YPOG Briefing:

Art. 4 AI Act: The Underestimated Challenge on the Road to AI Compliance

Berlin, January 27, 2025 | Anna Eickmeier, Charlotte Petrasch

After a lengthy legislative process that was influenced by a variety of different stakeholder interests, the EU Regulation on Artificial Intelligence (EU) 2024/1689 ("**AI Act**") entered into force on August 1, 2024. With its adoption, the European Union has set itself the ambitious goal of creating a harmonized legal framework for dealing with AI applications within the EU.

The AI Act pursues a risk-based approach that regulates AI systems and so-called general-purpose AI models along their entire value chain. As a result, the AI Act also addresses actors such as companies as so-called "deployers" that use AI systems without having developed or distributed them themselves.

Therefore, businesses now face the task of having to achieve AI compliance that is both economically appropriate and legally compliant. Notably, the first legal obligations of the AI Act will become legally binding **from February 2, 2025**. In particular, this applies to the rules on so-called "**AI literacy**" in accordance with Art. 4 AI Act. This provision entails new obligations which – in contrast to many other provisions of the AI Act – apply to **all providers and deployers** of AI systems regardless of any risk level that might be attributed to them under the AI Act. Hence, Art. 4 AI Act also applies to **companies that use and deploy AI systems, even if they only do so to a limited extent**.

In view of the imminent enforceability of the AI literacy obligations, the so-called Office for Artificial Intelligence, which the European Commission has established as part of the AI Act, has announced that it will hold a webinar on AI literacy on February 20, 2025 (see https://digital-strategy.ec.europa.eu/en/events/third-ai-pact-webinar-ai-literacy). Therefore, affected companies should seize the remaining time to address the upcoming obligations to pave the way for an AI literacy framework that is tailored to their individual needs.

The following article seeks to provide an overview of the upcoming obligations for providers and deployers of AI systems and show how successful AI compliance can be achieved, how the regulatory requirements of the AI Act can be taken into account and how the use of AI systems can continue to make economic sense.

1. What does "AI literacy" mean?

Art. 4 AI Act demands of providers and deployers of AI systems to

"*take measures to ensure, to their best extent, a **sufficient level of AI literacy** of their **staff** and other persons **dealing with the operation and use of AI systems on their behalf** [...].*"

In this context, "AI literacy" relates to the skills, knowledge and understanding that allows providers, deployers and affected persons to make an **informed deployment** of AI systems, as well as to gain awareness about the **opportunities and risks** of AI and **possible harm** it can cause, see Art. 3 No. 56 AI Act.

Thus, providers and deployers are responsible for the AI literacy of employees and related groups, such as freelancers. However, according to the wording of Art. 4 AI Act, these obligations also apply to other persons tasked with the operation and use of AI systems on behalf of addressees. In its recitals, the AI Act further broadens the scope of addressees: In particular, all "affected persons" and "actors in the AI value chain" should exhibit AI literacy to understand how AI-based decisions affect them (see recital 20). Therefore, it is currently difficult to predict with certainty which other affected persons, such as (depending on the individual area of application) customers or students, will be subject to the obligations outlined in Art. 4 AI Act in the future.

The level of AI literacy that is sufficient in each individual case should be determined by the **technical knowledge, experience, level of education and training** of those affected and the **context** in which the AI systems are used.

In view of this abstract explanation of the AI Act, it remains largely unclear which specific skills and knowledge are required to achieve sufficient and appropriate AI literacy. Moving forward, courts or the European Commission should therefore further clarify the undefined legal concept of AI literacy in a legally certain manner, such as through court decisions, interpretative guidance, or codes of conduct, thus bringing it to life with practical meaning.

However, providers and deployers of AI systems, who will be subject to the obligations from February 2, 2025, cannot afford to wait for such clarifications. Therefore, it is strongly advisable to take measures now to ensure AI literacy and mitigate potential liability risks.

2. Who are the addressees of the obligations?

The obligation to establish AI literacy applies to all providers and deployers of AI systems. Thus, Art. 4 AI Act covers a large number of AI use cases across industries and areas of application.

While "**providers**" are those actors who develop AI systems or have them developed and *place them on the market or put them into service* under their own name or trademark, "**deployers**" are those who *use* AI systems under their own responsibility**, *i.e.* any company that uses AI systems in a business context**.

