alliuris

ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS.

AI – Legal Management in Practice

Ulrich Herfurth, Attorney at Law in Hanover and Brussels

June 2026

The rapid development of artificial intelligence (AI) has led to profound changes in the economy and society in recent years. Companies are increasingly using AI systems to automate processes, optimize decision-making and gain competitive advantages. At the same time, however, new legal, ethical and organizational challenges are emerging. Against this backdrop, the European Union has, for the first time, created a comprehensive legal framework for the use of AI with the so-called AI Act.

The EU AI Act came into force on 1 August 2024 and is regarded as one of the world's most ambitious regulatory projects in the field of artificial intelligence. The first binding provisions came into force as early as 2 February 2025. These early regulations include, in particular, a ban on certain particularly high-risk AI applications, such as systems for the biometric categorization of sensitive characteristics or for the social assessment of individuals. In addition, an obligation regarding so-called 'AI literacy' has been introduced, i.e. raising awareness and training staff in the use of AI systems.

Further key requirements have been added since 2 August 2025. These include governance rules, the introduction of so-called '*Notified Bodies*', comprehensive transparency and documentation obligations, and specific regulations for so-called *General Purpose AI (GPAI)*. Confidentiality and sanction provisions have also been clarified.

The AI Act will be fully implemented in stages by 2 August 2026, with transition periods until 2027 provided for certain systems. As this is an EU regulation, it applies directly in all Member States without the need for national implementation. Nevertheless, national authorities, such as the Federal Network Agency (*Bundesnetzagentur*) in Germany, have been designated as the competent bodies..

Timeframe	*Obligations for businesses*
from 1 August 2024	AI Act is in force, applicable in Germany
from 2 February 2025	Ban on certain AI applications, mandatory AI literacy
since 2 August 2025	Designation of authorities, establishment of governance, preparation for GPAI transparency
since 2 August 2025	GPAI obligations, reporting and transparency requirements, sanctions possible
from 2 August 2026	Obligations for high-risk AI systems commence
until 2 August 2027	Final obligations also apply to systems placed on the market before 2025

For businesses, this means they must address the requirements at an early stage. In addition to legal aspects, organizational and technical issues also play a key role. In particular, businesses must analyze their existing AI systems, assess risks and establish appropriate governance structures.

Obligations & Liability

The entry into force of the AI Act will impose extensive obligations on companies. One of the most important tasks is to create a complete AI inventory and categorize all systems in use. This involves checking whether they involve prohibited practices, general-purpose AI systems or high-risk applications. Prohibited systems must be discontinued immediately, whilst particularly strict requirements will apply to high-risk systems in future.

Another key aspect is the obligation regarding AI literacy. From February 2025, companies will be required to train their staff in the use of AI. These training courses are intended not only to impart technical knowledge but also to raise awareness of risks such as bias, data protection issues or a lack of transparency. This is particularly important as the misuse of AI systems can have significant legal and economic consequences.

Requirements regarding transparency and documentation have also increased significantly. In particular, providers of general-purpose AI models must provide detailed information about their systems, including technical documentation and details of training data. This serves to enhance the traceability and trustworthiness of AI systems. In addition, a voluntary 'Code of Practice' has been introduced to provide guidance to companies.

Furthermore, companies must establish appropriate governance structures. These include clear responsibilities, processes for complying with reporting obligations, and close cooperation with authorities. Internal control mechanisms and risk management systems are also required, particularly for high-risk applications.

Adherence to these regulations is not only a matter of compliance but also of liability. Breaches of the AI Act can result in substantial fines – up to €35 million or 7% of global annual turnover. This demonstrates that companies must take the new regulations seriously and implement them systematically.

Measures

To meet the requirements of the AI Act, companies should take targeted measures. There are three key areas of action: check-up, training and governance. Together, these form the basis for effective AI management within the company.

These three areas are interlinked and should not be viewed in isolation. Whilst the check-up enables an assessment of the current situation and a risk evaluation, training ensures the necessary expertise within the company. Governance, in turn, ensures that clear structures and processes are established to guarantee long-term compliance with the regulations.

Check-up

The first step involves creating a comprehensive AI inventory. The aim is to obtain a complete overview of all AI systems used or developed within the organization. This should take into account not only internal developments but also external tools.

