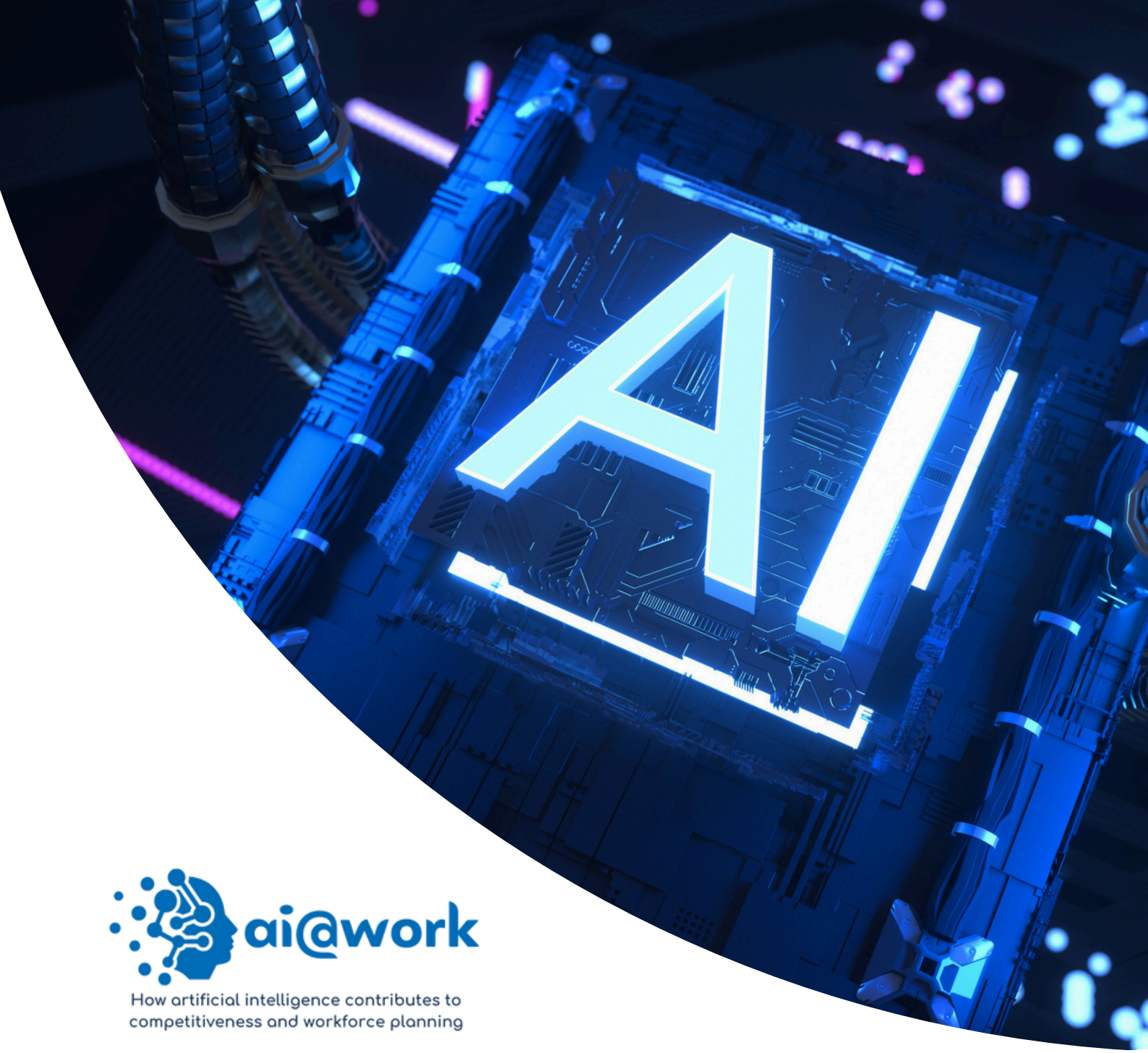

ai@work

How artificial intelligence contributes to competitiveness and workforce planning

AI regulation in the EU: implications for the workplace

ai@work
How artificial intelligence contributes to competitiveness and workforce planning

Table of contents

Introduction

Artificial Intelligence (AI) is a key technology with considerable economic and social potential. Companies in Europe can improve their efficiency if they succeed in deploying AI in corporate processes. However, beside significant benefits, AI applications may also harbour risks which may counteract European values, for example if AI supports discrimination or violates people's privacy. For this reason, AI is subject to specific regulation in the EU. A comprehensive regulatory framework – the AI Act – was introduced in 2024 that focuses on harmonising various AI-related regulations and establishing a standardised set of rules across the EU (Official Journal of the European Union, 2024). Companies in Europe that deploy or plan to implement AI must comply with this regulation. Besides the AI Act, further regulations exist that intersect with AI usage.

