

Blog Post

N° 01/2024

# EU AI Act comes into force

*What companies need to consider now*

Dr. Andreas Windisch

**ASQUARED**

**asquared Blog Post N° 01/2024**

August 2024

Copyright © asquared GmbH

*The EU AI Regulation (EU AI Act) entered into force on August 1, 2024. It regulates the use of AI according to risk levels – from minimal to unacceptable – and obliges companies to ensure transparency, documentation, risk management, and training. While bans will take effect from February 2025, the strict requirements for high-risk AI will become mandatory from 2026. Strategic preparation is crucial now.*

## **The EU AI Act**

On August 1, 2024, the European Regulation on Artificial Intelligence (EU AI Act, also known as the AI Regulation) officially entered into force. This is the world's first comprehensive law regulating AI systems. The AI Regulation is intended, on the one hand, to minimize risks and potential harms caused by AI (such as discrimination, manipulation, or surveillance) and to protect citizens' fundamental rights, health, and safety. On the other hand, it is not intended to stifle innovation but rather to create a uniform legal framework that promotes trustworthy AI and provides companies with planning security.

For managing directors and IT managers of medium-sized and large companies, this means they must familiarize themselves with the new rules early on.

## **What does the AI Act regulate?**

The idea for the AI Regulation was presented in April 2021; the regulation was adopted by the European Parliament and Council in December 2023. Its aim is to protect EU citizens from the negative impacts of AI applications while promoting innovation. The AI Regulation creates a uniform regulatory framework in all EU member states and, in accordance with the market place principle, also applies to providers outside the EU if their AI systems are placed on the market or used in the EU.

A central principle of the law is the risk-based approach: the higher the risk an AI application poses to people or society, the stricter the requirements for that application. The regulation defines four risk levels for AI systems – from minimal to unacceptable – and sets graduated requirements for each level. Furthermore, the roles along the value chain are clearly defined (from the AI provider, through importers and distributors, to the AI user or operator within the company), and specific obligations are assigned to each. Companies should therefore first understand which AI systems they use and what role they play in order to determine the relevant obligations.

## Overview of risk classes for AI systems

The AI Regulation divides all AI applications into four risk classes. Companies must classify their existing and planned AI systems accordingly, as they are subject to different requirements. The categories are defined as follows:

- **Minimal risk:** The vast majority of AI systems fall into this category, e.g., spam filters or AI-assisted video games. Such applications are considered harmless and are not subject to any specific regulations. However, companies are encouraged to voluntarily develop good practice guidelines or codes of conduct to ensure responsible use of AI.
- **Limited or low risk (transparency obligations):** For AI systems with only low risk, the AI Regulation primarily stipulates transparency requirements. This means that users should be able to recognize that they are dealing with an AI. Specifically, chatbots or virtual assistants, for example, must clearly indicate that they are machines and not human interlocutors. Certain AI-generated content (such as deepfakes or synthetic media) must also be labeled as such to prevent anyone from mistaking it for authenticity. Beyond these information obligations, however, there are no further regulatory requirements at this level.
- **High risk:** AI systems that pose significant risks to health, safety, or fundamental rights are considered high-risk. These include, for example, AI-based medical diagnostic software, algorithms for applicant selection in human resources, or AI systems in credit approval. Strict requirements apply to such high-risk AI (details in the next section). Examples from Annex III of the regulation include AI in safety-critical infrastructure (transport, energy), in educational or professional assessments, in workforce management (e.g., CV screening tools), in access to essential services (e.g., credit scoring), in law enforcement or migration, as well as in justice and democratic processes. In short, if an AI application assesses people in important aspects of life or makes decisions with significant consequences for individuals, it is likely to be classified as high-risk AI.
- **Unacceptable risk:** AI systems that pose an unacceptable threat to security or fundamental rights are prohibited. This category is narrowly defined and includes, for example, AI methods for behavioral manipulation that subconsciously influence people (e.g., subliminal techniques), the exploitation of the weaknesses of vulnerable groups (e.g., AI that specifically manipulates children), social scoring by authorities or companies (social scoring based on a person's behavior), and certain forms of biometric mass surveillance (e.g., real-time facial recognition in public spaces without legal basis). Such applications are considered disproportionately dangerous and must be removed from the market by February 2025 at the latest (see schedule below).