As part of this check-up, a systematic survey of all relevant systems is carried out, involving various departments such as IT, data science, HR or sales. The systems are then categorized in accordance with the requirements of the AI Act. It is particularly important to

identify high-risk applications used, for example, in areas such as recruitment or critical infrastructure.

Another key component is the collection of metadata, such as information on manufacturers, versions, areas of application or training data. This information is crucial for subsequent assessment and documentation.

Building on this, an initial risk assessment is carried out. In particular, transparency, bias and security risks are analyzed. Systems with increased risk must in future undergo a detailed conformity assessment.

The result of this process is a central AI inventory, which is continuously updated as a 'living document'. It forms the basis for all further measures in AI management.

Training concept ("AI literacy")

Another key component is staff training. The aim is to provide a basic understanding of AI, as well as its opportunities and risks. The training should be tailored to the different roles within the organization. Developers, for example, require in-depth technical knowledge, whilst managers need to understand strategic and legal aspects.

The training content covers both basic knowledge of AI and the AI Act, as well as practical guidelines for action. Raising awareness of ethical issues is particularly important, for instance when dealing with bias or personal data.

The choice of suitable formats also plays an important role. E-learning courses are suitable for teaching the basics, whilst workshops and face-to-face sessions are particularly useful for key roles. Regular refresher courses ensure that knowledge remains up to date.

Another important aspect is the traceability of training. Companies should document which employees have participated in which training courses. This is particularly important with regard to potential audits.
The result is a structured training plan that covers both the delivery and the evaluation of the training measures.

Governance structure

In addition to the assessment and training, establishing a suitable governance structure is crucial. The aim is to create clear responsibilities and processes.

An important step is defining roles and responsibilities. This includes, for example, appointing an AI Compliance Officer who acts as an interface between technology, legal and management. In addition, an interdisciplinary body, such as an AI Risk Committee, can be established.

Furthermore, appropriate processes must be established. For example, new AI systems should only be introduced following a prior compliance review. Internal reporting channels for risks or incidents are also advisable.

Another important aspect is communication with regulatory authorities. Companies must ensure that they fulfil their reporting obligations and can respond quickly when necessary. This also includes preparing the relevant documents and reports.
Finally, continuous monitoring is required. This includes regular audits as well as monitoring systems that record and evaluate changes to AI systems.

The result of these measures is a comprehensive AI governance manual that is integrated into existing compliance and risk management systems.

Conclusion

In summary, the EU AI Act presents companies with new, complex challenges. At the same time, however, it also offers the opportunity to shape the use of AI in a systematic and responsible manner.

The three key areas of action – AI inventory, training and governance – form a solid foundation for implementing the requirements. Companies that establish appropriate structures at an early stage are not only better protected legally but can also strengthen the trust of customers and partners.

In the long term, it will become clear that professional AI management is not merely a regulatory obligation, but a crucial factor for success in the digital age. Companies that use AI responsibly can drive innovation whilst minimising risks. AI management thus becomes a central component of modern corporate governance.

+ + +

The Alliuris Group

The Alliuris Group consists of 20 law firms and 400 business lawyers within Europe, Asia and America.

Contact	Ulrich Herfurth Alliuris Communication
Web	www.alliuris.law
Mail	info@alliuris.org
Fon	+49-511-307 56-20
Fax	+49-511-307 56-21

IMPRINT

EDITORS: ALLIURIS A.S.B.L. ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS | BRUSSELS

MANAGEMENT: Luisenstr. 5, D-30159 Hannover
Fon +49-511-307 56-20, Fax +49-511-307 56-21

BRUSSELS · PARIS · LONDON · AMERSFOORT · UTRECHT · KNOKKE · LUXEMBURG · LYON · MADRID · BARCELONA · LISBON · MILAN · COPENHAGEN · HANOVER · ZUG · VIENNA · SALZBURG · MOSCOW MINSK · SOFIA · ATHENS · ISTANBUL · BEIJING · SHANGHAI · GUANGZHOU NEW DELHI · MUMBAY · NEW YORK · MEXICO CITY SAO PAULO · RIO DE JANEIRO · BRASILIA · BUENOS AIRES · LIMA

EDITORIAL DEPARTMENT
Ulrich Herfurth, Rechtsanwalt