EU AI Act: What has applied since August 2026 – and what organisations should do now.

A practical guide for businesses using AI systems, generative AI, chatbots and AI-powered business applications

Since 2 August 2026, the transparency obligations under Article 50 of the EU AI Act have been in effect. Depending on the use case, businesses must inform people when they are interacting with AI, label deepfakes and certain texts on matters of public interest, and verify whether providers apply machine-readable markings to synthetic content. The obligations for high-risk AI have been postponed until 2 December 2027 and 2 August 2028, respectively. However, the requirements relating to transparency, AI literacy and prohibited AI practices have not been postponed.

For most organisations, the practical work begins with five questions: Where is AI already being used? Are we a provider or a deployer? Who is accountable for each use case? Which data and identities can the system access? And can we demonstrate how it is controlled?

Ask Marketing, HR, Customer Service and IT where AI is being used, and you will often receive four different lists. The gaps between these lists represent the first risk. An AI system that nobody knows exists cannot be governed, secured or documented.

THE SHORT ANSWER: The EU AI Act has not simply been "postponed". The transparency obligations under Article 50 already apply. Only certain obligations for high-risk AI will take effect later. Businesses should use this additional time to establish an AI inventory, define clear roles and accountability, and implement technical controls and documentation.

What changed on 2 August 2026?

Article 50 of the AI Act became applicable. It establishes transparency obligations for providers and deployers of certain AI systems, including interactive AI, generative AI, emotion recognition and biometric categorisation systems, deepfakes, and certain AI-generated texts concerning matters of public interest.

The European Commission has also begun enforcing the rules applicable to providers of general-purpose AI models. For a typical business purchasing AI solutions, however, the immediate question is rarely whether it is training a foundation model. What matters is whether a specific AI use case triggers obligations relating to disclosure, labelling, security or governance.

© Bacher Systems EDV GmbH

What has been postponed – and what has not?

Regulation (EU) 2026/1744, the Digital Omnibus on AI, postponed the application of the main obligations for high-risk AI. The reason was that harmonised standards, guidelines and national implementation frameworks were not yet sufficiently available. These obligations have been rescheduled, not removed.

2 December 2027: Standalone high-risk AI systems under Article 6(2) and Annex III.

2 August 2028: High-risk AI systems used as safety components of regulated products under Article 6(1) and Annex I.

The postponement provides additional preparation time – not a reason to wait. Risk management, technical documentation, logging, human oversight and cybersecurity all depend on design decisions being made today. Reconstructing this evidence after a year of production use is slower, more expensive and less reliable than documenting it from the outset.

First Question: Are You a Provider or a Deployer?

A provider develops an AI system, has one developed, or places it on the market under its own name or trademark. A deployer uses an AI system under its own authority in a professional context. Most businesses using third-party AI tools are deployers. However, their role may change if they substantially modify a system or offer it under their own name.

The same organisation may be a deployer for one use case and a provider for another. It is therefore important to clarify the role for each system individually. This determines who is responsible for implementing disclosures within the system design, applying machine-readable markings, visibly labelling content and retaining technical evidence.

Understanding the transparency obligations under Article 50

1. Inform People When They Are Interacting with AI

Providers of AI systems that interact directly with people must design their systems so that users are informed they are interacting with AI, unless this is obvious to a reasonably well-informed, observant and circumspect person. For a customer service chatbot or AI agent, this information should be provided at the beginning of the interaction rather than hidden in the terms and conditions.

© Bacher Systems EDV GmbH

2. Make Synthetic Content Machine-Readable

Providers of systems that generate synthetic audio, images, video or text must ensure that their outputs are marked in a machine-readable format and can be identified as artificially generated or manipulated. This obligation applies to providers. Nevertheless, businesses using third-party tools should verify which technical capabilities their providers offer and incorporate these requirements into procurement, integration and content workflows.

For providers of relevant generative AI systems that were already on the market before 2 August 2026, a transitional period for this specific marking obligation applies until 2 December 2026.

3. Disclose emotion recognition and biometric categorisation

Deployers of emotion recognition or biometric categorisation systems must inform affected individuals, subject to the exceptions and conditions set out in the AI Act. Although these use cases are less common than chatbots, the sensitivity of the data involved makes system discovery and access control particularly important.

4. Label deepfakes and certain texts on matters of public interest

Deployers must disclose when image, audio or video content qualifies as an AI-generated or manipulated deepfake. AI-generated or manipulated texts intended to inform the public about matters of public interest must also be labelled if they have not undergone human review or editorial control. This does not mean that every marketing sentence created with AI assistance must automatically carry a visible label. The organisation's role, the content, its context and the review process are decisive.

AI literacy remains important

The AI literacy requirements have applied since 2 February 2025. Following the amendments introduced by the Digital Omnibus, providers and deployers must take measures to support the development of AI literacy among employees and other individuals who operate or use AI systems on their behalf. The legislation does not require businesses to guarantee a specific level of competence for every individual. However, it does require appropriate, demonstrable measures tailored to the relevant context.