Figure 1 summarizes the risk classification.

AI System Risk Classification	Compliance Requirements	Example AI Systems	Deadline / Responsibilities
<b>Unacceptable Risk</b> (Article 5)	<b>Prohibited</b> May not be offered or used	<ul style="list-style-type: none"> <li>Social scoring by government agencies</li> <li>Real-time facial recognition in public spaces</li> <li>Emotion recognition of employees in the workplace</li> <li>Targeted manipulation of children</li> </ul>	<b>February 2nd, 2025</b> Identify and decommission or rebuild prohibited systems.
<b>High Risk</b> (Article 6, Chapter III)	<b>Permitted</b> Subject to compliance with the requirements of chapter III	<ul style="list-style-type: none"> <li>Credit checks at financial institutions</li> <li>Automatic pre-sorting of CVs</li> <li>Medical diagnostic systems</li> <li>Management of energy and transport infrastructure</li> </ul>	<b>August 2nd, 2026 / 2027</b> Plan and launch compliance projects.
<b>Limited Risk</b>	<b>Permitted</b> Subject to compliance with transparency requirements	<ul style="list-style-type: none"> <li>Chatbots in customer service</li> <li>Text, image, and video generators (clearly labeled as AI-generated)</li> </ul>	<b>August 2nd, 2026</b> Plan and launch transparency measures.
<b>Minimal Risk</b>	<b>Permitted</b> Voluntary compliance with the code of conduct	<ul style="list-style-type: none"> <li>Spam filters in email systems</li> <li>AI-powered video games</li> <li>Recommendation algorithms in stores or streaming services</li> </ul>	- Observe, no obligation

Source: asquared / As of August 2024  
 ASQUARED

Figure 1: Overview of risk classification of the EU AI Act

This risk classification forms the core of the AI Regulation. For companies, this means identifying which of your current or planned AI systems fall into which risk class. While trivial use cases require little action, high-risk systems entail comprehensive obligations, and prohibited practices must be stopped immediately.

## Strict Requirements for High-Risk AI

For AI systems in the high-risk category, the regulation prescribes a whole range of strict requirements before such systems may be placed on the market or put into operation in the EU. These obligations are intended to ensure that high-risk applications are technically reliable, traceable, and can be used in a humane manner. The most important requirements include:

- Risk management and mitigation:** Suppliers must maintain a continuous risk management system to identify and minimize potential hazards, malfunctions, or misuse of their AI. This includes safeguards against discrimination due to distorted data sets (keyword: bias) – for example, through high-quality, diverse training data and appropriate data governance.
- Technical documentation & transparency:** Before a high-risk system is placed on the market, detailed technical documentation must be created. This must describe, among other things, the purpose of the system, its design and functionality, the training data used (including origin, properties, and data cleansing), and built-in security and control measures. These documents are used by market supervisory authorities to verify conformity and by users (operators) to ensure safe use.

Furthermore, high-risk AI systems must automatically record logs during use to make their decisions and performance transparent afterward.

- **Accuracy, robustness, cybersecurity:** High-risk AI must meet certain performance standards. The systems should be sufficiently accurate, robust against disruptions, and designed to be cybersecure. In particular, technical and organizational measures must be taken to prevent and defend against attacks on the AI (e.g., adversarial attacks, data or model poisoning). Even if the AI system continues to learn or adapt after deployment, it must be ensured that it does not develop undesirable biases or risks over time.
- **Human oversight:** Despite automation, human oversight must not be omitted. Providers must provide concepts for human oversight of high-risk AI. In practice, this means that people should be able to correctly interpret AI outputs, be warned against overconfidence, and, if necessary, be allowed to override AI decisions, correct them, or shut down the system. Companies must therefore ensure that there are always responsible individuals in the processes who can monitor the AI results and intervene.
- **Clear information and usage instructions:** The provider of a high-risk AI must provide understandable instructions to subsequent users (operators). These instructions must include, among other things, the provider's contact information, the intended use and performance limitations of the AI, information on the required human supervision and interpretation of the results, and information on how to retrieve log data. The goal is to ensure that companies deploying such AI have all the information they need for safe operation.
- **Conformity assessment and CE marking:** High-risk systems may only enter the EU once they are formally compliant. This means they must undergo a prescribed conformity assessment procedure (similar to certification). Only when all requirements are met does the provider issue an EU declaration of conformity and award the CE marking. This CE mark (physical or digital) signals that the AI system complies with European standards and may be freely distributed within the internal market. Changes to the system may require further testing.
- **Post-market monitoring:** Responsibility does not end with the sale. Suppliers must establish a post-market monitoring system to observe the AI's performance in the field and identify any problems at an early stage. Serious incidents or malfunctions must be reported to the authorities (mandatory reporting), and corrective measures must be taken immediately if necessary. Operators, i.e. companies that use high-risk AI, are also required to do so: They should provide feedback to the provider or directly to the market supervisory authority if there are doubts about legal compliance and, in an emergency, suspend use.

