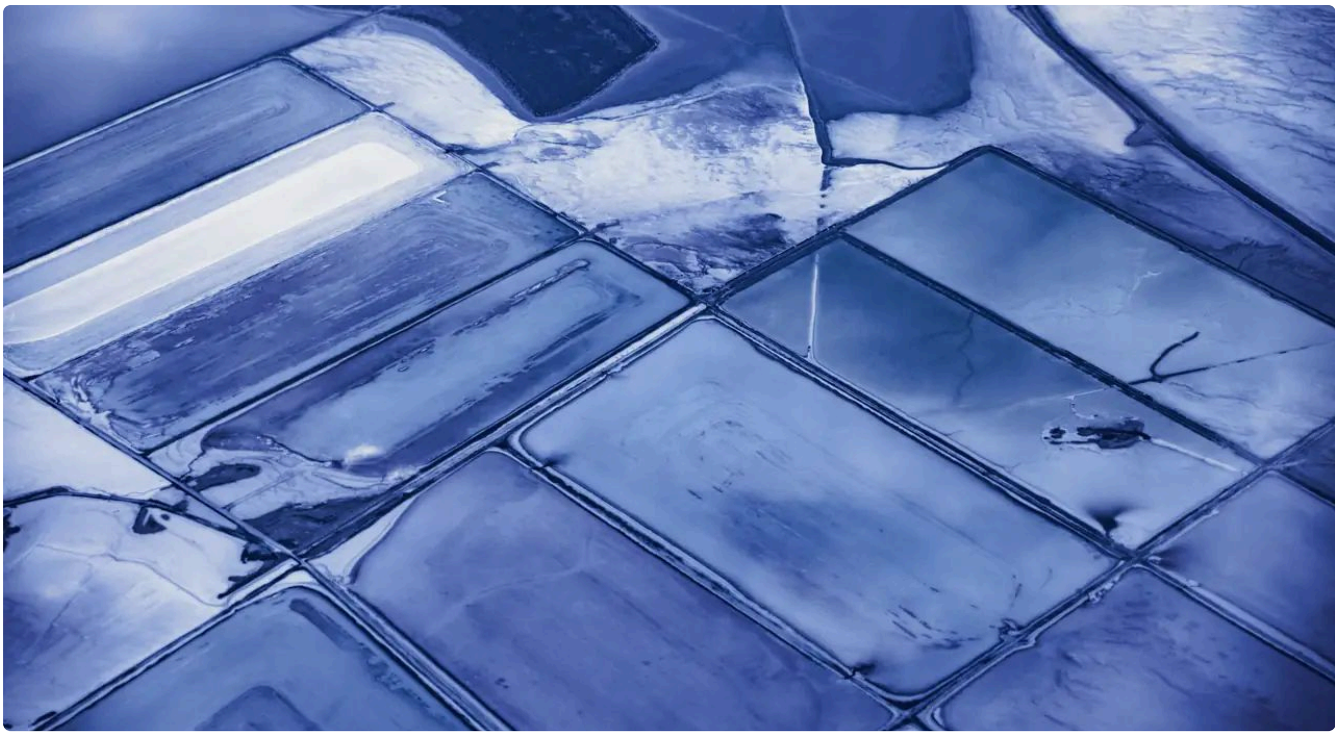


GUIDE · NOVEMBER 2026 · 12 MIN READ

The EU AI Act without the fuss

What applies when, which role your company plays and how to prepare in five steps



Philipp Pöschke
Founder, Paice

AT A GLANCE

- For most companies, three sets of AI Act obligations apply today: measures to support AI literacy, staying clear of prohibited practices and, depending on the use, transparency obligations, for example for chatbots or AI-generated images.
- Following an amendment in July 2026, obligations for high-risk systems, such as those used in recruitment or credit checks, apply from 2 December 2027, and for AI in regulated products from 2 August 2028.
- If you record your AI systems now and document the role and risk class of each one with your reasoning, you have the basis for every later obligation.

