EU AI ACT RISK CATEGORIES

WRITTEN BY: Németh Valentin - Goexo.eu

The full official text of the EU AI Act (2024/1689) can be found on the EUR-Lex website in several languages, including English. This regulation entered into force on 1 August 2024 and will be fully applied in practice from 2026. Below is a three-page summary, as well as a table of the regulation's risk categories, typical company examples and compliance requirements. For further information and comprehensive compliance support, please contact us!

https://goexo.eu

@: ai@goexo.eu

I. Purpose and scope of the regulation

The European Union Artificial Intelligence Regulation (AI Act) aims to create a uniform legal framework for the development, placing on the market, putting into service and use of AI systems in the EU. The regulation supports AI to be human-centric, safe, trustworthy and transparent, while protecting health, safety, fundamental rights (e.g. data protection) and democracy within the EU. Although it is a product regulation, it covers AI developers, deployers and operators (not individuals) – including companies outside Europe if they provide AI services or products in the EU.

Classically it does not apply to:

- AI systems exclusively for military, national security, research or private purposes.

- The research phase of the development of AI systems (until they are on the market).

II. Risk-based classification: four main categories

The regulation defines different compliance requirements according to the risk of the systems. The main categories are as follows:

1. Unacceptable risk systems:

- These are prohibited in the EU.

- Examples: social scoring, real-time biometric identification in public spaces (e.g. facial recognition), intentional manipulation of vulnerable groups, behavioral manipulation, hidden emotion recognition.

2. High risk systems:

- These must be developed, implemented and monitored according to detailed, strict rules.

- Two subgroups: (a) Products subject to product safety regulation — medical devices, toys, cars, aircraft, etc.; (b) Special areas — critical infrastructure management, education, employment, access to essential services, law enforcement, migration/border protection, justice.

- Typical industries: healthcare (diagnostics, medical technology), finance (credit assessment), transportation (self-driving cars, airplanes), utilities, government service providers.

3. Limited risk systems:

- Mainly transparency obligations apply (e.g. chatbots must indicate that AI is responding).

- Mainly generative AI models such as ChatGPT fall into this category.

4. Minimal risk systems:

- Typical examples: spam filters, AI-based video games, warehouse management systems, simple search engines.

- There is no strict regulation for these, voluntary good practices are recommended.

III. Main compliance requirements by category

The compliance obligations of all AI systems vary depending on the risk classification:

Unacceptable risk

- The placing on the market, provision and use of such systems is prohibited.

High risk

- Mandatory: risk management system, data quality and governance, technical documentation, logging, transparency, human oversight, cybersecurity, continuous review.
- Registration with a supervisory body.
- Continuous reporting and notification obligations (e.g. serious incidents).
- Implementation of quality management, maintenance of technical and legal documentation.
- Training obligations for personnel responsible for AI.

Limited risk

- User information (AI-generated content, marking of deepfakes).
- Prevention of the generation of illegal content.
- Transparency about the copyright of training data.

Minimal risk

- No mandatory legal compliance requirements.

IV. EDUCATION AND LITERACY REQUIREMENTS

IV. Training Requirements

The EU AI Act clearly requires training of employees working with AI systems and the development of general awareness of artificial intelligence (AI) ("AI literacy"). These obligations apply to all organizations developing, marketing and operating AI, regardless of the risk category of the AI system, but are more stringent for higher risk.

AI Act Section 4:

Developers, distributors and operators of AI systems must ensure that all staff involved in the operation, deployment, monitoring or customer interaction of AI systems have an appropriate level of AI literacy. AI literacy here means the skills, knowledge and understanding that enable the informed and safe use of artificial intelligence systems, the recognition of opportunities and risks and compliance with the law.

What is “AI literacy”?

- A comprehensive understanding of the operation, opportunities, limitations, risks and legal responsibilities of AI systems.

- The ability to recognise potential harm, bias, unethical use or privacy issues arising from the use of an AI system.

Who needs to be trained?

- All employees and other persons involved in the development, operation, deployment, monitoring or use of AI systems.

- The obligation may extend to external partners, subcontractors, or even to support customers who come into direct contact with AI.

What should be considered during training?

- The technical background, experience, responsibilities, and the context of use of the AI system are key when planning appropriate training or knowledge transfer.

- In the case of high-risk AI systems, training should be more comprehensive and detailed (technical knowledge, compliance obligations, ethical and data protection aspects).

- In the case of limited risk, basic awareness-raising training may be sufficient (e.g. recognition of AI systems, transparency, risks).

How to comply?

- Introduction of documented training, workshops, and knowledge transfer programs within the organization (it is recommended to log this to prove compliance).

- Examples of training topics: AI legislation and ethics, transparency, system operation, data management, bias reduction, responsibilities, incident management.

- In the case of high risk, the law specifically requires regular, refresher training for colleagues involved in AI development and operation.

When is it mandatory?

- The AI literacy requirement will apply to all AI companies from February 2, 2025.

Verification and mandatory documentation

- Direct measurement is not mandatory, but it is necessary to be able to prove that training or knowledge transfer has taken place, either with an internal protocol or training log.

- There is no separate penalty for “lack of training”, but the deficiency may aggravate the assessment of other violations!

Examples of compliance practices

- AI training, an induction program for all new employees set out in the regulations.

- Specialized training for high-risk AI applications (e.g. healthcare, finance).

- Archiving online platforms for knowledge sharing or curriculum/certification of external courses.

In summary, every AI-related organization must ensure that its employees have the “AI literacy” level, in a scalable manner and adapted to the level of the given system. This is especially true in high-risk areas, where the technical, legal and ethical aspects of education are also emphasized.

V. Supervisory and penalty mechanisms

- A European Artificial Intelligence Board and an AI Office will be established.

- Severe fines of up to €35 million or 7% of global turnover can be imposed for the most serious violations.

- Each actor (developers, distributors, importers, users) has a specifically defined responsibility.

- Special emphasis on AI literacy within the company, especially for managers and employees dealing with AI.

Table: EU AI Act risk categories, typical industries, example companies, compliance requirements

Risk category	Typical industries/ application examples	Typical company examples	Compliance requirements
Unacceptable (Prohibited)	Public sector, law enforcement, tech startups	Biometric database operators, facial recognition startups	Market entry/operation prohibited (social scoring, manipulation, real-time biometric AI)
High risk	Healthcare, transport, finance, public administration, education, critical infrastructure	Healthcare companies, banks, energy, utilities, transport companies, self-driving car companies	Risk management system, data governance, audit, regular reporting, documentation, AI training, transparency, quality assurance
Limited risk	IT, customer service, creative industries, media	Chatbot developers, content generator companies, generative AI platforms	Content transparency, AI tagging, deepfake labeling, copyright disclosure of data
Minimal risk	Game development, logistics, administrative systems	Software developers, gaming companies, warehouse automation	No mandatory compliance, voluntary “good practice” recommended

2025. 08. 15.