

EU RULE · ARTIFICIAL INTELLIGENCE

AI Act: AI products for the EU market

The AI Act applies wherever the provider is based, as soon as an AI system is offered in the EU or its output is used there. The obligations phase in step by step; the dates for high-risk systems were pushed back in July 2026.

LEGAL BASIS	AMENDED BY	HIGH-RISK (ANNEX III)	AFFECTS
Regulation (EU) 2024/1689	Regulation (EU) 2026/1744	Dec 2, 2027	Providers and deployers of AI systems

In brief

The AI Act classifies AI systems by risk. Certain practices are prohibited, such as social scoring or manipulative techniques that cause harm (Art. 5). High-risk systems are allowed but tightly regulated. They include systems for recruitment, creditworthiness assessment, education and exams, critical infrastructure, and AI used as a safety component in products such as machinery or medical devices (Art. 6 with Annexes I and III). Chatbots and AI-generated content are subject to transparency obligations (Art. 50). General-purpose AI models, meaning large language and image models, have rules of their own (Art. 53 et seq.).

Most AI applications in companies, such as suggested replies in customer service or inventory forecasts, fall into none of these groups or only under the transparency obligations. The real effort is concentrated on high-risk systems.

Violations are expensive. For prohibited practices, Article 99 provides for fines of up to 35 million euros or 7% of worldwide annual turnover; for most other obligations, up to 15 million euros or 3%. For small and medium-sized enterprises, the lower of the two amounts applies in each case.

In July 2026, the EU used Regulation (EU) 2026/1744, the “Digital Omnibus on AI”, to postpone several deadlines and adjust individual obligations. It was published in the Official Journal on July 24, 2026 and entered into force three days later.

Who it affects in South America

Under Article 2(1)(a), the regulation applies to providers that place AI systems on the market or put them into service in the EU, regardless of where they are based. Under point (c), it also applies to providers and deployers in third countries if the output of the system is used in the EU. A startup in Buenos Aires that sells candidate screening software to HR departments in Germany is therefore the

provider of a high-risk system within the meaning of the regulation.

Providers of high-risk systems and of general-purpose AI models that have no establishment in the EU must appoint an authorized representative in the EU (Art. 22 and Art. 54).

Even if you only use AI, you can have obligations. The regulation calls this a “deployer”. A logistics company in Montevideo that uses an AI tool to evaluate staff at its Spanish branch is the deployer of a high-risk system in the EU. It must use the system according to the instructions, monitor it and keep logs.

Development service providers are indirectly affected. A team in Medellín that trains a fraud detection model for a French provider has no provider obligations of its own. The client, however, needs documentation on the data, training and testing to pass its conformity assessment. Article 25 governs responsibilities along the value chain and requires suppliers of components to provide the information needed for this.

Typical high-risk cases from the region: scoring software from fintechs in São Paulo or Bogotá for EU lenders, HR tools from Santiago, learning platforms with automated grading from Montevideo, image analysis for medical devices.

Deadlines

The regulation has been in force since August 1, 2024. Its obligations apply in stages. The overview below reflects the changes made by Regulation (EU) 2026/1744.

FROM	WHAT APPLIES
Feb 2, 2025	Prohibited practices (Art. 5) and the AI literacy requirement for staff (Art. 4)
Aug 2, 2025	Obligations for general-purpose AI models, governance, penalties
Aug 2, 2026	Transparency obligations under Art. 50
Dec 2, 2026	End of the transition period for marking AI-generated content (Art. 50(2)) for systems placed on the market before Aug 2, 2026
Dec 2, 2027	High-risk systems under Annex III, e.g. HR, credit, education (originally Aug 2, 2026)

FROM	WHAT APPLIES
Aug 2, 2028	High-risk AI in products under Annex I, e.g. machinery, medical devices

The postponement buys time, but the requirements themselves are unchanged. If you are developing a high-risk system for the EU market, you need risk management, data quality, logging and human oversight from the start. Retrofitting them later is hardly possible.

