AI Act: Insight and recommendations for implementing the new requirements

On August 1, 2024, the "Regulation laying down harmonised rules on artificial intelligence" of the European Union (hereinafter: AI Act) came into force. The AI Act focuses on product safety law. However, various new obligations apply not only to companies that offer AI systems on the market, but also to those that operate the AI systems themselves or otherwise use them. The scope of the obligations varies greatly depending on the type of use of the AI systems and how an actor deals with AI.

We present the new obligations of the AI Act – applying to companies as well as public bodies – in detail and provide recommendations for implementation.

A. Temporal scope of application of the AI Act

Some of the new obligations of the AI Act will apply from February 2, 2025, which is why every company should deal with the requirements of the regulation immediately and check which legal requirements need to be implemented. In many cases of AI use, there are only isolated obligations. Nevertheless, internal company documentation is essential, as it is necessary to ensure knowledge of when the extensive obligations are to be implemented.

The different scope of the obligations is already evident in the time frame for the introduction of the obligations. The AI Act introduces a phased approach to the application of the standards in order to give stakeholders sufficient time to adapt. The following **important timelines** are set for certain obligations:

From February 2, 2025:

- **Every entity that uses AI** is obliged to train employees who use or otherwise deploy AI systems (Article 4 AI Act)
- **Prohibition of certain AI systems** with unacceptable risk; providers and deployers are affected (Article 5 AI Act)

From August 2, 2025:

- Obligations for **General Purpose AI** (GPAI), such as GPT-4o or Gemini 1.5, come into force; providers of GPAI must act quickly, while deployers will be subject to monitoring obligations
- The EU member states must designate **supervisory authorities** (and implement further obligations); the sanctions specified in the AI Act will also apply

From August 2, 2026:

- Regulations for high-risk AI systems become partially obligatory (Article 6 (2) AI Act)
- Special transparency obligations come into force (Article 50 AI Act)

From August 2, 2027:

- Only now specific regulations on high-risk AI in areas relevant to product safety are effective (Article 6 (1) AI Act)

In view of the considerable extent of possible fines, all entities should deal with the specific requirements at an early stage and make adjustments in order to comply with the legal provisions in good time. We are happy to assist you with the assessment.

B. Assignment of responsibilities according to the AI Act

The regulations of the AI Act affect all parties along the AI supply chain, including Importers (Article 3 No. 6 AI Act), Distributors (Article 3 No. 7 AI Act) and Operators (Article 3 No. 8 AI Act). Primarily affected are Providers (Article 3 No. 3 AI Act) and Deployers (Article 3 No. 4 AI Act), whose obligations we present in more detail below.

- **Providers** of AI systems are natural or legal persons who develop an AI system themselves or have it developed and place it on the market in their own name or with their own trademark (Article 3 No. 3 AI Act), e.g. Microsoft with Copilot. They are subject to the majority of legal obligations with various technical and organizational requirements.
- **Deployers** of AI systems are persons, companies or public bodies that use AI systems under their own responsibility and in a professional context (Article 3 No. 4 AI Act). Deployers within the meaning of the AI Act are therefore all companies that use AI systems supplied by providers or integrate them into their own products. The scope of the obligations strongly depends on the respective AI

system. In any case, deployers are responsible for ensuring that the AI systems they use comply with the regulations and that the necessary training and safety precautions are carried out.

C. Risk levels and obligations for companies

The AI Act takes a risk-based approach to address the different potential risks posed by AI systems. It distinguishes between four risk levels: prohibited practices, high-risk AI, AI systems with transparency requirements and other AI systems. In addition, there are special regulations for general purpose AI (GPAI). Each of the levels is associated with specific compliance requirements.

General obligation: Training in all companies that use AI systems

All providers and deployers of AI systems must ensure sufficient "**AI literacy**" in their operational environment (Article 4 AI Act). It must therefore be ensured that all persons who come into contact with the operation and use of AI systems have a sufficient understanding of AI, its legal framework and its risks.

This results in **training obligations** in practically every company, as every company will be classified as a deployer. All employees using AI systems must be trained in AI.

