



Artificial Intelligence and Human Resources in the EU: a 2026 Legal Overview

What You Need to Know

Key takeaway #1

Many AI tools deployed for HR purposes are likely to be classified as "high risk" under the AI Act, triggering strict obligations for employers, including mandatory human oversight and transparency requirements toward employees and their representatives. Full application of these obligations was initially scheduled for August 2026.

Key takeaway #2

The European Commission's Digital Omnibus package, currently under discussion, proposes to make the application of high-risk AI system obligations conditional on the availability of harmonized technical standards. In the absence of a Commission decision confirming such standards, the deadlines would be set no later than December 2027 or August 2028, depending on the classification of the high-risk system.

Key takeaway #3

Regardless of any postponement of AI Act deadlines, Article 26(7) of the AI Act and applicable national legislation already require employers to inform and consult employee representative bodies prior to deploying high-risk AI systems. In Belgium, Collective Bargaining Agreement No. 39 of December 13, 1983 imposes a prior consultation obligation when new technologies have significant collective consequences on employment or working conditions.

Client Alert | 6 min read | 02.24.26

The year 2026 marks a major regulatory turning point for European companies using or considering the use of artificial intelligence in their human resources (HR) processes. The **Regulation (EU) 2024/1689 on artificial intelligence** (the AI Act) is entering a critical implementation phase, while the European Commission's "Digital Omnibus" package will clarify several obligations and modify certain deadlines.

As announced during our webinar on November 24, 2025 on AI in the Workplace, we are launching a series of alerts dedicated to AI issues in HR. This first publication provides an overview of current regulatory developments and their impact on the HR function. Our upcoming alerts will examine, among other topics:

- Algorithmic transparency and the fight against bias in HR systems
- AI literacy under the AI Act: scope and limits of employer training obligations
- Personal data processing at the intersection of the GDPR and the AI Act
- AI-based workplace surveillance: how far can employers go?

1. The Regulatory Framework: The AI Act and Its Risk-Based Approach

Entered into force on August 1, 2024, the AI Act establishes a harmonized framework at the European level for the use of AI systems. Its philosophy follows a risk-based approach.

1.2 The Four Risk Levels

Unacceptable risk

AI systems are prohibited when they risk posing a serious threat to the EU's fundamental values. These include:

- Social scoring systems
- Emotion recognition in certain contexts (particularly in the workplace and in education)
- Exploitation of vulnerabilities of specific groups

High risk

An AI system is classified as high risk when it is used in sensitive areas likely to significantly affect the rights of persons, such as education, public safety or recruitment. HR applications are explicitly identified among high-risk areas. Examples of such high-risk AI applications notably include:

- Automated candidate selection
- Performance evaluation
- Workplace monitoring
- Employee turnover prediction systems
- Decision-making relating to promotion or termination of contracts

Limited risk

An AI system is classified as limited risk when it can be used safely subject to specific transparency obligations. Users must be informed that they are interacting with an AI system, and AI-generated content must be appropriately marked.

Examples include:

- Self-service portals equipped with AI algorithms
- HR chatbots
- Virtual assistants for employees

Affected employees must be informed that they are interacting with an AI system.

Minimal risk

This category covers all other AI systems not falling into the above categories. This includes, for example, spam filters to prevent unwanted emails. The vast majority of AI systems currently used in the EU fall into this category. For such systems, no particular regulatory requirements are imposed but other contractual and legal obligations should still be observed.

1.3 Focus on High-Risk Systems in the HR Sector

Many AI tools specifically deployed in human resources should be classified as high risk. Initially, the full application of obligations relating to these systems provided for in Chapter III was expected in August 2026. However, this deadline is subject to discussions within the framework of the Omnibus procedure (see below).

1.4 Obligations of Employers Deploying High-Risk AI Systems

Companies using such systems must comply with a set of strict requirements established by the AI Act, including but not limited to:

Mandatory human oversight

The AI Act requires that high-risk AI systems be designed and used in a way that allows for effective human oversight. This means:

- Persons responsible for this oversight must be properly trained and qualified
- Ongoing training is required to maintain compliance over time
- Supervisors must have the effective capacity to intervene and modify the system's decisions

This obligation is distinct from but reinforces the GDPR's Article 22 right not to be subject to a decision based solely on automated processing.