What EU customers actually ask for

EU customers now buy AI with their own list of questions. Expect the following:

- A classification of your system as prohibited, high-risk, subject to transparency obligations or without special obligations, with the reasoning.
- For high-risk systems, the technical documentation under Annex IV, the conformity assessment, the EU declaration of conformity and registration in the EU database.
- Information on training data: origin, rights, quality and how bias is handled.
- Instructions for use for the deployer, so your customer can meet its own obligations as a deployer.
- Logging and the ability to provide human oversight.
- Marking of AI-generated text, images, audio and video where Art. 50 requires it.
- The name of your EU authorized representative, if you need one.
- Often an [ISO/IEC 42001](#) certificate as evidence of an AI management system.

If your system processes personal data, the [GDPR](#) applies as well. Many of the questions overlap, for example on data origin and purpose limitation.

AI clauses are showing up more and more in contracts: a commitment that customer data will not be used for training, notice of significant model changes, cooperation with audits. The law does not always require them, but they reflect your customer's due diligence obligations.

First steps

1. Record every AI feature in your products and services, including embedded third-party models.
2. Assign each feature to a risk group. Check Annex III carefully, because the list of high-risk areas is specific.
3. Clarify your role: are you a provider, a deployer or a supplier to an EU provider?

4. Train your team. The AI literacy requirement has applied to all providers and deployers since February 2, 2025.
5. For high-risk systems, start on documentation and risk management now so that you are ready before December 2, 2027.
6. Check whether an ISO/IEC 42001 management system would make a difference to your customers.

Put the results in writing. A short list with the system, its purpose, the risk group and the person responsible is enough to start with, and it answers the first question every EU customer asks. If the list grows, a GRC platform such as [Sightadel](#), which supports the EU AI Act as a framework, can hold the inventory, the tasks and the evidence for each system.

The free [EU Readiness Check](#) shows where you stand overall.

How it relates to certifications

[ISO/IEC 42001](#) describes a management system for AI: roles, risk assessment, life cycle and data handling. It is not required by law, but it covers many of the regulation's organizational obligations and EU customers are asking for it more and more. For the security of systems and data, [ISO/IEC 27001](#) remains the standard; the two can be built up together. In [Sightadel](#), work already done for ISO/IEC 27001 can be reused for ISO/IEC 42001. If you supply AI software to banks, you should also know [DORA](#). AI in connected products also falls under the [Cyber Resilience Act](#).

FAQ

Does the AI Act apply to my company in South America?

Yes, if you offer an AI system in the EU or its output is used there (Art. 2(1)(a) and (c)). For pure development service providers, it usually applies indirectly through the client.

What did the Digital Omnibus change?

Among other things, Regulation (EU) 2026/1744 postponed the obligations for high-risk systems under Annex III to December 2, 2027 and for products under Annex I to August 2, 2028.

Is my chatbot a high-risk system?

Usually not. Chatbots are, however, subject to the transparency obligation: users must be able to tell that they are talking to an AI (Art. 50).

Do I need ISO/IEC 42001?

Not by law. The certificate does help you show EU customers that your AI management is in order. More on the [ISO/IEC 42001](#) page.

Which tool helps with AI Act and ISO/IEC 42001 documentation?

[Sightadel](#) is a GRC platform from Germany that supports the EU AI Act and ISO/IEC 42001 as frameworks, with templates, tasks and evidence per requirement. The classification of your systems remains your decision, and an ISO/IEC 42001 certificate is issued by an accredited certification body.

Sources · Last updated: October 11, 2026

Regulation (EU) 2024/1689 (AI Act), EUR-Lex: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

Regulation (EU) 2026/1744 (Digital Omnibus on AI), EUR-Lex: <https://eur-lex.europa.eu/eli/reg/2026/1744/oj>

European Commission: Regulatory framework for AI: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

General information, not legal advice. The official texts are authoritative.

PUT IT INTO PRACTICE WITH TOOLS MADE IN GERMANY



Sightadel

Sightadel walks your team through the EU AI Act: templates, tasks, evidence and audit preparation in one place. Built and hosted in Germany, with an optional consultant package.

[See Sightadel →](#)

Sightadel, veyrisk and Valar are products of neonotu GmbH, which operates MercoEU.

Which of these apply to your company?

The free EU Readiness Check shows you by industry and country in 10 minutes.

<https://www.mercoeu.com/en/eu-readiness-check>