These requirements are primarily directed at providers/manufacturers of high-risk AI. However, users (operators) of such systems within companies also have obligations: For example, they must strictly adhere to the instructions provided by the provider and use the AI system only within the intended scope, ensure continuous human monitoring during real-time operation, and retain the logs generated by the system for at least six months. They must also check whether the provider has issued an EU declaration of conformity and whether the system has been registered in the EU database. If a company finds anything suspicious about an AI system it uses (e.g., regarding security or regulatory compliance), it is obligated to notify the provider or the relevant supervisory authority. In short, companies cannot blindly rely on the technology – they share responsibility for ensuring that high-risk AI is operated safely and in compliance with regulations.

Caution: A company that significantly changes an existing AI solution or uses it for a new purpose can legally become a provider itself and thus must assume all manufacturer obligations. For example, anyone who extensively adapts a purchased high-risk AI module or resells it under their own name will be treated by law as an AI provider. This rule is intended to prevent shifts in responsibilities or gaps from arising. Companies should therefore carefully examine their respective roles and the associated obligations.

## Transparency obligations and generative AI

In addition to the extensive provisions for high-risk applications, the AI Regulation also contains rules for lower risks, particularly transparency obligations for certain AI systems. These requirements are relevant for many companies, as they also affect everyday AI use, such as in customer service, marketing, or the internal use of generative AI. Two aspects are particularly important here:

- 1 **Labeling of AI content and interactions:** If an AI interacts directly with people, those affected must be informed. A company that uses a chatbot in customer service, for example, is obligated to clearly inform users that they are dealing with an AI (and not a human employee). Likewise, AI-generated content must be recognizable as such in certain contexts, especially if it appears deceptively real. Manipulative deepfake images or videos, for example, or AI-generated texts presented to the public as news, must be clearly labeled as artificially created. This transparency is intended to strengthen trust and prevent people from being unknowingly misled by AI content.
- 2 **Rules for Generative AI and Basic Models (GPAI):** For the first time, so-called general-purpose AI models (GPAI for short) are also being regulated. These are large, broadly applicable generative AI models, such as ChatGPT. Such models can pose systemic risks if they are highly powerful and widely used. The AI Regulation

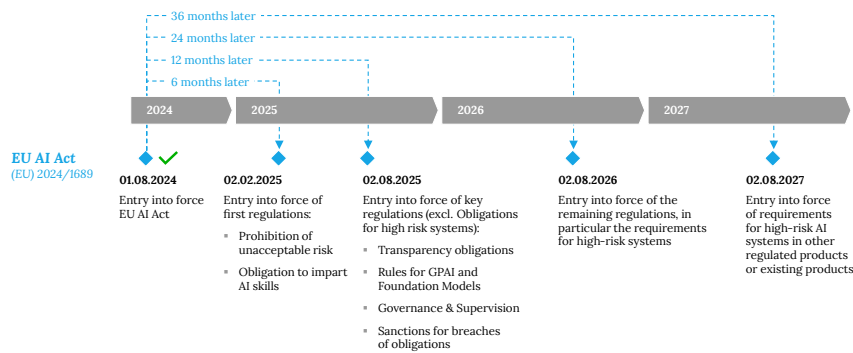
imposes additional due diligence obligations on providers of these generative AI models starting in August 2025. These include, among other things, comprehensive technical documentation on the AI model (including descriptions of the training data and procedures), compliance with copyright rules during training (training must not be based on illegally obtained or copyrighted data without a license), and transparency information for downstream users. Providers must, for example, provide a type of user manual explaining the suitability of the model and the risks associated with its use. For particularly powerful AI models with systemic risk (such as very large models exceeding certain parameter or computing power thresholds), even stricter requirements apply to ensure their use is monitored.

