

RocaJunyent

Report

Labour Law and
Data Protection and Technology



The AI Act is already binding on companies: key points for its application in people management

The AI Act is now in force

Regulation (EU) 2024/1689 on Artificial Intelligence (hereinafter the “**AI Act**”)¹ is not a piece of legislation that affects only technology companies. It establishes a binding legal framework for any organisation using AI systems and applies across the entire AI value chain, covering, among others: (i) providers, who develop or market AI systems; (ii) deployers, who use AI systems under their own authority (a category which includes most companies that use AI tools in people management); and (iii) importers and distributors, who place AI systems on the Union market or otherwise make them available within it.

¹Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Regulation), available at: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81079>

“

The regulatory framework is sufficiently established to take action: if your company uses AI in people management and has not yet begun its compliance process, now is the time.



Timetable for the implementation of the AI Act



2 February 2025

Absolute prohibitions (Art. 5)

→ Restrictions on certain AI practices deemed unacceptable come into force.



2 August 2025

General-purpose AI models (Chapter V)

→ Obligations for providers of general-purpose models come into force.



2 August 2026

High-risk systems (Annex III, point 4)

→ The obligations for high-risk AI systems, including those in the workplace, are fully enforceable.

It is also important to bear in mind that, given the regulatory and operational complexity of the AI Act, the European Commission itself has proposed an extension of deadlines and a simplification of obligations in the so-called Digital Omnibus Regulation on AI², which is currently making its way through the legislative process. If approved – as is expected before August this year – the date from which the obligations apply would be pushed back and proportionality requirements would be adjusted for smaller operators, which could partially alter this timetable and the expectations of the various market players.

In the workplace, the AI Act has a particularly significant impact in two areas. First, among the absolute prohibitions already in force, of particular note is the ban on the use of AI systems designed to infer the emotions of natural persons in the workplace (Article 5.1.f of the AI Act), as well as biometric categorisation systems that infer specially protected characteristics such as race, political opinions or sexual orientation. Second, Annex III, point 4 of the AI Act classifies as high-risk all systems used in employment, the management of workers and access to self-employment, distinguishing between two categories: (a) systems intended for the recruitment or selection of individuals, in particular for publishing targeted job advertisements, analysing and filtering job applications, and assessing candidates; and (b) systems intended to inform decisions affecting the terms and conditions of employment or the promotion or termination of employment contracts, the allocation of tasks based on individual behaviour or personal traits or characteristics, or the monitoring and assessment of individuals' performance and behaviour within the context of such employment relationships. Notwithstanding the timetable set out above, organisations wishing to assess the use of systems that may fall within these categories should begin their compliance strategy now.

² REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the application of harmonised rules on artificial intelligence (Digital Omnibus Regulation on AI), available at: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52025PC0836>

The regulatory framework is sufficiently established to take action: if your organisation uses AI in people management and has not yet begun its compliance process, now is the time.

Classification of HR tools as high-risk systems

In practice, the high-risk classification may affect tools that your organisation has already implemented: your CV-screening ATS, your performance appraisal platform, the system that assists with promotion or dismissal decisions, and even AI modules integrated into your ERP or payroll software.

Classification as a high-risk system triggers a set of obligations for providers and deployers. The AI Act requires, among other things, the implementation of a risk management system throughout the system's lifecycle (Article 9 of the AI Act), automatic logging of events to ensure traceability (Article 12 of the AI Act), a pre-deployment conformity assessment (Articles 43 et seq. of the AI Act), enhanced transparency and information obligations towards data subjects (Article 13 of the AI Act), the governance of training data and bias control (Article 10 of the AI Act), and effective human oversight of the system's decisions (Article 14 of the AI Act). For more detailed information on the scope and practical application of these obligations, please consult the guidelines published by the Spanish Artificial Intelligence Supervisory Agency ("AESIA") at <https://www.aesia.gob.es>.

In practice, compliance with these obligations entails a significant administrative burden and requires a precise understanding of the requirements applicable to each system. The first step – and the most practical and effective one – is to establish an internal classification system that enables: (i) identification of which tools constitute AI systems for the purposes of the AI Act and which do not; (ii) identification of which of them fall within any of the absolute prohibitions set out in Article 5 of the AI Act; (iii) determination of the applicable risk category (and whether they qualify as high-risk systems under the AI Act); and (iv) mapping of the obligations that apply to each category within that classification. Without this preliminary exercise, any compliance strategy will be incomplete.

