d)** the system performs a preparatory task to an assessment relevant for Annex III purposes.

Even if the exception applies: Profiling is always high-risk.

Art. 6(4) still requires documenting the exception assessment. Art. 49(2) still requires EU database registration before market placement.

C. Core High-Risk Obligations (8 of 12)

If your system is HIGH-RISK, you need all of these. Four more are listed below.

OBLIGATION	ARTICLE	WHAT IT MEANS
Risk management system	Art. 9	ongoing, documented process across the system's life
Data governance	Art. 10	quality controls for training, validation, and test data
Technical documentation	Art. 11	full technical file as set out in Annex IV
Record-keeping / logging	Art. 12	automatic logs of events and usage
Transparency for deployers	Art. 13	written instructions for use
Human oversight	Art. 14	measures that let humans actually supervise the system
Accuracy, robustness, cybersecurity	Art. 15	kept at a sufficient level across the system's life
Conformity assessment	Art. 43	self-assessment, or notified body for biometrics

+ 4 further obligations to check:

Quality Management System (Art. 17) | EU database registration (Art. 49)
Post-market monitoring (Art. 72) | Serious incident reporting (Art. 73)

D. Key Compliance Deadlines

- **Feb 2, 2025** Prohibited practices (Art. 5) and AI literacy (Art. 4) *in force*
- **Aug 2, 2025** General-Purpose AI (GPAI) provisions *in force*
- **Aug 2, 2026** Full application: high-risk, transparency, remaining
- **Aug 2, 2027** Annex I high-risk systems (already regulated products)