AI & Partners
Amsterdam - London - Singapore

Transparency Requirements for AI Systems
Users must understand systems' functioning

Co-authored with Yonah Welker, *Public Technologist*

18 August 2025

---

4. Transparency and Information Obligations — Disclosure, Clarity, Oversight, Records

4.1 Transparency Requirements for AI Systems	4.2 User Awareness and Human Oversight	4.3 Labelling and Disclosure of AI-Generated Content	4.4 Data Governance and Record-Keeping
Users must understand systems' functioning	*AI use must remain supervised*	*Flagging content made by AI.*	*Maintaining logs and data quality.*

Introduction to Transparency in AI

Transparency is one of the foundational principles of the EU AI Act (Recital 44, Articles 13, 50, and 53). It serves as a safeguard for accountability (Article 72 on post-market monitoring), human autonomy (Article 14 on human oversight), and informed decision-making (Article 13 on user information requirements). In a digital environment increasingly shaped by opaque algorithms and autonomous systems, the need for users—and regulators—to understand how AI works is not merely technical. It is political, social, and legal, as emphasized in Recitals 2, and 5, which stress that AI must be developed and deployed in alignment with Union values, including respect for fundamental rights under the Charter of Fundamental Rights of the EU (Recital 6).

The AI Act introduces clear transparency requirements that apply to a wide range of systems, particularly those classified as high-risk (Articles 6 and 7) or designed to interact directly with humans. These obligations ensure user trust and meaningful engagement with AI systems, supported by EU AI Office and national supervisory authority oversight.

Why Transparency Matters

Artificial intelligence often operates behind the scenes, quietly influencing hiring decisions, financial approvals, medical assessments, and public safety interventions. When users do not know they are interacting with AI—or cannot understand the system's rationale—the risk of misunderstanding, manipulation, or harm increases.

Transparency requires AI systems to be explainable, identifiable, and traceable—enabling users to understand system behavior and contest outcomes. It allows regulators to enforce compliance and helps businesses demonstrate accountability. In effect, transparency transforms AI from a black box into a governed and comprehensible system.

The AI Act embeds this principle throughout its framework, with specific rules based on system type, risk level, and context of use.

General Obligations for High-Risk AI Systems

High-risk AI systems, such as those used in critical infrastructure, education, employment, and biometric identification, are subject to detailed transparency obligations under the Act. Providers of these systems must ensure that users can access information about:

- The system's intended purpose
- The functioning logic and underlying methodology
- The roles and responsibilities of human operators
- The limitations and expected performance of the system

This information must be clear and accessible to intended users, enabling informed decisions rather than mere technical disclosure. The goal is not technical disclosure for its own sake, but functional understanding that enables users to make informed decisions about using or relying on the system.

Providers must also maintain internal documentation and technical files demonstrating compliance, which may be reviewed during conformity assessments or audits.

Implementation Timeline and Key Dates

Under the EU Artificial Intelligence Act (Regulation (EU) 2024/1689), transparency and compliance obligations are introduced through a phased timeline:

- **February 2025 (Article 5)**: Provisions relating to prohibited AI practices (e.g., social scoring by public authorities, certain forms of real-time biometric surveillance in public spaces) become enforceable.
- **August 2026 (Article 96)**: Obligations for most high-risk AI systems take effect, including transparency (Article 13), human oversight (Article 14), record-keeping (Article 16), and labelling of AI-generated content (Article 50). Providers must complete conformity assessments (Article 43) before placing such systems on the market.

Fundamental Rights Impact Assessments

Providers of high-risk AI systems must perform and document a **Fundamental Rights Impact Assessment (FRIA)** prior to deployment (Article 27). This requirement applies when systems are likely to significantly affect fundamental rights, such as privacy, non-discrimination, and freedom of expression. The FRIA must assess potential harms, mitigation strategies, and whether human rights principles are respected in practice.

Disclosure of AI Interaction

Under the EU AI Act (Article 50), AI systems that interact with humans—especially those that may be mistaken for people—must clearly disclose their artificial nature. This obligation ensures users know when they are engaging with AI rather than humans.

This applies to:

- Chatbots and virtual assistants – disclosure at first interaction
- Emotion recognition or biometric categorization tools – explicit notification
- AI-generated or recommended content – clear labelling, including for deepfakes
- Systems simulating human traits – prevention of anthropomorphic deception

Disclosure must be immediate and unambiguous. For example, a chatbot must identify itself as AI before speaking. This protects user autonomy and prevents manipulation—especially in sensitive areas like healthcare, legal advice, or advertising.

These rules safeguard informed consent and reinforce the Act's core principle: users must always know when they are interacting with a machine.

Transparency in Emotion Recognition and Biometric Categorization

AI systems used for emotion recognition or biometric categorization—such as assessing age, gender, or emotional state—must meet specific transparency obligations. Individuals must be:

- Clearly informed that the technology is in use
- Told what data is being collected
- Given the purpose and expected outcomes

Because these systems often process sensitive data, transparency is essential to prevent covert profiling or surveillance. In public spaces, clear signage or digital notices may be required. In workplaces or schools, written disclosure and informed consent are typically necessary.