The EU AI Act (Regulation (EU) 2024/1689) has been in force since 1 August 2024 and applies in stages. It classifies AI systems by risk and assigns obligations to everyone who develops, sells or uses a system. That's why it also matters for companies that don't build any AI themselves.

In July 2026 the framework changed twice. The EU amended the regulation through the Digital Omnibus on AI (Regulation (EU) 2026/1744), in force since 27 July 2026. The amendment postpones the obligations for high-risk systems, rewrites the AI literacy obligation and adds two prohibitions. Two days later, Germany's Act on Market Surveillance and Innovation Promotion of Artificial Intelligence (KI-MIG) entered into force. It makes the Federal Network Agency (Bundesnetzagentur) the central supervisory authority.

This guide sets out what applies when, how to determine your company's role and which obligations follow from it. It's written mainly for companies that use AI and reflects the position as of 17 November 2026.

What applies when

FIGURE 1

What applies when (as of 17 November 2026)

1 August 2024
AI Act enters into force

2 February 2025
Prohibited practices (Art. 5) and the AI literacy obligation (Art. 4)

2 August 2025
Obligations for providers of general-purpose AI models, rules on authorities and penalties

27 and 29 July 2026
Amending Regulation (EU) 2026/1744 and Germany's KI-MIG enter into force

2 August 2026
General application, including the transparency obligations (Art. 50)

2 December 2026
Two new prohibitions; machine-readable marking (Art. 50(2)) also for systems already on the market before August 2026

2 December 2027
High-risk systems under Annex III, such as HR, credit, education, critical infrastructure

2 August 2028
High-risk systems in products under Annex I

Paice, based on Articles 111 and 113 of Regulation (EU) 2024/1689 as amended by Regulation (EU) 2026/1744 (EUR-Lex, consolidated version of 27 July 2026) and the Bundesnetzagentur

The dates of application are set out in Article 113 of the AI Act, and the transitional rules for systems and models already on the market before a given date in Article 111. For a company that uses AI, three groups of obligations apply today. The prohibitions in Article 5 and the AI literacy obligation in Article 4 have applied

since 2 February 2025, and the transparency obligations in Article 50 since 2 August 2026. The extensive obligations for high-risk systems follow from 2 December 2027 for the use cases in Annex III and from 2 August 2028 for AI in products covered by Annex I.

The postponement buys time. For deployers, the requirements themselves stay largely the same. If you deploy a high-risk system, you'll need named oversight staff, logging and reporting channels that work in day-to-day operations by the deadline. That takes lead time, especially when several departments and the works council are involved.

The current consolidated version on EUR-Lex is the authoritative text. The Commission adds guidelines. They're not binding, but they show how the Commission interprets the regulation. It published draft guidelines on classifying high-risk systems in May 2026; on 17 November 2026 its website still showed the draft.

Which role does your company play?

Which obligations apply depends on the role a company has for a particular system. The regulation mainly distinguishes two roles (Art. 3):

- **Providers** develop an AI system or have it developed and place it on the market or put it into service under their own name, whether for payment or free of charge.
- **Deployers** use an AI system under their own authority. Only purely personal, non-professional use is excluded.

The regulation also covers importers, distributors and authorised representatives. Providers carry most of the obligations.

Most companies are mainly deployers. They buy software with AI features and use it. Three situations turn a deployer into a provider:

01 **Your own development, including for internal use.** Under Article 3(11), putting into service includes supplying a system for your own use. If you build your own assistant on top of a licensed language model and use it in your company, you're both provider and deployer of that system. For a system that isn't high-risk, the additional obligations are limited.

02 **Changes to high-risk systems.** Under Article 25, you take on the obligations of a provider if you market a high-risk system under your own name, substantially modify it or change the purpose of another system so that it becomes high-risk.

03 **Significantly modified models.** Using a general-purpose AI model through an interface doesn't make you its provider. Only significant modifications to the model can trigger provider obligations. The Commission's guidelines for these models describe where the line falls.

So you determine the role system by system. A company can be a deployer for one tool and a provider for the next.

An example

A constructed example shows how differently this can turn out. A manufacturing company uses three AI applications.