Therefore, all companies that offer or provide AI systems for their employees must ensure that these persons use AI systems responsibly. This means that the mere use of in-licensed programs from third-party providers can be sufficient to trigger the obligations of Art. 4 AI Act. Consequently, the obligation to establish AI literacy will also extend to companies using software products that align with market standards, provided they employ AI-powered tools. This includes the increasingly widespread use of chatbot applications (such as ChatGPT or Microsoft Copilot) as well as AI applications in the field of programming, translations, recruitment processes, or accounting.

3. What practical measures should companies take to establish "AI literacy"?

An overall analysis of the AI Act's provisions on AI literacy reveals that the EU legislator is pursuing a holistic approach: AI literacy must not only encompass legal requirements, but also technical and ethical dimensions. Only in this way can the informed use of AI, as required, be effectively achieved.

Companies are expected to "*take measures*" to achieve AI literacy. Yet, the AI Act does not specify what these measures should entail. However, due to the legislative decision to establish a level of AI literacy that takes into account individual circumstances, the AI Act does not follow a "*one size fits all*" approach. Thus, the type and scope of the measures to be taken depend, *inter alia*, on the size of the company and the extent of its use of AI. Further, the level of risk of the individual AI systems should, in our view, also be considered when designing these measures.

In order to determine the type and scope of the necessary measures, companies should, *inter alia*, consider the following aspects, both individually for each AI system and as part of a holistic assessment of all AI systems in use:

- To what extent are AI systems currently in use, and how is their use anticipated in the foreseeable future?
- What tasks are the AI systems used for?
- How central are the AI systems to the company's workflows and business activities?
- Who interacts with the AI systems?

Such an assessment can represent the first step towards AI compliance. While the specific choice of measures will typically be determined on a case-by-case basis, it is nonetheless advisable to rely on certain categories of measures for practical implementation.

A range of different measures can contribute to holistic AI compliance. For instance, establishing dedicated points of contact for affected persons may be beneficial to provide specific guidance on handling AI tools, or to access further individual training. Furthermore, establishing processes for the documentation and handling of critical incidents can contribute to a comprehensive and sustainable AI compliance system that guarantees the protection of the rights and interests of all parties involved.

In the practical implementation of Art. 4 AI Act, however, particular attention should be paid to two key instruments: the (regular and recurring) **training of employees** (see 3.1) and the **introduction of internal AI guidelines** (see 3.2). Additionally, the **appointment of an AI officer** may be advisable in certain cases (see 3.3).

3.1. AI trainings

To ensure that all affected persons have sufficient AI literacy, conducting regular trainings is particularly advisable. Such trainings should aim at enabling personnel to harness the opportunities provided by AI technology responsibly while identifying and addressing potential risks at an early stage.

Therefore, teaching AI literacy must **be practical** and go beyond theoretical knowledge to foster a fundamental understanding of how AI systems operate and what their impact may be.

Companies should also tailor training content to its respective target group. Firstly, it is crucial to tailor trainings to the **individual level of knowledge** of the affected persons: For instance, a CTO will usually have more in-depth technical knowledge than employees from other departments may. In addition, training should be tailored to **the specific areas of application** of the AI systems: Different responsibilities within a company – from AI solutions to support developers to managers using AI tools in business operations or as a sales product – require a customized selection of compliance measures.

For instance, the use of AI systems in the context of job applications will require a different type and depth of information than AI systems used for the efficient analysis of Excel spreadsheets. What is more, the use of AI systems in direct customer interactions, such as in customer support, may require a different level of understanding and oversight compared to purely internal AI tools that streamline work processes but are not intended to provide users or third parties with specific assistance or make binding decisions.

Affected parties should understand training measures as an **iterative process**. This is particularly important in the context of the rapid technological developments of AI in the mid- and long-term: Alongside general introductions to the use of AI systems, companies should consider specific trainings in case of new systems, functionalities or areas of application. In addition, it may be beneficial to provide targeted training on a case-by-case basis, for example addressing any misuse or newly identified risks at an early stage.

Finally, a key approach to conveying the benefits and risks of AI applications – especially in case of first-time usage – can be the principle of "*learning by doing*". Such hands-on experience can be an effective means of developing the basic understanding of how AI systems work. Nevertheless, it is advisable to create learning environments for affected persons to explore these fundamentals under expert guidance.

3.2. AI guidelines

Furthermore, internal AI guidelines will likely constitute a central building block for the responsible and safe use of AI systems in organizations. Such guidelines may define the framework within which AI systems are used and, thus, provide personnel with clear guidelines.

