



AI Transparency Isn't Just a Compliance Checkbox; It's a Design Choice

©Bloor Research September 2026

What “AI Transparency” Usually Means

For most enterprises right now, AI transparency means a specific, regulatory obligation. Article 50 of the EU AI Act requires providers of AI systems that interact directly with people to make sure those people are told they're dealing with an AI and requires anything generating synthetic audio, image, video, or text to mark it as artificially generated, in each case no later than the first interaction. The UK's ICO frames the same idea through data protection law: organisations have to be clear about how personal data is being processed inside an AI system, including the purpose, retention, and who else receives it.

Both are real obligations, and neither is optional. But both describe transparency as a disclosure that gets added to a system – a label, a notice, a line in a privacy policy – after the system itself has already been built.

Where Compliance Transparency Stops

That's a bolted-on pattern, not a design principle, and it shows up elsewhere in AI governance too: it's the same structure [human-in-the-loop design](#) usually takes, oversight added to a system to satisfy a regulatory requirement, rather than built in because the system was designed around a person from the start. A disclosure notice satisfies Article 50. It doesn't, by itself, make the system trustworthy – it just makes the fact that it's a system visible.

Enterprises evaluating AI vendors on “transparency” usually end up checking whether the disclosure box is ticked, not whether the system was built to be legible to the people relying on it. Those are different questions, and only one of them predicts whether the system will actually earn trust once the novelty of the disclosure notice wears off.

Disclosed, Not Disguised: Transparency as a Design Choice

Bloor Research's own description states the alternative directly: transparency is built in, Digital MeSM is disclosed, not disguised, and trust is a design requirement rather than an afterthought. Practically, that means the system is structured from the outset so that anyone interacting with it always knows they're interacting with a person's Digital MeSM – not because a notice says so, but because the system was never built to pass as anything else.

***“Transparency is built in.
Digital Me is disclosed, not disguised.
Trust is a design requirement,
not an afterthought.”***

Bloor Research International

It's the same origin-first logic behind OAISM: a system built around a specific person's knowledge from the start doesn't need disclosure retrofitted onto it, because there was never a moment it was designed to be mistaken for something else.

What This Looks Like for Enterprise Buyers

For a buyer, the practical test isn't whether a vendor can point to a disclosure notice – every compliant vendor can. The test is whether disclosure is structural or cosmetic: does the system's design make it obvious who or what someone is dealing with by default, or does it take a notice to make that clear because the interface was built to feel as human as possible first?

That test maps onto the “trustworthy AI” standard enterprises are increasingly asked to evaluate against but answers it more specifically than a checklist can: a system designed to be disclosed from the start satisfies the letter of Article 50 and the ICO's transparency principle as a side effect, rather than as the entire point of the exercise.



Frequently Asked Questions (FAQs)

1. What does AI transparency mean under the EU AI Act?

Under Article 50, providers of AI systems that interact directly with people must ensure those people know they're interacting with an AI, and any AI-generated synthetic audio, image, video, or text must be marked as artificially generated, both no later than the first interaction.

2. Is trustworthy AI the same thing as transparent AI?

Related, not identical. Transparency (disclosure that a system is AI, and how it uses data) is one input into trustworthiness, but a system can disclose correctly and still not be trustworthy if that disclosure was bolted on rather than built in.

3. What's wrong with treating transparency as a compliance checkbox?

Nothing is wrong with the compliance itself it's required. The problem is stopping there: a disclosure notice added to a system built to seem human doesn't change how the system was designed, only what it says about itself afterward.

4. How does Digital MeSM handle disclosure differently?

It's structured from the outset so people always know they're dealing with a specific person's Digital MeSM – disclosed, not disguised – rather than relying on a notice added after a general-purpose system was already built.

Sources

- [EU Artificial Intelligence Act – Article 50, Transparency Obligations](#)
– disclosure requirements for AI interaction and synthetic content.
- [ICO – “How do we ensure transparency in AI?”](#)
– UK data-protection transparency requirements for AI systems.

ARTICLE REPRINT



**BLOOR
RESEARCH**

+44 (0)1494 311 460
info@bloorresearch.com
www.bloorresearch.com