Transparency and information obligations

Before deploying a high-risk AI system, Article 26(7) requires the employer to inform in a clear and comprehensive manner:

- Employee representatives (works council, trade union delegates)
- Directly affected employees

National provisions relating to the consultation of representative bodies must also be complied with.

2. The Impact of the "Digital Omnibus" Package

On November 19, 2025, the European Commission presented its "Digital Omnibus" package, aimed at revising and harmonizing key EU legislation relating to the digital single market. This initiative pursues several objectives: closing regulatory gaps, eliminating overlaps, and strengthening legal certainty for companies, particularly SMEs and SMCs (small mid-caps). In addition, a separate legal proposal within the package introduces amendments to the AI Act, seeking to facilitate the smooth and effective application of the rules for a safe and trustworthy development and use of AI.

The Omnibus package contains several relief measures for companies. The most significant element for HR departments concerns the AI Act-GDPR articulation. The interaction between the two texts raises numerous practical questions, which should be clarified.

Furthermore, the application deadlines for requirements relating to high-risk systems will be changed. Rather than a fixed date (August 2026), the entry into force of obligations provided for in Title III would be conditional on the availability of harmonized technical standards and compliance tools developed by European standardization bodies. Concretely, these obligations would only become applicable six or twelve months after a Commission decision confirming the availability of relevant standards, depending on the system category. In the absence of such a decision, the deadlines would be set no later than December 2027 or August 2028, depending on the classification of the high-risk system. According to the Commission's projections, this postponement could be up to 16 months, pushing back certain key deadlines to December 2027.

Important: the Omnibus package remains a proposal subject to the trilogue process (EU Council and European Parliament). Companies must therefore continue to prepare for a potential entry into force as early as August 2026, while closely monitoring the evolution of legislative negotiations.

3. Social Dialogue: An Enduring Imperative

Even if certain AI Act application deadlines are postponed, the involvement of employee representatives will remain an absolute priority in 2026. AI is perceived not solely as a work-facilitating tool, but also as a potential threat to job security and working conditions.

3.1 Mandatory Consultation

In most Member States, the introduction of new AI systems, particularly in the HR field, requires prior consultation with employee representative bodies pursuant to both Article 26(7) of the AI Act and applicable national legislation. This process should ideally be conducted before costly systems are acquired.

By way of illustration, in Belgium, Collective Bargaining Agreement No. 39 of December 13, 1983 requires that an employer who decides to invest in new technologies with significant collective consequences in terms of employment, work organization, or working conditions must consult with worker representatives on these social consequences.

In light of these issues, it is therefore strongly recommended that employers adopt a proactive approach by engaging in constructive dialogue with employee representatives well in advance of deploying any AI system.

The development of an AI policy defining the rules for the use of artificial intelligence within the company constitutes a judicious approach. This document can serve as a common reference and reassure stakeholders regarding the oversight of these technologies, while demonstrating the company's commitment to ethical and responsible use of AI.

4. Practical Recommendations

In this rapidly evolving regulatory context, companies are invited to undertake the following actions:

- **Map** all current and future AI systems and classify them according to the risk categories established by the AI Act, identifying, in particular, any high-risk AI systems
- **Train** HR and IT teams on the joint requirements of the AI Act and GDPR
- **Perform impact assessments** before adopting new AI tools
- **Establish** regular dialogue with employee representative bodies to anticipate concerns and build a climate of trust
- **Actively monitor** the evolution of discussions relating to the Omnibus package at the EU Council and European Parliament level

For any questions concerning the adoption of AI within your company, please do not hesitate to contact our team.

Contacts

Emmanuel Plasschaert

Partner

Brussels D | +32.2.282.4084

eplasschaert@crowell.com

Sari Depreeuw

Partner

Brussels D | +32.2.282.18.49

sdepreeuw@crowell.com

Evelien Jamaels

Partner

Brussels D | +32.2.214.2814

ejamaels@crowell.com

Sofiane Fergali

Associate

Brussels D | +32.2.214.2850

sfergali@crowell.com

