12 Jan 2026

--> Logo

European Union: The EU Artificial Intelligence Act - Key takeaways for HR

02 Aug 2024 | 7 minute read

Artificial Intelligence | AI | TMT Featured Content

In brief

The use of AI in the workplace and its potential to influence or make decisions affecting individuals, perhaps without their knowledge, brings with it many ethical and regulatory considerations for employers.

Although data privacy and employment rights obligations already apply, systems using AI will be subject to more comprehensive regulation by the EU Artificial Intelligence Act ("**Act**") with significant fines in the event of non-compliance.

Potentially touching many areas of a business operation, we pull out some of the key provisions of the Act that will be relevant to organizations in their capacity as employers.

Key takeaways

Background

The Act is part of a wider European Commission 'Data Strategy'. Broadly, this aims to provide a sound legal framework that enables investment and innovation in the development and use of safe and trustworthy AI systems across the EU's single market while ensuring respect and protection of fundamental rights of EU citizens.

Where does it apply?

The Act applies not only to organizations within the EU but also those based outside it where they deploy an AI system in any EU member state; this means many multinational companies will be caught by its provisions.

Provider of an AI system or deployer?

There are significantly more obligations on those organizations that are 'providers' of AI systems – broadly those that develop AI systems - than those that use or 'deploy' them. In most cases, an organization implementing or maintaining an HR related AI system will be a deployer rather than a provider; we focus below on some of the key obligations for deployers.

It's important to note, however, that in some circumstances, an employer could be deemed to be a provider of an AI system and subject to more extensive obligations. This could be the case where it customizes or modifies an existing AI system or puts it into service under its own name or trademark.

AI literacy

Both providers and deployers are required under the Act to ensure a sufficient level of AI literacy among any of their staff using the relevant AI system or anyone using it on their behalf. Although this will be contextual, broadly employers will need to ensure that anyone using AI systems within their operation is trained on the relevant system and aware of the opportunities and risks of AI and the possible harm it can cause. This will be an ongoing responsibility from recruitment onwards with records kept of completion of training in order to demonstrate compliance.

Interaction with data protection obligations and employment rights

Given the heavy reliance of AI systems on processing personal data there are many points of overlap between the Act and the General Data Protection Regulation (GDPR).The data protection principles will be relevant throughout the lifecycle of the AI system; these include obligations on lawful processing of data, transparency around processing, accuracy of data, purpose limitation, data minimization, storage limitation and integrity and confidentiality requirements. Carrying out a data protection impact assessment will almost certainly be required and GDPR provisions around automated decision making and rights to require human intervention or challenge a decision are likely to apply.

The potential for discrimination risks as result of AI systems is ever present and although there are obligations on providers to take steps to mitigate these when developing an AI system, employers will need to be alert to the bias and fairness issues and how those with protected characteristics could be adversely impacted.

Increased risk, increased regulation

The Act takes a risk-based regulatory approach and categorizes AI systems into different risk levels; the higher the risk, the higher the compliance standard for the relevant system.

Where a system has been identified as posing an 'unacceptable risk', it is prohibited; this includes the use of AI-based emotion-recognition systems in the workplace.

Of particular relevance for employers is that the Act expressly categorizes as 'high risk' those AI systems that are used for recruitment, in particular to place targeted job advertisements, analyze and filter applications and evaluate job candidates. The same is true for AI that enables monitoring and evaluation of performance, allocates tasks based on individual behavior or personal characteristics and makes decisions on promotion, termination or the terms that apply to a working relationship. While some AI systems that would otherwise be

high risk could fall outside this category where certain conditions are met, an employer would need to explain and document its reason for treating a particular system as outside the scope of the high risk regulatory requirements.

Helpfully, the European Commission is required under the Act to provide guidance on the classification of AI high risk systems; this is to include a list of examples of those that are high risk and those that are not. Codes of conduct are also to be developed by the new European AI Office.

In some instances, the use of AI systems will present a 'limited risk' – chatbots used for employment-related questions could fall into this category – and although there are fewer regulatory requirements, transparency obligations still apply.

Regulatory requirements for 'high risk' systems

The use of high-risk AI systems will trigger a set of obligations on deployers under the Act in addition to those that apply under the GDPR and other employment rights obligations.

These include:

- Informing job applicants and workers that that they will be subject to the use of a high risk AI system. Worker representatives also need to be informed of this.
- Taking appropriate technical and organizational measures to ensure the system is used in accordance with instructions.
- Assigning human oversight of the AI system to individuals with sufficient competence, training and authority.
- Ensuring that any input data is relevant and sufficiently representative taking into account the purpose of the system.
- Monitoring its operation on an ongoing basis and where a relevant risk is identified, complying with appropriate notification requirements e.g., to the provider, market surveillance authority.
- Providing a clear and meaningful explanation of the role of the AI system in the decision-making process where requested by anyone subject to a decision which has legal effects or an adverse effect on health, safety or fundamental rights.
- Retaining logs generated by the system to the extent that these are under the deployer's control.

Worker representatives

In some jurisdictions, introduction of new technology that impacts the workforce will trigger information and consultation obligations with worker representatives under local law; in some cases their consent to implementation may be required. This is the case in Austria, for example, where in the absence of the required agreement, the works council can enforce the deactivation of the AI system via a court ruling and in some cases even via a preliminary injunction. Early engagement with worker representatives is therefore advisable.

Costs of non-compliance

Fines of up to 35 million euros or 7% of global annual turnover whichever is the higher could be payable for non-compliance with the Act in some circumstances. This is in addition to any fines applied for breach of the GDPR and any compensation awarded in relation to breaches of equality or any other employment rights.

Getting ready for the Act

Ensuring AI regulatory compliance will be a cross-organization project. From an HR perspective it will be important to feed into that project and have a general awareness of the applicable regulatory requirements, bearing in mind that adoption of AI systems and its impact can be a particularly sensitive issue for the workforce and its representatives.

A good understanding of where AI systems are used in the employment sphere, how they work and where they sit in terms of risk will help to equip HR professionals for relevant discussions with key stakeholders and assist with understanding, explaining and assessing the impact on the workforce.

Some other action points aimed particularly at HR and others with workforce responsibilities include the following:

- Develop and implement relevant workforce training for anyone using an AI system. This should also cover related data protection and employment rights.
- Determine the risk category which will apply to the proposed AI system and the related obligations.
- Engage with worker representatives well in advance of implementing AI systems and check in which jurisdictions information, consultation and co-determination rights may apply as that will impact implementation timescales.
- Develop appropriate workforce policies e.g., about responsible use of AI; the process to challenge an AI-generated decision and the circumstances in which it applies.
- Continue to monitor AI use and the evolving legislative and social landscape to ensure HR policies remain up to date.
- Look out for guidance/codes of conduct from the European Artificial Intelligence Office and the European Commission.

European AI Office | Shaping Europe's digital future.

Contact Information

Antonio Luigi Vicoli
Partner
Milan
Read my Bio
antonioluigi.vicoli@bakermckenzie.com

Francesca Gaudino
Partner
Milan
Read my Bio
francesca.gaudino@bakermckenzie.com

Andrea Haiden
Associate
Vienna
Read my Bio
andrea.haiden@bakermckenzie.com