- **A writing assistant in its office software, bought in.** The company is the deployer of a system that isn't high-risk. The main obligation is AI literacy.
- **A chatbot on its website, built in-house.** The company is the provider. Since 2 August 2026 the chatbot has to be designed so that users can tell they're talking to an AI system (Art. 50(1)).
- **Applicant management software that pre-sorts applications.** Annex III, point 4, expressly lists systems that filter applications or evaluate candidates. As a rule, the company is therefore the deployer of a high-risk system and has the obligations under Article 26 from 2 December 2027. Independently of the AI Act, German law requires the works council to be informed at the planning stage; section 90 of the Works Constitution Act (BetrVG) expressly mentions the use of artificial intelligence.

Obligations by risk class

Classification depends on the intended purpose. The check runs from top to bottom, from prohibited practices to systems with no specific obligations.

FIGURE 2

Obligations by risk class

01

Prohibited (Art. 5)

Since 2 February 2025, for example emotion recognition in the workplace, social scoring and manipulative techniques. From 2 December 2026 also AI that generates intimate images without consent or child sexual abuse material.

02

High-risk (Art. 6, Annexes I and III)

For example recruitment, creditworthiness, education, critical infrastructure or AI as a safety component in products. Deployer obligations under Art. 26 from 2 December 2027, for products from 2 August 2028.

03

Transparency (Art. 50)

Since 2 August 2026. Chatbots identify themselves as AI, generated content is marked in a machine-readable way, deepfakes are disclosed.

04

All other systems

No specific obligations beyond AI literacy (Art. 4). According to the Commission, the vast majority of AI systems in use fall into this group.

05

General-purpose AI models (Chapter V)

Obligations for model providers since 2 August 2025, such as technical documentation and a copyright policy. Companies that only use a model are generally not affected.

Paice, based on Regulation (EU) 2024/1689 as amended by Regulation (EU) 2026/1744 and the European Commission

For deployers, the transparency obligations matter mainly for deepfakes and for AI-generated text published to inform the public on matters of public interest. For such text, disclosure isn't required if a person has reviewed it and someone holds editorial responsibility (Art. 50(4)). The Commission published guidelines on Article 50 in July 2026.

What deployers of high-risk systems must do

Among other things, Article 26 requires deployers to

- use the system in accordance with the provider's instructions for use,
- assign human oversight to people who have the necessary competence, training and authority,
- ensure that input data under their control is relevant and sufficiently representative for the intended purpose,
- monitor operation and report risks and serious incidents,
- keep automatically generated logs for at least six months,
- inform workers' representatives and affected employees before using the system in the workplace,
- inform people that they're subject to decisions the system makes or helps to make.

Public bodies, private entities providing public services and deployers of systems for credit scoring and for risk assessment and pricing in life and health insurance must also carry out a fundamental rights impact assessment before first use (Art. 27).

AI literacy after the amendment

The July 2026 amendment rewrote Article 4. Providers and deployers must take measures to support the AI literacy of their staff and of other people who work with AI systems on their behalf. They expressly don't owe a particular level of competence for any individual. The measures should reflect prior knowledge, the context of use and the people affected. For overseeing high-risk systems, the stricter requirement in Article 26 still applies.

Penalties

Fines are tiered (Art. 99). Breaches of the prohibitions can cost up to €35 million or 7% of worldwide annual turnover, and breaches of most other obligations, including Articles 26 and 50, up to €15 million or 3%. Supplying incorrect or misleading information to authorities can cost up to €7.5 million or 1%. As a rule, the higher amount applies. For small and medium-sized enterprises the lower amount applies, and since the amendment this is also the case for small mid-caps at the two lower tiers.

