

EU AI Act Article 50 Readiness Assessment

Know where you stand before August 2, 2026

APPLIES FROM	PENALTY EXPOSURE	SCOPE	RISK TIER
2 August 2026	€15M or 3% of turnover	Providers & deployers	Applies regardless

Article 50 Article 50 establishes transparency obligations whenever AI:

- Interacts directly with people
- Generates synthetic content
- Is used for emotion recognition
- Generates deepfakes or public-interest text

Step 1 - Establish your role per system

- ☐ The same organisation can be a provider on one tool and a deployer on another, proceed system by system
- ☐ List every AI system in use or on the market that interacts with people, generates content, does emotion/biometric analysis, or touches deepfakes or public-interest text
- ☐ For each: are you the provider (built it / put it on the market under your name) or the deployer (using someone else's system under your own authority)?
- ☐ Flag systems where you're both: ex. an in-house tool you built and use

Step 2 - Map each system against the four triggers

Trigger	Responsible party	What it covers
50(1) Direct interaction	Provider	Chatbots, AI agents, avatars — anything a person has a conversation with
50(2) Synthetic content marking	Provider	Systems generating audio, image, video, or text: machine-readable, detectable marking
50(3) Emotion / biometric recognition	Deployer	Any system inferring emotional state or sorting people by biometric data
50(4) Deepfakes & public-interest text	Deployer	AI-generated/manipulated image, audio, video, or text on matters of public interest

Step 3 - Obligation-specific checks

If you are a provider - 50(1) - direct interaction

- ☐ Is it obvious to a “reasonably well-informed, observant and circumspect” person that they’re talking to an AI? If not, is disclosure built into the design?
- ☐ Confirm disclosure happens at the interaction layer

Not required where use is authorised by law for detecting, preventing, investigating, or prosecuting criminal offences, subject to safeguards.

If you are a provider - 50(2) - synthetic content marking

- ☐ Is output marked in a machine-readable format?
- ☐ Is the mark detectable by downstream systems, not just visible to humans?
- ☐ If you rely on a third-party GPAI model to generate content, who owns the marking obligation contractually?

Timeline: systems already on the market before 2 August 2026 have until 2 December 2026 to comply. Systems placed on the market from 2 August 2026 onward must comply immediately.

If you are a deployer - 50(3) emotion recognition / biometric categorisation

- ☐ Are exposed individuals informed the system is operating on them?
- ☐ Is the notice clear, distinguishable, and accessible?

If you are a deployer - 50(4) deepfakes & public-interest text

- ☐ Is artificially generated/manipulated image, audio, or video disclosed as such?
- ☐ Is AI-generated/manipulated text published to inform the public on matters of public interest labelled as AI-generated?
- ☐ If relying on the editorial-review exception for text, is the review process documented: who reviewed, what was changed, rather than just asserted?

Exceptions:

Deepfakes: not required where authorised by law for detecting, preventing, investigating, or prosecuting criminal offences. Artistic, satirical, or fictional works: disclosure is lighter (existence of manipulation, in a way that doesn’t disrupt the work) but not eliminated.

Public-interest text: not required where a human has reviewed and substantially modified the content before publication.

Step 4 - Third-party & supply-chain checks

- ☐ Does incoming synthetic content from subcontractors include C2PA or equivalent provenance metadata?
- ☐ Do outgoing contracts with EU partners protect against regulatory fines for unlabelled synthetic media?
- ☐ Are upload settings on platforms you publish to (YouTube, TikTok, etc.) configured to self-declare synthetic content?
- ☐ If you’re a deployer relying on a third party’s system, does your contract confirm the provider has met their 50(1)/50(2) duties?

Step 5 - The gap log

Score each system as Conformant (C), Partial (P), or Gap (G) to identify technical and operational exposure.

System	Role	Trigger(s)	Status	Action needed	Owner	Deadline

This is a starting-point diagnostic, not a compliance certification. Use it to find where the real gaps are before drafting remediation. This is not a substitute for legal review.