Prohibited AI systems

The regulation lists a catalogue of so-called **prohibited AI practices** (Article 5 AI Act). This includes certain practices - classified by the legislator as particularly intrusive - whose prohibition of use is primarily aimed at public authorities, e.g. the ban on biometric categorization systems that use sensitive characteristics (such as political or religious preferences). For the private sector, the complete ban on emotion recognition in the workplace is particularly relevant, which covers, for example, (alleged) burnout risk detection or the transcription of emotions in video conferences.

Companies that disregard this ban and still use prohibited AI practices can be fined up to EUR 35 million or 7% of the global annual turnover of the previous financial year (Article 99 (3) AI Act). The distinction between the AI systems used and prohibited AI is often not clear, which is why we strongly recommend a case-by-case examination. If you offer AI systems in areas that could be prohibited - e.g. biometric real-time monitoring - you should carry out an examination without delay.

Classification as high-risk AI

At the heart of the AI Act are the extensive obligations (only) for AI systems that are considered to be high-risk. If companies offer systems that are classified as high-risk, they will be subject to a broad **catalog of obligations** in future. Companies that operate such systems will primarily have monitoring and documentation obligations. The classification is based on a dynamic classification system that is primarily based on the intended use of the AI system (Article 6 and 7 AI Act). Classification as high-risk AI covers two subareas:

- High-risk AI exists when an AI system is used in **certain sensitive areas** that pose potentially significant risks to health, safety or human rights (Article 6 in conjunction with **Annex III** AI Act). These areas include critical infrastructures, education and professional education, employment, human resources management, health and financial services, law enforcement, justice and democratic processes.

Annex III No. 4 of the Regulation is particularly relevant for companies operating AI. This classifies certain AI systems in the field of **employment** and **personnel management** as high-risk AI. These include systems that are used for the targeted placement of job advertisements, the analysis and filtering of applications and the assessment of applicants. Also included are AI systems that make decisions on the terms and conditions of employment, promotions and terminations of employment, assign tasks based on individual behavior or personal characteristics and monitor and evaluate the performance and behavior of individuals. Therefore, an in-depth **review** of AI systems in the **HR department** is urgently required.

Even if AI systems fall into one of the categories in Annex III, they can be classified as non-high-risk under a **derogation rule** if there is no significant risk to the health, safety or fundamental rights of natural persons (Article 6 (3) AI Act). This may be the case if the AI system only fulfils a narrowly defined procedural task, improves the result of a human activity or recognizes decision-making patterns without replacing a human assessment.

- In addition, according to Article 6 in conjunction with **Annex I** of the AI Act, high-risk AI may exist if an AI system is used as a safety component in certain products that must comply with specifically defined Union harmonization legislation or must undergo a conformity assessment due to EU requirements. This applies, for example, if the AI systems are used as safety components in airplanes, vehicles or elevators.

Obligations for the providers of high-risk AI

The extensive obligations of the AI Act apply to **providers of high-risk AI**, which have an indirect impact on the deployers. In this respect, providers in particular are obliged to take the measures outlined below. Deployers must check their implementation. The following applies in particular:

- A **comprehensive risk management system** must be established to ensure the identification and mitigation of risks over the entire life cycle of the AI system (Article 9 AI Act).
- Prior to market launch, AI systems must be tested **under real-life conditions** to ensure that they are fit for purpose. Furthermore, the training, validation and test data sets must comply with the **data governance standards** set out in the Regulation (Article 10 AI Act).
- Compliance with the requirements must be demonstrated by means of **technical documentation**, which must be created prior to commissioning and continuously updated (Article 11 AI Act). The documentation is carried out as part of a self-assessment or with the involvement of notified bodies. After a successful conformity assessment, the AI system must be entered in an EU database and given a **CE marking** (Article 16 AI Act).
- Providers must also ensure that high-risk AI systems can be operated **transparently and monitored effectively** (Article 13 AI Act).

When using high-risk AI (Article 26 of the AI Act), **deployers** are also subject not only to the **control obligation** with regard to the above-mentioned obligations of the providers, but also to various **primary obligations**:

- Taking technical and organizational measures to ensure compliance with the **operating instructions**
- Ensuring **human supervision**
- **Checking the input data** with regard to its intended purpose and representativeness
- **Monitoring the operation** of the AI system and providing information to various bodies in the event of incorrect processing
- Generating and **storing the automatically generated logs** for at least six months
- **Informing** affected **employees** and **employee representatives** before commissioning a high-risk AI system in the workplace
- Compliance with **data protection regulations**, in particular carrying out a **data protection impact assessment**
- Special obligations exist when operating a system for **remote biometric identification**.