Objectives

The purpose of this fact sheet is to provide orientation on the relevant regulatory framework for AI with a specific focus on the workforce. It is intended to support companies in Europe that are planning to implement AI as they take the first steps towards fulfilling the related obligations.

Scope

Companies may apply AI for different purposes. They may use it for process optimisation, for example if AI robotics applications are deployed in production processes or if AI is used to support recruitment processes. In this sense, companies deploy AI for internal purposes. Likewise, companies may use AI for external purposes, for example if generative AI applications such as chatbots are provided to clients as part of the company's services. This fact sheet focuses on internal AI use and the associated obligations for companies.

Identifying the company's AI role

To identify a company's obligations with respect to AI, it first needs to define its **AI role**. The AI Act differentiates between:

1. **AI deployers** that use AI systems which were not developed in-house but were acquired from other companies, and
2. **AI providers** that develop AI systems themselves and/or place them on the market.

The key difference between the two roles is that AI providers are responsible for ensuring that the AI system complies with the AI Act before it enters the market, including technical documentation and risk assessments. In contrast, AI deployers are responsible for using the AI system properly, following the provider's instructions, monitoring its performance and reporting incidents during use. Essentially, providers focus on compliance during the development phase, while deployers focus on safe and lawful application.

A representative company survey conducted in 2024 revealed that most German companies use free or purchased AI tools and rarely develop AI tools themselves (Engels et al., 2025, 11). With an AI usage rate of 20 per cent, Germany has a higher AI usage rate than other EU Member States, compared to the EU average of 13 per cent (Eurostat, 2025). It is therefore likely that the proportion of AI providers in other EU countries is not significantly higher than in Germany. Given this context, this fact sheet focuses on AI deployers.

Regulatory requirements and obligations under the AI Act

The core of the AI Act is a risk-based approach that classifies each AI application into one of four **risk classes**:

1. AI applications of **unacceptable risk** are prohibited in the EU. An example is an AI system designed to infer emotions of a natural person in the workplace.
2. **High-risk** AI systems are subject to strict obligations. For example, deployers of high-risk AI systems such as AI tools to support recruitment processes must ensure human oversight and comply with strict transparency obligations and CE marking, which demonstrates that a high-risk AI system has passed a conformity assessment.
3. AI applications of **limited risk** such as chatbots or AI systems that generate deepfakes are subject to lighter transparency obligations in the sense that end-users have to be informed that they are interacting with AI.
4. AI systems of **minimal risk**, such as AI-enabled video games and spam filters that account for most AI applications currently available in the EU are unregulated (Official Journal of the European Union, 2024, 39).

To comply with the AI Act, it is crucial that companies in Europe first determine the risk class and the associated obligations of each of its AI applications.

AI-based human resources (HR) services are often classified as high risk (Official Journal of the European Union, 2024, 127). One example of such a service is a CV-scanning tool that ranks job applicants and evaluates candidates. At the same time, these AI systems are generally of great benefit to companies. They can assess the skills of the existing workforce, allowing companies to better understand their in-house talent and how to develop it more effectively, for example (WEC, 2023). Employees can also benefit if AI-based HR services help them to understand their own skills profile and the way that profile can best be developed to achieve their career goals.

However, these AI tools carry the risk of biased or discriminatory decisions. Discrimination patterns could be reproduced or reinforced due to the training data used, as the Amazon case demonstrated in 2014. In this case, a machine-learning algorithm designed to review CVs and propose suitable candidates systematically discriminated against women applying for technical jobs, such as software engineering positions, as the existing pool of Amazon software engineers was predominantly male, and the AI tool was fed data from the CVs of these engineers (ACLU, 2018).

To mitigate these risks, there are several **obligations for deployers of high-risk AI systems**, according to Article 26 of the AI Act. These include, for example:

1. The AI tool must be used strictly as instructed by the provider.
2. The AI deployer must ensure humans review and control input data.
3. Employee representatives and the affected employees or applicants must be informed that AI is used, and companies must explain the role of the AI.
4. System logs must be preserved for accountability purposes.
5. The AI deployer must monitor performance and report any incidents to the AI provider and to the relevant market surveillance authorities.