These measures ensure individuals are aware, not unknowingly monitored—upholding ethical standards and legal rights.

Facing the Algorithm: Transparency in Emotion and Biometric Classification

Under Article 50(3), using emotion recognition or biometric categorization on vulnerable individuals—such as children, the elderly, or persons with disabilities—requires heightened transparency. Providers must clearly communicate the system's purpose, logic, and limitations in a form accessible to those individuals or their legal representatives.

Synthetic Content and Deepfakes

The EU AI Act (Article 50) addresses the growing use of AI-generated content—synthetic audio, video, or images that may be mistaken for human-created material. When this risk exists, providers must clearly inform users (Article 50(1)).

This includes deepfakes: realistic synthetic media that mimic real people or events (Recital 134). Whether used for satire, entertainment, or deception, deepfakes threaten trust, authenticity, and democratic integrity.

Disclosure is required to:

- Counter disinformation
- Protect individual privacy and reputation
- Help users distinguish between real and synthetic content

Exceptions (Article 50(2)) apply in limited cases, such as minor edits, legal investigations, or assistive functions that do not alter content meaning. Still, the default rule holds: synthetic or manipulated content must be clearly labelled.

These obligations reinforce the EU AI Act's rules on AI-human interaction and support transparency for general-purpose AI systems used to generate or alter media at scale.

Documentation and Record-Keeping

In addition to user-facing transparency, the Act requires that providers of high-risk systems maintain comprehensive internal documentation. This includes:

- Technical specifications and system architecture
- Training and testing data sources
- Risk assessments and mitigation strategies
- Human oversight protocols

This documentation serves multiple purposes. It supports conformity assessments, facilitates post-market monitoring, and provides a record for regulators to verify claims. Importantly, it creates a traceable record of how and why the system behaves the way it does.

Deployers—those who use the system in practice—are also required to log system operation and performance data, particularly where the system may impact rights or safety. These records must be made available to authorities upon request and retained for a defined period.

Accessible and Understandable Information

Transparency is not achieved simply by publishing technical documents. The information provided must be appropriate to the audience. This means using plain language, visual aids, or structured summaries where necessary. For example:

- A system used by medical professionals should provide clinical decision support explanations
- A system used by consumers should offer intuitive descriptions of what it does and how it works

- A system used by public authorities should highlight implications for legal rights or service access

The AI Act thus promotes **layered transparency**, where different levels of detail are available depending on the user's role and expertise.

Limits to Transparency: Trade Secrets and Security

While transparency is a core requirement, the AI Act also acknowledges legitimate concerns around **trade secrets, intellectual property, and cybersecurity**. Providers are not expected to disclose source code or proprietary algorithms unless required during formal investigations or legal proceedings.

The aim is to strike a balance between public accountability and business confidentiality. Regulators are expected to handle sensitive disclosures under strict confidentiality rules, ensuring that transparency obligations do not become a barrier to innovation or competitive strategy.

However, claiming trade secret protection cannot be used as a blanket excuse for opacity. Providers must still meet all user-facing disclosure requirements and provide adequate information to demonstrate compliance.

Enforcement and Oversight

Transparency obligations are enforceable under the AI Act's broader compliance framework. Failure to disclose AI interactions, provide understandable explanations, or maintain proper documentation can result in penalties, including:

- Fines for non-compliance
- Mandatory system modifications
- Suspension or withdrawal of CE marking
- Public reprimands or corrective disclosures

National supervisory authorities are responsible for monitoring these requirements, and individuals may have the right to lodge complaints or seek redress if they are not properly informed.

The EU Artificial Intelligence Office also plays a coordination role, offering guidance on best practices and helping to harmonize transparency standards across Member States.

Conclusion

Transparency is not a technical footnote in the EU AI Act—it is a central obligation that underpins trust, accountability, and fairness in AI use. In requiring clear disclosure, accessible explanations, and traceable documentation, the Act ensures that users are not left in the dark about how AI systems operate and impact their lives.

These requirements are not just about compliance—they are about empowering users, building public confidence, and aligning AI development with democratic values. As AI continues to evolve and integrate into daily life, transparency will remain a defining feature of lawful, ethical, and effective AI systems in the European Union.

Glossary

Act or EU AI Act: European Union Artificial Intelligence Act

AI: Artificial Intelligence

Board: European Union Artificial Intelligence Board

EU: European Union

SME: Small and Medium-Sized Enterprise

How can we help?

AI & Partners
Amsterdam - London - Singapore

AI & Partners ' –AI That You Can Trust'

At AI & Partners, we're here to help you navigate the complexities of the EU AI Act, so you can focus on what matters—using AI to grow your business. We specialize in guiding companies through compliance with tailored solutions that fit your needs. Why us? Because we combine deep AI expertise with practical, actionable strategies to ensure you stay compliant and responsible, without losing sight of your goals. With our support, you get AI you can trust—safe, accountable, and aligned with the law.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.