Companies that are active in the area of high-risk AI need to start implementing the measures now at the latest, as some of them have a long lead time. Experience from the introduction of the General Data Protection Regulation (GDPR) shows that last-minute compliance efforts tie up significantly more resources than dealing with the issue at an early stage.

Obligations for General Purpose AI (GPAI)

GPAI refers to the **models** that serve as the **technical basis for various well-known AI systems**. One example is the Large Language Model (LLM) GPT-4 from the company OpenAI, on which the popular ChatGPT tool is based. The AI Act also differentiates between GPAI with and without **systemic risk**. A systemic risk exists if the GPAI model has a potentially detrimental impact on public health, safety, fundamental rights or society as a whole. The classification is made either by a corresponding classification by the EU Commission or if the computing power required to train the model, measured in floating point operations (FLOPs), exceeds 10^25 (Article 51, 52 AI Act).

GPAI providers are obliged to create and continuously update **technical documentation** that includes information on the training and testing procedure as well as the test results (Article 53 AI Act). Providers must also ensure that they comply with **copyright provisions** and make a summary of the **training content publicly available**. For models with systemic risk, additional measures are required, such as carrying out a model evaluation, assessing and mitigating systemic risks, reporting and documenting serious incidents and complying with cybersecurity requirements (Article 55 AI Act).

Transparency obligations for certain AI systems

General obligations to provide information about the use of an AI system exist for **providers** of AI systems (Article 50 (1) and (2) of the AI Act) that can **interact with data subjects**, e.g. emotion recognition systems or chatbots, and for AI systems that generate synthetic audio, image, video or text content, e.g. offers that can be used to generate images. In such cases, information must be provided in particular that an AI system is active.

Deployers of certain AI systems also have transparency obligations in various cases (Article 50 (3) and (4) of the AI Act): On the one hand, the obligations apply to **emotion recognition systems** or systems for **biometric categorization**. On the other hand, the obligations also apply to the results of so-called **deepfakes**, the definition of which is broad and can therefore also include image generators. These requirements raise the question of whether and how

they can be handled sensibly, especially in areas such as journalism or Art.

AI systems with no particular risk

There are no obligations in the AI Act for all other AI systems. However, according to Article 95 AI Act, providers can voluntarily establish **codes of conduct**.

D. Our recommendations for you and your company to implement the AI requirements

For the development or use of AI systems in general and the implementation of the AI Act in particular, **we recommend that you start promptly with various measures** to safeguard yourself. This applies both if you expect to be classified as a provider or only as a deployer of AI systems. **Immediate measures** should definitely include checking **which risk class** your own AI systems fall into and implementing the **training obligations** under Article 4 of the AI Act that will apply from February 2025.

In detail, we recommend the following steps:

1. Analyze and determine all types of AI use: audit the AI tools used in the company

Create a list of all AI systems that are already in use in your company. This includes both internal and external systems that are used for different business areas. It can also include software that only contains individual AI functions or that is being newly introduced by the software provider. Identify the functions and purpose of each AI system. Consider that AI functions can be added to standard software as part of updates, which must be evaluated in detail. It can be assumed that such functionalities will be added to a large number of applications in the near future.

2. Examination of possible provider status

Document which AI systems you develop, distribute or put into operation under your own name within the scope of the AI Act definition. When taking over externally developed AI systems, it must be checked on a case-by-case basis whether you are to be classified as a provider or deployer.

3. Checking which obligations apply

Companies must determine and document at an early stage which obligations apply to them. Classification as a prohibited AI system and GPAI will only apply to individual cases. The classification of AI as high-risk AI can be relevant in any company, especially in the HR department. In any case, the transparency obligations must be checked and staff training on AI must be carried out. In detail:

- Check whether a potentially prohibited AI is being used and whether an exemption applies; for this purpose, the AI systems used should be compared with the list of prohibited practices with regard to the processing purposes
- If the AI system should be classified as a GPAI, analyze whether there is a systemic risk within the meaning of Article 55 AI Act
- Familiarize yourself with the extensive obligations that apply to providers and deployers of high-risk AI and GPAI (see above)
- Analyze all other AI systems in your company that could be classified as other AI and familiarize yourself with the transparency obligations.