Who supervises in Germany

Under the KI-MIG, the Bundesnetzagentur is the market surveillance authority unless the act provides otherwise (section 2(1) KI-MIG). It's also the single point of contact and handles complaints. For businesses it runs an AI service desk with an online tool for a first assessment of the risk class. Other authorities remain responsible in certain areas:

- BaFin for AI systems directly linked to supervised financial services,
- the existing market surveillance authorities for AI in products such as medical devices, lifts or toys,

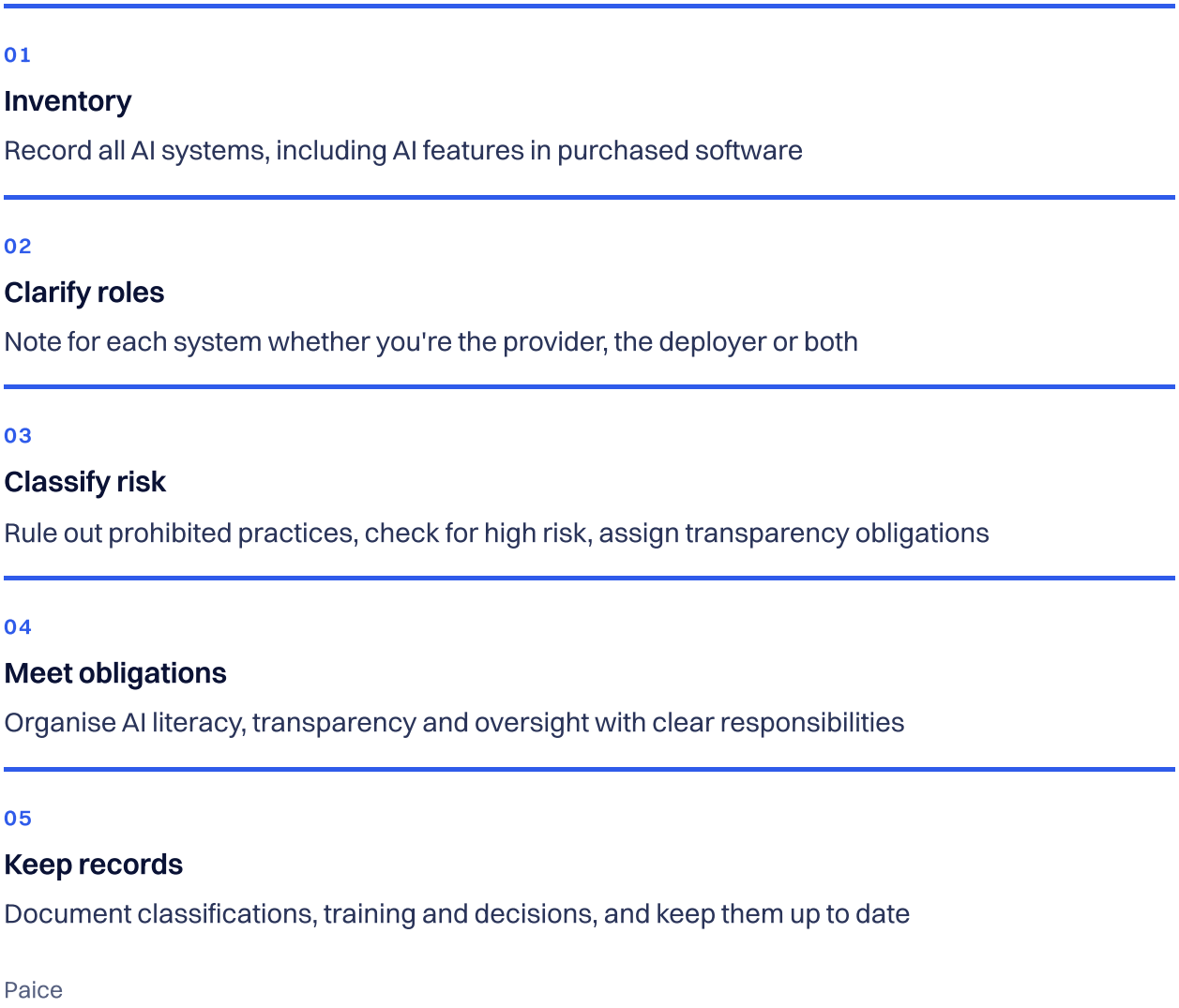
– authorities of the federal states for AI used by state public bodies and for media services.