AI literacy and other obligations under the AI Act

According to Article 4 of the AI Act, AI providers and deployers must take measures to ensure a sufficient level of **AI literacy** of their workforce from February 2025 onwards, regardless of the risk class. To meet this requirement, companies can define practical and binding guidelines for using AI tools properly or offer training programmes, for example (ifaa, 2025). In addition, employees with existing AI knowledge and experience can play a central role as multipliers by sharing practical knowledge. Companies can also hire new employees with a high level of AI literacy (Büchel et al., 2025).

In general, developing AI applications is rather complex and requires specific technical knowledge. From a corporate perspective, building up literacy for AI development can therefore be more costly than building up literacy for AI deployment, especially when it comes to modern generative AI applications that are typically easy to use without extensive prior knowledge and specific expertise. So far, it remains unclear what consequences companies can expect if they do not fulfil the requirement for AI literacy.

Even in the absence of strict consequences, it is important that companies mandate the prudent use of AI applications in order to proactively address regulatory requirements. For example, information entered into AI-based chatbots must comply with **data security and copyright laws.** It is crucial that companies draw up guidelines for protecting trade secrets before AI chatbots are used so that employees do not enter sensitive data into generative AI applications. This applies to both personal and non-personal data because generative AI applications might use the data as training data.

Data privacy and data storage obligations under the GDPR

Depending on what data is used by AI systems, companies may need to comply with additional regulations, such as the **General Data Protection Regulation** (GDPR, Official Journal of the European Union, 2016). This covers the processing of personal data. Such data must be processed lawfully and transparently. Deploying AI in the workplace may involve the collection and processing of employee data which raises concerns about data protection and privacy and requires careful consideration in its management. The GDPR also applies in case of AI use: companies are only allowed to process personal data with the consent of the persons concerned. AI systems, such as HR service applications, which process such data, as well as AI applications used in production processes may fall under the GDPR. This may be the case if data from productivity monitoring or workplace surveillance, including surveillance of employees themselves, is processed, for example (Paliokaitė et al., 2025). Companies using AI in the workplace must therefore navigate the interaction between different legislations carefully to be fully compliant.

Additionally, **data storage** outside the EU and unclear **data ownership** or control over data used by AI tools can expose AI deployers to further compliance, transparency and accountability risks, especially when using cloud-based AI tools from providers that are located outside the EU. If the AI provider stores or processes data outside the EU, the AI deployer still remains responsible for ensuring GDPR compliance. The AI deployer must inform natural persons whose data is stored that way of where and how their data is stored and processed. This may result in data security and sovereignty concerns.

The role of social dialogue

Employees, just as the management, may have reservations about AI. A representative company survey conducted in 2024 showed that one in three German companies cites a lack of willingness to change within the company as an obstacle to its AI use (Scheufen et al., 2025). **Reservations** can arise if employees are worried that AI could increasingly take over their work activities, for example. However, the results of another international employee survey in the financial and manufacturing sectors show that the majority of employees rate AI positively (Lane et al., 2023). Nevertheless, existing reservations against AI should not be underestimated, as employees might ultimately be required to work with AI. Teaching AI competencies and ensuring that employees receive timely, clear and accessible information on how AI systems function and how they affect their work may reduce these reservations (ifaa, 2025).

Employee representatives can help to address the reservations of employees towards AI and agree on a fair, transparent and sensible use of AI within companies. Therefore, a close, trusting relationship between company management and employee representatives may, in some companies, support implementation of AI in the workplace. However, it is likewise possible that employee representatives may also actively resist or delay the introduction of AI, for example if they lack a sufficient understanding of the strategic importance of AI implementation. In some EU Member States such as Germany companies must inform works councils of any planned AI deployment (BMJV, 2024). In Spain, the so-called "Rider Law" granted works councils the right to be informed about the parameters, rules, and instructions governing algorithms or AI systems that impact working conditions, hiring, or retention (Boletín Oficial del Estado, 2021). In addition to these options, it is conceivable that there might be relevant provisions under collective agreements. With regard to high-risk AI systems, Article 26(7) of the AI Act stipulates that AI deployers shall inform employee representatives and the affected employees that they will be subject to the use of the high-risk AI system before putting it into service or using it at the workplace.