A single general training presentation each year will rarely be sufficient for every role. A developer integrating an AI model, a marketing employee approving synthetic content and a service desk employee using an AI assistant face different risks and therefore need different guidelines.

What penalties may apply?

Violations of the transparency obligations under Article 50 may result in fines of up to EUR 15 million or 3% of a company's total worldwide annual turnover, whichever is higher. The higher threshold of EUR 35 million or 7% applies to prohibited AI practices under Article 5 – not to every violation of the AI

Act. The AI Act provides for more proportionate calculations for SMEs. Actual enforcement depends on the individual circumstances and national procedures.

Key AI Act dates at a glance

Date	What applies
2 Feb 2025	Prohibited AI practices and AI literacy requirements
2 Aug 2025	Rules for general-purpose AI models and EU governance provisions
2 Aug 2026	Article 50 AI transparency obligations; Commission enforcement of applicable GPAI rules
2 Dec 2026	End of the transition for Article 50(2) marking by providers of relevant systems already on the market before 2 Aug 2026
2 Dec 2027	Main high-risk obligations for stand-alone systems under Article 6(2) and Annex III
2 Aug 2028	Main high-risk obligations for AI safety components in regulated products under Article 6(1) and Annex I

A practical 90-day plan for AI Act readiness

1. **Establish a central AI inventory.** Record each system, its provider, business purpose, owner, user groups, data categories, connected applications, affected individuals, provider/deployer role, risk indicators, external labelling, logging and contractual status. Start with a controlled register. Technical maturity can develop over time.

2. **Assess roles and risks together with legal counsel.** Distinguish between the obligations of providers, deployers, importers and distributors. Flag prohibited and potentially high-risk use cases for expert review. Legal classification should not be left to IT alone.

3. **Review all transparency touchpoints.** K Examine chatbots, AI agents, avatars, emotion recognition, biometric categorisation, synthetic media and content relating to matters of public interest. Verify both visible disclosures and machine-readable markings wherever applicable.

4. **Implement technical controls around each use case.** Define identities and access permissions, protect prompts and sensitive data, enable appropriate logging, monitor integrations, manage machine identities and document human review and escalation procedures.

© Bacher Systems EDV GmbH

5. **Establish evidence and accountability.** Assign a responsible owner, document decisions, retain provider information, define review intervals, record training activities and establish reporting that demonstrates the effectiveness of implemented controls.

Three questions organisations frequently ask

Has the EU AI Act been postponed?

No. Certain obligations for high-risk AI have been postponed. The transparency obligations under Article 50 have applied since 2 August 2026, while other provisions of the AI Act have already been applicable since 2025.

Does every AI-generated text need to be visibly labelled?

No. Providers must apply machine-readable markings to relevant synthetic outputs. Deployers must visibly label deepfakes and texts concerning matters of public interest that have not undergone human review or editorial control. The specific use case determines which obligations apply.

Does using a third-party AI tool make us a provider?

In most cases, an organisation using a third-party AI tool is considered a deployer – but not always. Businesses that offer a system under their own name or substantially modify it may assume a different role. Each system and deployment should therefore be assessed individually.

Official sources

- Europäische Kommission: Quick Facts - Transparency rules for AI systems
- Europäische Kommission: Leitlinien zu den Transparenzpflichten aus Artikel 50
- EUR-Lex: Verordnung (EU) 2024/1689 - Artificial Intelligence Act
- EUR-Lex: Verordnung (EU) 2026/1744 - Digital Omnibus on AI
- Rat der EU: endgültige Annahme der Vereinfachungsregeln

From regulatory requirements to technical operations: How Bacher Systems can helg

Legal assessments should be carried out by qualified legal counsel. Our work begins where those assessments need to be translated into a secure, transparent and manageable IT environment.

© Bacher Systems EDV GmbH

- **Consulting and Roadmap:** Analysing the existing environment, identifying technical gaps, prioritising initiatives and developing a realistic AI governance roadmap.

- **Implementation and Migration:** Turning the target architecture into operational solutions, integrations, processes and platform adjustments – supported by project management and proven best practices.

- **Data Analytics and Observability:** Bringing together logs, metrics, traces and events to provide visibility, dashboards, alerts and reporting across AI-powered services.

- **Cybersecurity and Digital Identities:** Protecting data, models and integrations through access management, privileged access controls, machine identity management and continuous security monitoring.

- **Support und Managed Services:** Operating and monitoring platforms, managing incidents, changes and lifecycles, and continuously improving solutions after go-live.

The last point is particularly important. AI Act readiness is not a one-off technology implementation. Through our Adoption Circle, we continue working closely with our customers after go-live to increase the value delivered by their platforms, adapt roadmaps and respond to evolving technical and regulatory requirements. We share accountability for the outcome – not just the technology.

Learn more:

Use AI Securely & Effectively | Bacher Systems » Bacher Systems Website

Important: Bacher Systems is not a law firm and does not provide legal advice. We can help translate legal assessments into technical reality – from AI inventories, roadmaps and secure architectures to access management, logging, observability, reporting, implementation and ongoing managed services.

© Bacher Systems EDV GmbH