Even where a system is not high-risk, certain obligations already apply

It should not be forgotten that the AI Act is not the only regulation to consider. A company may formally comply with the AI Act and yet still face penalties from the Labour Inspectorate, the invalidation of internal policies and legal proceedings. Spanish law imposes its own obligations, which apply in addition to those under the AI Act, and failure to comply has already had real consequences in the courts (including, among others, under the Organic Law on Data Protection³ ("LOPDGDD"), amendments to the Workers' Statute⁴ ("ET"), and the Remote Working Act⁵). Some of the most relevant are:

- **Art. 64.4.d) ET (algorithmic transparency):** The works council has the right to be informed of the parameters, rules and instructions on which algorithms or artificial intelligence systems are based where they affect decision-making that may have an impact on working conditions, access to and retention of employment, including profiling. The provision was introduced in connection with the phenomenon of digital platforms, but its scope is general: any company using algorithmic systems that have an impact on employment is subject to this obligation.
- **Articles 87.3, 89 and 90 of the LOPDGDD and Royal Decree-Law 9/2021:** Workers have the right to privacy when using digital devices made available to them by their employer. The employer may access the content solely to monitor compliance with employment obligations, but must first establish criteria for use that respect minimum standards of privacy protection — with the involvement of workers' representatives in their drafting — and inform workers of these criteria.

³ Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights. Available at: <https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf>

⁴ Royal Legislative Decree 2/2015 of 23 October, approving the consolidated text of the Workers' Statute Act. Available at: <https://www.boe.es/buscar/act.php?id=BOE-A-2015-11430>

⁵ Act 10/2021 of 9 July on remote working. Available at: <https://www.boe.es/buscar/act.php?id=BOE-A-2021-11472>

- **GDPR, Act 31/1995 on Occupational Health and Safety and Organic Law 3/2007 on Effective Equality between Women and Men:** Data processing in performance appraisals triggers impact assessments, and algorithms that replicate biases based on gender, age or ethnic origin give rise to liability under equality legislation and regulations on the prevention of psychosocial risks.

"It is not enough to comply with the AI Act in isolation: a compartmentalised approach creates compliance gaps and increases legal exposure."

“

It is not enough to comply with the AI Regulation in isolation: a compartmentalised approach creates compliance gaps and increases legal exposure.

The practical implication is clear: it is not enough to comply with the AI Act in isolation. A compartmentalised approach – one that addresses the AI Act without considering the Workers' Statute, or that reviews data protection without assessing the impact on collective bargaining – creates compliance gaps and increases legal exposure. Managing people using AI requires advice that integrates all disciplines from the outset.

The Supreme Court has already confirmed the invalidity of digital monitoring policies drawn up without the involvement of workers' legal representatives (Article 87(3) of the LOPDGDD), with the added consequence that evidence obtained under such policies may be declared unlawful.

It is the grey areas that pose the greatest practical risk: it is in systems that do not formally meet the high-risk threshold under the AI Act, but which give rise to real legal exposure under employment and data protection legislation, that companies are most likely to misjudge the risks. These systems are widespread in day-to-day operations; consider, for example, video surveillance and monitoring systems (performance monitoring via cameras, automatic screen captures or on-screen activity analysis may technically constitute an AI system that does not meet the high-risk threshold, but may breach Article 20 bis of the Workers' Statute, the GDPR and the LOPDGDD); or algorithms for allocating shifts and workloads (these automatically distribute shifts and may not be high-risk if they do not make binding decisions on essential conditions; however, if they affect work-life balance, health or fairness, they may engage obligations relating to collective bargaining, occupational health and safety regulations and equal treatment, among others).

Immediate steps towards AI compliance

These are the steps that any company can take now to begin developing its AI strategy:

1. **AI systems inventory.** Identify and classify the AI systems used in people management: ATS, performance appraisal tools, AI modules in ERP, payroll or internal communications. Without an inventory, compliance is impossible.
2. **Check for absolute prohibitions and high-risk classification.** Review your inventory against the prohibitions set out in the AI Act. If any tool falls into a prohibited category, it must be deactivated immediately. Identify high-risk systems to determine which obligations apply.
3. **Informing the works council.** Assess the extent to which you must comply with the obligation regarding algorithmic transparency set out in Article 64.4.d) of the Workers' Statute. This obligation has been in force since 2021, irrespective of the AI Act.
4. **Genuine human oversight.** Human oversight must be effective, not merely a formality. Consider a process that enables this to be carried out in accordance with the requirements of the legislation.

5. **Audit of AI-based digital monitoring policy.** If your digital monitoring policy was not drawn up with the involvement of workers' legal representatives, it could be declared null and void if challenged (Article 87(3) of the LOPDGDD). If AI systems are not disclosed, the policy may be incomplete.
6. **Review of supplier contracts.** Check that they include clauses on compliance with the AI Act, personal data processing, and guarantees that your employees' data will not be used to train third-party models.
7. **AI literacy and training.** Article 4 of the AI Act requires that all staff and other persons dealing with the operation and use of AI systems on behalf of the deployer have a sufficient level of AI literacy, considering their technical knowledge, experience, education and training.
8. **Adopt an AI usage policy.** A policy that guides your staff and governs the use of AI, the criteria for human oversight and the limits of technological control significantly reduces the risk of disputes and strengthens the company's position in court.

This content is for information purposes only and does not constitute legal advice. For a specific assessment of your situation, please contact our team.