Overcoming existing reservations about AI is crucial as an even greater risk to job opportunities, employment protection and the welfare of individuals in Europe lies in the failure to effectively implement AI in business. If companies in Europe do not fully harness the productivity and efficiency gains offered by AI, this will undermine competitiveness, threaten job creation, limit wage growth, and ultimately weaken the European social model.

Conclusion

AI represents a **huge opportunity for companies**. However, there are many areas in the workplace where regulatory requirements need to be met to realise this opportunity. These regulations result in costs for compliance that pose challenges. To ensure compliance, companies can build up the necessary expertise themselves or seek advice from legal or IT service providers.

Furthermore, AI deployment in the workplace involves several **transaction costs**, including raising awareness among the workforce and establishing a company-wide information structure regarding proper AI use. Some employees may still perceive AI as a threat to their jobs rather than a tool that could support them. Demystifying AI is therefore essential to enable all sectors across the value chain to fully embrace AI.

In addition, employee **training** and the development of the necessary **skills** for the employees is key. Legal and IT service providers can help companies to overcome these challenges. Depending on the specifics, public sector support might also be possible.

Generally, **companies urgently need to provide employees with clear rules** on the use of AI, for which companies themselves may require guidance. In total, this can enable a greater use of AI in the EU, ensuring that AI is used in a compliant way, avoiding undesirable risks and exploiting the potential of AI to a larger extent.

Literature

- ACLU – American Civil Liberties Union, 2018, Why Amazon's Automated Hiring Tool Discriminated Against Women, https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against [07.08.2025]
- Boletín Oficial del Estado, 2021, Real Decreto-ley 9/2021 para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de plataformas digitales, Madrid
- BMJV – Bundesministerium der Justiz und für Verbraucherschutz, 2024, Betriebsverfassungsgesetz, Berlin
- Büchel, Jan / Engler, Jan Felix / Mertens, Armin, 2025, KI-Jobs in Deutschland: Stagnation statt Boom. Eine Analyse von Online-Stellenanzeigen. Study on behalf of the Bertelsmann Stiftung (Hrsg.), Gütersloh
- Engels, Barbara / Scheufen, Marc / Schmitz, Edgar, 2025, Artificial Intelligence as a Competitive Factor for the German Economy. Empirical Findings and Policy Recommendations for the Use of AI in German Companies, IW-Report, Nr. 33, Köln
- Eurostat, 2025e, Artificial intelligence by size class of enterprise [isoc_eb_ai], https://ec.europa.eu/eurostat/databrowser/product/page/ISOC_EB_AI [18.07.2025]
- ifaa – Institut für angewandte Arbeitswissenschaft e. V., 2025, EU AI ACT. Was Artikel 4 für Unternehmen bedeutet, Düsseldorf
- Lane, Marguerita / Williams, Morgan / Broecke, Stijn, 2023, The impact of AI on the workplace: Main findings from the OECD AI surveys of employers and workers, OECD Social, Employment and Migration Working Papers, Nr. 288, Paris
- Paliokaitė, Agnė et al., 2025, Study exploring the context, challenges, opportunities, and trends in algorithmic management – Final report. Publications Office of the European Union, Luxembourg
- Official Journal of the European Union, 2024, Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence, Brussels
- Official Journal of the European Union, 2016, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, Brussels
- Scheufen, Marc / Engels, Barbara / Schmitz, Edgar, 2025, Artificial Intelligence in the German Economy – An Empirical Survey of Companies' Aims, the Obstacles Encountered and the Perceived Cost-benefit Ratio, in: IW-Trends, 52. Jg., Nr. 2, S. 67-86
- WEC – World Employment Confederation, 2023, Code of Ethical Principles in the use of Artificial Intelligence, https://wecglobal.org/uploads/2023/04/AI-principles-WEC-AI-Code-of-Conduct-March-2023.pdf [16.07.2025]

ai@work
How artificial intelligence contributes to competitiveness and workforce planning

Contact us

Website
www.eei-institute.eu/publications/project/ai-work/

E-mail
info@eei-institute.eu

Author: **Jan Büchel** (German Economic Institute)

LinkedIn
European Employers' Institute

Published by: **EEI, 2025**

Ai@Work Consortium:

Coordinated by:

Ceemet European Tech & Industry Employers

Co-partners:

iw ifaa EEI European Employers' Institute

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.