CLARAUDIT

EU AI ACT TRANSPARENCY OBLIGATIONS

WHAT ARTICLE 50 REQUIRES OF SME DEPLOYERS

AUGUST 2, 2026

A GUIDE FOR SME DEPLOYERS

Most SMEs misread their position under Article 50. This guide shows how to read it correctly.

August 2, 2026 is the operative date for most EU AI Act transparency obligations under Regulation (EU) 2024/1689. If your business runs a customer-facing chatbot, uses an AI tool that interacts with clients, or generates synthetic content on behalf of customers, the regulation applies to you in some form. The question is which obligations are yours, and which belong to someone else in the supply chain.

This guide explains what Article 50 actually requires. It does not tell you whether your specific business is compliant — that depends on a structured assessment of the AI tools you use and how you use them. What it does is give you the analytical frame to run that assessment, or to have a substantive conversation with whoever helps you run it.

What this guide covers

01 The provider / deployer distinction under the AI Act, and why it determines your obligations.

02 When Article 25 shifts a deployer into provider-equivalent territory, and when it does not.

03 The four transparency obligations under Article 50, mapped by which actor they sit on.

04 When and how disclosures must be made under Article 50(5).

05 What Article 50 does not cover, and where other obligations begin.

SECTION 1 · PROVIDER, DEPLOYER, OR BOTH

The Question That Shapes Everything

Before mapping Article 50 obligations, answer one question: is your business acting as a provider, a deployer, or both, for each AI system it runs? Article 50 places some obligations on providers and others on deployers. Getting the classification wrong means preparing for the wrong set of requirements.

Providers, under the AI Act, are entities that develop or place an AI system on the market under their own name. OpenAI, Anthropic, Google — these are providers of the underlying models most SMEs use.

Deployers are entities that use an AI system in the course of a professional activity. Most SMEs are deployers. If your business uses a third-party chatbot platform to handle customer queries, you are the deployer.

Most commentary on Article 50 misreads the boundary, in one direction or the other. The careful reading takes more work.

Article 25(1) of the AI Act sets out when a deployer becomes a provider for regulatory purposes. The provision applies specifically to *high-risk* AI systems: those falling under Annex III, including recruitment screening, credit scoring, education, and certain law enforcement uses. For high-risk systems, a deployer that puts its name or trademark on the system, or makes a substantial modification to it, takes on provider obligations under Article 16. Article 25(1)(c) extends the bridge in one further direction: a deployer who modifies a non-high-risk AI system into a high-risk use becomes the provider for the resulting system.

Most SME deployments fall outside this scope. Customer support chatbots, AI-driven marketing tools, and content-generation interfaces built on LLM APIs typically are not high-risk under Annex III. Article 25 does not bridge to make the deployer a provider-equivalent for these limited-risk systems. The Article 50(1) disclosure obligation sits with the underlying provider, not with the SME wrapping the model.

SCENARIO · LIMITED-RISK SME

A 30-person SaaS company running a branded chatbot

The underlying model belongs to the LLM provider; the chatbot is branded under the SaaS company's name. The chatbot is not, by default, a high-risk AI system. Article 25 does not flip the SaaS company into provider-equivalent territory simply because of the branded interface. The Article 50(1) legal obligation rests with the LLM provider.

That does not mean the SME can treat Article 50(1) as someone else's problem in practice. The provider's obligation flows through the system the deployer operates. The disclosure must appear in the user-facing interface for the provider to comply, and the deployer is the one who controls that interface.

Most LLM providers' terms of service make the deployer responsible for surfacing required disclosures. Customer expectations around transparency are independently building. Contractual conditions can make this a commercial issue regardless of where the formal legal obligation sits.

Where Article 25 does bridge: when an SME deploys a high-risk system under Annex III and either brands it or substantially modifies it, or when an SME modifies a non-high-risk system into a high-risk use. In those cases, full provider obligations under Article 16 apply.

SECTION 2 · THE FOUR TRANSPARENCY OBLIGATIONS

Article 50's Transparency Obligations, Mapped by Actor

Article 50 contains four main obligations. Each runs to a specific actor and covers a distinct situation. The mapping below shows which obligation sits on the provider and which sits on the deployer.

PROVIDER

Article 50(1) — Interaction Disclosure

Providers must ensure that AI systems designed to interact directly with natural persons inform those persons that they are interacting with an AI system. The obligation does not apply where this is "obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect."

The "obviously AI" exception is narrower than many SMEs assume. A chat interface that answers in fluent natural language and operates under a branded persona does not obviously read as AI to a reasonably informed user.

DEPLOYER

Article 50(3) — Emotion Recognition & Biometric Categorisation

Deployers of emotion recognition or biometric categorisation systems must inform natural persons exposed to those systems of their operation, and process personal data in accordance with the GDPR and applicable Union law.

This is a direct deployer obligation. If your business runs a tool that infers emotional states or categorises individuals by protected characteristics, the disclosure sits with you.