4. Check whether AI systems are classified as high risk

Companies must check whether AI systems used in their operations (as providers or deployers) are considered high-risk AI. If this is the case for individual AI tools, there are various obligations, the implementation of which must be prepared in a structured manner. As a first step, documentation should be requested from the providers of the AI systems.

5. Implementation of the obligations

Once your company has identified the relevant obligations under the AI Act, it is important to plan and initiate concrete steps to implement these obligations. Here are some basic recommendations on how to proceed:

- Develop a detailed implementation plan that takes into account all identified obligations under the AI Act
- Define clear responsibilities and accountabilities for the implementation of each identified obligation
- An action plan should be drawn up for the implementation of the legally binding measures, which is individually adapted to the company and the AI systems used
- Offer training and awareness-raising measures for all employees who are involved in the implementation of the AI Act or use AI systems
- Record the measures and processes implemented in text form and update the documentation continuously.

6. Transparency requirements and training

In most cases, companies will offer or use AI systems that are designed to interact with humans. In these cases, you should prepare training for your employees on AI in general and the tools used in particular. Furthermore, the transparency requirements must be implemented (possibly in the context of the legal notice or privacy policy).

7. In addition: Consideration of further legal requirements

The requirements of the Ai-Act will apply in addition to the existing legal requirements and create new obligations. Irrespective of the new obligations, existing legal requirements and actual risks must therefore be considered. This includes, in particular, ensuring compliance with the GDPR and other data protection requirements, ensuring that copyrights are checked and that you protect your trade secrets. It is therefore important that AI systems are not used across the board, but that a review is carried out of systems that employees like to use and that a uniform policy is defined for the use of AI tools and functions in the company.

Further obligations may also arise in the future from the Data Act, which we will inform you about separately.

8. Recommendation: Creation of an internal AI policy

We recommend introducing a comprehensive internal AI policy now, independently of the AI Act, in order to uniformly address the legal hurdles of AI systems and ensure the implementation of the above-mentioned obligations. The guideline can regulate the selection, procurement and use of AI tools by employees and define requirements for the responsible use of AI as a user. In addition to the provisions of the AI Act, aspects such as labor, data protection, competition, copyright, trademark and patent law must be taken into account. You should also regulate whether and how your own or third-party trade secrets subject to special confidentiality may be processed and how these can continue to be protected.

We have already drawn up **AI guidelines** and comprehensive AI guidelines on the legal framework conditions for several clients and conduct **training courses** for managers and employees to develop and maintain the legally required **AI literacy**. We have also been advising clients on various **AI projects** for several years and offer company-specific **auditing** with regard to the obligations of the AI Act.

We would also be happy to support you in legally securing the use of AI in your company or the public sector entites.

Our experts for AI and data law

Dr. Matthias Lachenmann
Attorney-at-Law | Partner
Matthias.Lachenmann@bho-legal.com
☏ + 49 (0) 221 270 956 180

Dr. Philip Lüghausen
Attorney-at-Law | Partner
Philip.Lueghausen@bho-legal.com
☏ + 49 (0) 221 270 956 210

Gerhard Deiters
Attorney-at-Law | Partner
Gerhard.Deiters@bho-legal.com
☏ + 49 (0) 221 270 956 160

BHO Legal consults European and national authorities, public clients and private companies on all aspects of Technology Law. We focus on aerospace, research and development, IT and digitization, security and defense. Our practice focuses on national and international Procurement law, Contract law, Air and Space law, IT and Data Protection law, Intellectual Property law, as well as state aid law.

www.bho-legal.com

LinkedIn-Profil

BHO Legal – Baumann, Heinrich, Ortner Rechtsanwälte Partnerschaft mbB
Hohenstaufenring 29-37
50674 Köln
☏ + 49 (0) 221 270 956 0
🖷 + 49 (0) 221 270 956 222
cologne@bho-legal.com