A key purpose of these AI guidelines is to highlight the **risks and limits of AI use**. Users should understand which tasks an AI system can solve – and where its limits lie. In particular, it is important to raise awareness of the fact that AI systems, such as those that may generate text- or image-based content, can never guarantee this content's accuracy. A clear understanding of these limits helps to avoid misinterpretations and incorrect work results.

Furthermore, AI guidelines play a decisive role in the definition of **usage restrictions** (so-called "Acceptable Use Policies"). This way, companies may create awareness about the importance of not using AI systems for undesirable or harmful purposes. To develop AI guidelines that are both legally compliant and practicable, companies can initially rely on general guidelines already established for handling AI systems. For instance, companies can prohibit the input of trade secrets and personal data or explicitly exclude certain use cases, such as the use of AI for discriminatory or unethical purposes.

However, organizations should regard such standard concepts as a useful starting point, but not as a final product. This is because AI guidelines should always be adapted to the individual requirements of the individual business case concerned. Especially in complex or highly regulated industries, it is often advisable to make additional adjustments or obtain further expertise. This way, companies can further ensure that their AI-related instructions are in line with other regulatory areas, such as data protection or product liability law.

Furthermore, AI guidelines can provide employers with mechanisms under labour law in the event of violations of the Acceptable Use Policy. In this way, AI guidelines can serve not only as a tool for AI governance but also an effective means of legal protection.

Therefore, AI guidelines may complement the trainings mentioned before, as companies may constantly adapt them flexibly to new AI use cases.

3.3. Appointment of an AI Officer

Although the AI Act does not mention the position of a designated AI officer, such appointment can be another valuable measure to ensure the responsible use of AI systems and compliance with regulatory requirements: By creating such a position, expertise can be pooled and existing best practices from the context of data protection officers can be put to good use. In addition, – and in contrast to the requirements of the GDPR – the appointment of an AI officer does not create any specific legal obligations under the AI Act. Thus, an AI officer can act as a central link between technology, compliance and strategic business objectives.

The typical tasks of an AI officer can include, for example the

- Monitoring of AI compliance
- Carrying out of risk assessments
- Development of AI guidelines
- Organisation and responsibility for AI training courses
- Support of management and other business units in strategic decisions regarding the use of AI systems
- Point of contact for external organisations

Depending on the size and structure of the concerned company, it may also make sense to bring in an external expert with specific expertise as an AI officer.

Employing such a specialized contact person can create clarity and structure when dealing with complex issues relating to AI. For instance, an AI officer may act as a mediator between different departments and external stakeholders, thereby strengthening general confidence in the use of AI systems.

Regardless of the possible advantages of an AI officer, such appointment alone cannot be sufficient to establish a level of AI literacy that meets the requirements of Art. 4 AI Act: The understanding of AI systems and their effects must encompass all areas and stakeholders of a company – ranging from the management level to IT departments and operational teams. Therefore, appointing an AI officer should not be treated as a standalone measure but rather as part of a comprehensive and sustainable AI strategy that is future-proof.

4. Conclusion

Art. 4 of the AI Act emphasizes that AI literacy is an essential component of the legally compliant use of AI systems. Hence, companies should regard it as a central pillar of their (AI) compliance.

Due to its open and broadly phrased wording, the AI Act largely leaves it up to the providers and deployers of AI systems to develop measures to ensure AI literacy. In light of the imminent legally

binding nature of Art. 4 AI Act – effective as early as February 2, 2025 – companies should promptly analyze the scope of their AI use to develop measures that ensure AI literacy, thereby contributing to the development of best practices from the outset.

A recent presentation by the AI Office for the members of the so-called "AI Pact", a voluntary association of AI stakeholders committed to the early and responsible implementation of the AI Act, suggests that the European Commission may not begin enforcing the discussed obligations until August 2, 2025. Affected companies should take this (albeit non-binding) "extension of the deadline" as an opportunity to use the remaining time to meet their legal obligations.

AI literacy measures are not only a means of minimizing risk, but also an important basis for companies' long-term success. Successful internal AI governance ensures the smooth implementation of AI technology in existing workflows. Further, AI literacy documents a reliable and knowledgeable handling of AI to customers. Thus, companies may benefit greatly from this technology once the first steps towards AI compliance have been taken.

***