This will be indirectly important for most companies: Only a few companies develop such large AI models themselves, but many use them. The new obligations mean that providers such as OpenAI, Google, or others that provide generative models must provide more information and safeguards. Companies that use these AI models (e.g., integrate them via API or develop solutions based on them) should use the information provided to ensure compliance. For example, it can be expected that in the future it will be easier to understand which data a model was trained on in order to assess potential risks (biases in training, protected content, etc.). Furthermore, the EU Commission is working on a voluntary code of conduct for GPAI providers that addresses topics such as transparency, copyright protection, and risk management. This is expected to be available in spring 2025 and will provide companies with further guidance.

Regardless of specific deadlines, it makes sense for companies to prioritize transparency now when using AI. Open communication about where AI is being used and what content has been generated automatically builds trust among employees, customers, and partners – and prepares for upcoming legal obligations.

## **When do which regulations come into force?**

Although the AI Regulation formally entered into force in August 2024, many requirements do not apply immediately. Instead, there are transitional periods. The regulations will gradually take effect over the next few years, giving companies time to adapt.



Source: asquared / As of August 2024  
ASQUARED

Figure 2: Expected timeline of the EU AI Act (as of August 2024)

The most important milestones are:

- **August 1, 2024:** Entry into force of the AI Regulation. From this date, the countdown begins for the phased application of the rules. Companies should start planning for implementation now.
- **February 2, 2025 (six months later):** The prohibitions on unacceptable AI practices will take effect. From this date at the latest, AI systems that fall under Article 5 (unacceptable risk, see above) will no longer be permitted to be operated or offered in the EU. Also from February 2025, the obligation to provide AI skills (Article 4 AI Regulation) will take effect – this means that companies must ensure that all employees who use or develop AI systems are appropriately trained and competent in using AI.
- **August 2, 2025 (twelve months later):** From then on, the governance rules and obligations for generic AI models (GPAI) will apply. In particular, providers of foundation models must now fulfill the documentation and transparency obligations described above, and the new European AI Office and national supervisory authorities will begin their work to verify compliance. Furthermore, EU member states must designate their respective AI supervisory authorities by this date.
- **August 2, 2026 (24 months later):** After a two-year transition period, most of the remaining provisions will become applicable, in particular the requirements for high-risk AI systems. From this point on, only compliant high-risk systems bearing the CE mark may be placed on the market, and companies using such AI must fully comply with the corresponding operator obligations. At the same time, from August 2026, authorities will be granted comprehensive sanctioning powers to prosecute violations (until then, the focus will be more on advice and building up supervision).

- **August 2, 2027 (36 months later):** In some special cases, longer deadlines apply. For example, certain rules for high-risk AI that are part of other regulated products (e.g., AI components in medical devices or machines) will only take effect after three years. This is intended to smooth out overlaps with sector-specific approval procedures.

In summary: By the beginning of 2025, all prohibited AI applications must be eliminated, and the first obligations (especially training/competence) must be implemented. Starting in 2025, new requirements will gradually come into force, with the major deadline in 2026, by which the majority of AI systems will be regulated. Companies should keep an eye on these deadlines and time their compliance projects accordingly.

## Preparation Tips

Especially for medium-sized and large companies, the AI Regulation is a wake-up call to strategically address the issue of AI governance. Even if some requirements will not become binding for another two years, now is the right time to set the course. If you haven't already done so, the following activities are important:

- 1 **AI inventory and risk analysis:** First, gain an overview of where AI is already being used in your company or is planned for use in the short term, and which risk category it falls into.
- 2 **Define responsibilities:** Determine the role your company and all stakeholders play in each AI application and ensure that everyone involved is internally clear about who is responsible for compliance with the respective requirements.
- 3 **Identify and eliminate prohibited applications:** Check whether you are using AI-based processes that fall under the prohibited practices – this is probably rarely the case. These should be adjusted.
- 4 **High-risk AI:** Initiate compliance projects: For purchased solutions, request the necessary information from the provider; for in-house developments, establish internal processes for risk management, documentation, quality assurance, and testing.
- 5 **Train employees (AI literacy):** Offer training and education so that employees who use AI tools or work on AI projects understand the functionality, opportunities, and risks of these systems.
- 6 **Establish internal policies and controls:** Develop internal company AI policies that define how AI systems are selected, operated, and monitored.