At EU level, the Commission's AI Office supervises providers of general-purpose AI models.

Prepare in five steps

FIGURE 3

Prepare in five steps



Paice

01 **Inventory.** Record every AI system in use or planned, including AI features in purchased software and tools that departments use on their own initiative. To start with, a few details per system are enough: purpose, department, responsible person, vendor, data processed and people affected. The Commission's guidelines from February 2025 explain whether a piece of software counts as an AI system under Article 3(1).

02 **Clarify roles.** Note for each system whether you're the provider, the deployer or both. In-house developments and changes to purchased systems deserve a second look.

03 **Classify risk.** First rule out prohibited practices, then check Annexes I and III, and finally the transparency obligations. For purchased systems, the provider's stated intended purpose helps. If you use a system differently from what's intended, its classification can change. A provider that considers an Annex III system not to be high-risk under Article 6(3) must document this before placing it on the market and register the system (Art. 6(4), Art. 49(2)).

04 **Meet obligations.** Due now are AI literacy measures tailored to each role, usage rules, transparency notices and involving the works council. For high-risk systems, you'll need named and trained oversight staff by December 2027, along with logging, reporting channels and contracts that set out what information and support the provider delivers.

05 **Keep records.** Document the inventory, each classification with its reasoning, training and responsibilities. Build the check into your existing processes for procurement, data protection and information security so that every new system goes through these steps. A management system under ISO/IEC 42001 can provide the framework. For providers of high-risk systems, EN 18286 has been the first harmonised standard for the AI Act since October 2026; it covers quality management under Article 17.

> A well-maintained register of AI systems is the basis for every further obligation and makes approving new initiatives predictable.

Common mistakes

- **Only recording your own projects.** AI features also arrive in standard software through updates, without anyone having approved an AI project.
- **Reading the postponement as an all-clear.** Prohibitions, AI literacy and transparency obligations already apply, and preparing for the high-risk obligations takes lead time.
- **Setting the role once for the whole company.** It applies per system. If you build your own AI system internally, you're its provider.
- **Ticking off AI literacy with a single mandatory course.** Article 4 requires measures that fit the role and the use. Anyone overseeing a high-risk system needs more than basic training (Art. 26(2)).
- **Treating the AI Act in isolation.** For high-risk systems, Article 26(9) refers to the data protection impact assessment under the GDPR. In Germany, the works council has a say in technical equipment that can monitor employees' behaviour or performance (section 87(1) no. 6 BetrVG).

This guide does not replace legal advice. It reflects the position as of 17 November 2026 and simplifies in several places. Whether a particular system is high-risk and which role your company plays should be checked legally if in doubt.

Sources

- Regulation (EU) 2024/1689 (AI Act), consolidated version, EUR-Lex, as of 27 July 2026
- Regulation (EU) 2026/1744 (Digital Omnibus on AI), Official Journal of the EU, 24 July 2026
- AI Act: timeline and overview, European Commission

- Guidelines on prohibited AI practices, European Commission, 4 February 2025
- Guidelines for providers of general-purpose AI models, European Commission
- Guidelines on transparency obligations under Article 50, European Commission, 2026
- Draft guidelines on the classification of high-risk AI systems, European Commission, 19 May 2026
- First harmonised standard supporting the AI Act (EN 18286), European Commission, 19 October 2026
- AI Act Service Desk, European Commission
- KI-MIG (German act implementing the AI Act), Federal Law Gazette 2026 I No. 223, gesetze-im-internet.de
- Bundesnetzagentur takes on key role in implementation of AI Act, Bundesnetzagentur, 29 July 2026
- AI service desk, Bundesnetzagentur (in German)
- Works Constitution Act (BetrVG), English translation, gesetze-im-internet.de

---



AUTHOR

Philipp Pöschke

Founder, Paice

Philipp Pöschke founded Paice in Bremen in 2026. He is personally accountable for every engagement and works hands-on on analyses, prototypes and solutions. He is the author of the articles in Insights.