DEPLOYER

Article 50(4) — Deepfakes & AI-Generated Public-Interest Text

Deployers using AI to generate or manipulate image, audio, or video content constituting a deepfake must disclose that the content has been artificially generated. An exception applies for evidently artistic, creative, or satirical works.

Separately, deployers publishing AI-generated text on matters of public interest must disclose the AI origin, unless the content has undergone human review with a natural or legal person holding editorial responsibility.

PROVIDER

Article 50(2) — Synthetic Content Marking

Providers of AI systems generating synthetic audio, image, video, or text must mark outputs in a machine-readable format as artificially generated. Its application date is also in flux under the proposed Digital Omnibus amendments.

For SME deployers, Article 50(2) is primarily the responsibility of the LLM provider, not yours. Understand it, note it, move on.

SECTION 3 · TIMING & MANNER

When and How Disclosures Must Be Made

Article 50(5) sets the timing and manner for all disclosures under paragraphs (1) to (4). The information must be provided "in a clear and distinguishable manner at the latest at the time of the first interaction or exposure." It must also conform to applicable accessibility requirements.

"Clear and distinguishable" is the operative standard, and it carries real weight. A disclosure buried in a terms-of-service document that users scrolled past on signup is not clear and distinguishable at the time of first interaction. A visible notice in the chat interface before the conversation begins — "You are now chatting with our AI assistant" — is.

The timing requirement is also more precise than many implementations allow. The disclosure must appear at the latest at first interaction, not at some later point in the customer relationship. A business that adds disclosure language to its privacy policy update in Q3 has not met Article 50(5) if its chatbot started interacting with customers before any disclosure appeared in the interface.

CASE · DUTCH DPA INQUIRY

A Rotterdam SaaS company, an AI support agent, and a 40-minute disclosure gap

A customer corresponded with an AI support agent for forty minutes before realising they were not speaking to a human. The regulatory complaint cited the absence of any disclosure in the chat interface. The DPA's first move was an inquiry to the SaaS company as the operator of the interface.

For the company, the consequences arrived before any enforcement decision: an enterprise customer had made verifiable AI disclosure compliance a condition of contract renewal. Whether the formal Article 50(1) obligation sat with the underlying LLM provider or, in narrower circumstances under Article 25, with the SaaS company itself, the commercial gap was the same. The compliance gap had commercial consequences on its own.

Article 50(5) also requires accessibility compliance for disclosures. A disclosure visible only to users without accessibility needs does not meet the standard.

SECTION 4 · BOUNDARIES

What Article 50 Does Not Cover

Two confusions appear consistently in SME commentary on this regulation. Both turn on assuming Article 50 says more than it says.

Article 50 is not Article 26. Article 26 sets deployer obligations for high-risk AI systems — the systems listed in Annex III, including AI used in recruitment, credit scoring, education, and law enforcement. Those obligations are stricter, include human oversight requirements under Article 14, and for standalone high-risk systems are now expected to apply from December 2, 2027 under the proposed Digital Omnibus amendments. If your business uses AI for recruiting or credit decisions, Article 26 applies on top of Article 50, not instead of it. Different regime, different obligations, different deadline.

Article 50(6) makes the floor explicit: paragraphs (1) to (4) do not affect requirements under Chapter III and are without prejudice to other transparency obligations in Union or national law. Article 50 compliance is necessary but not sufficient for most SME deployers with AI in their operations.

The provider/deployer boundary in genuinely ambiguous cases requires legal judgment, particularly where high-risk classification under Annex III is contested.

Article 25 establishes when the boundary shifts for high-risk systems, but determining whether a given system falls within Annex III in the first place, whether a customisation constitutes a "substantial modification," or whether a branded deployment triggers the trademark clause is a factual and legal question that turns on the specific facts of the deployment.

ClarAudit produces the structured documentation that frames those questions: an AI system inventory, a risk classification for each tool, and transparency notice templates based on the structured audit data. It does not substitute for professional counsel where the classification is genuinely contested.

SECTION 5 · WHAT YOU SHOULD DO NEXT

Three Questions for Every AI System You Run

The first step is an inventory. Before assessing Article 50 exposure, you need a complete list of every AI system your business uses, including tools that staff have adopted informally. The obvious three or four come quickly. The fifth and sixth emerge from the corners of the room — and the compliance picture changes.

01

Is this tool interacting directly with natural persons?

Maps to Article 50(1). If yes, the interaction-disclosure obligation is in scope. Identify whether the obligation sits with the provider or, under Article 25, with you.

02

Does it process biometric or emotional data?

Maps to Article 50(3). If yes, the disclosure sits directly on you as the deployer, alongside GDPR obligations.

03

Does it generate or manipulate synthetic content published externally?

Maps to Article 50(4). If yes, the deepfake disclosure or the public-interest-text disclosure may apply. The editorial-responsibility carve-out is narrower than it sounds.

This guide is for informational purposes and is not legal advice. ClarAudit produces compliance documentation but does not replace professional counsel for ambiguous or high-risk situations.

ClarAudit is a self-serve EU AI Act audit tool for European SMEs — €349, one sitting, full documentation pack delivered.