- 7 **Monitoring and audits:** Make monitoring AI systems a continuous process. High-risk AI, in particular, should be audited regularly to ensure it functions as expected and no new risks emerge.
- 8 **Stay up to date:** AI regulation is dynamic. Stay up to date on further developments and guidance. Since most regulations will not apply until 2026, there will be clarifications and possible adjustments by then.
- 9 **Senior management commitment** – Management must support these compliance efforts. The AI regulation will be as far-reaching as the GDPR – violations can be costly.

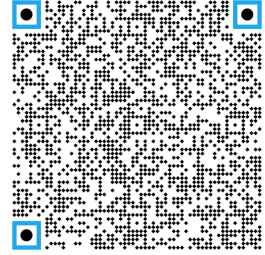
## Sources

- 1 European Commission, „Künstliche Intelligenz: Kommission begrüßt Inkrafttreten des weltweit ersten Rechtsrahmens für KI“, 1. August 2024, [https://ec.europa.eu/commission/presscorner/detail/de/ip\\_24\\_4201](https://ec.europa.eu/commission/presscorner/detail/de/ip_24_4201)
- 2 Federal Ministry for Economic Affairs and Climate Action (BMWK), „Der AI Act: Neue EU-Regeln für vertrauenswürdige KI“, Stand: July 2024, <https://www.bmwk.de/Redaktion/DE/Downloads/A/ai-act-eu-ki-verordnung.pdf>
- 3 KI.NRW, „Was Unternehmen über den EU AI Act wissen müssen – FAQ“, Version 2.0, June 2024, <https://ki.nrw/eu-ai-act-faq/>
- 4 Chamber of Commerce and Industry for Munich and Upper Bavaria, „Der EU AI Act – Was auf Unternehmen zukommt“, July 2024, <https://www.ihk-muenchen.de/ai-act>
- 5 ISACA, „Understanding the EU AI Act“, White Paper, May 2024, <https://www.isaca.org/resources/white-papers/2024/understanding-the-eu-ai-act>
- 6 ArtificialIntelligenceAct.eu, „High-Level Summary of the EU AI Act“, July 2024, <https://artificialintelligenceact.eu/high-level-summary/>
- 10 EUR-Lex, „Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 über künstliche Intelligenz“, Official Journal of the EU, 12. July 2024, <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32024R1689>

## Authors



**Dr. Andreas Windisch** is Managing Director at asquared. As a certified computer scientist and with a doctorate in engineering, he acted in leading positions in automotive, technology and consulting firms and disposes of many years of experience in the field of IT transformation management - especially in the banking and financial services sector.



## About asquared

Asquared is a Berlin-based consulting firm. Our work focuses on developing practical solutions for the regulatory, technologically and/or socially induced change, associated with direct application and confirmation in an industrial environment.

Our attention is focused on business and technology and their interaction. Reaching from the reorientation of strategies, over the (re)design of products and services to the operationalization - our work focuses on shaping change. On all levels.

We present selected insights of our theoretic and practical research work to a broader audience in the form of publications and lectures.

**asquared GmbH**


Pappelallee 78/79


10437 Berlin - Germany

Phone +49 (0) 30 22 66 79 60


E-Mail [contact@asquared.team](mailto:contact@asquared.team)

 [asquared.company](https://www.asquared.company)

 [asquared.blog](https://www.asquared.blog)

 [twitter.com/asquaredgmbh](https://twitter.com/asquaredgmbh)

 [instagram.com/asquaredgmbh](https://www.instagram.com/asquaredgmbh)

 [linkedin.com/company/asquared](https://www.linkedin.com/company/asquared)