Reuters Legal News

Workplace AI — how employers should prepare for the new EU AI Act deadline

By Yana Komsitsky, Esq., Paul Whinder, and Georgia Hill Smith, Seyfarth Shaw LLP

JULY 17, 2026

The handbrake has been pulled on aspects of the EU's AI Act (**Act**), with key workplace rules, particularly those on high-risk systems, pushed back from August 2, 2026, to December 2, 2027.

The delay may feel welcome for multinational employers keeping up with the spread of AI adoption across their organization, but it is an opportunity to get the groundwork done.

The European Commission in late May published draft guidelines on the classification of high-risk AI systems (**Guidelines**, https://bit.ly/4vDtgOV) for the Act. This is the clearest indication yet of how EU workplace AI tools will be treated, using many real examples.

To function efficiently across borders, business must incorporate these rules into their global compliance framework for legal, HR, talent acquisition, procurement, IT, data, compliance and operations.

The extra months are useful runway, because HR, recruitment, performance management and workforce allocation tools will require the full gamut of "high-risk" systems compliance. Global employers need time to work this into a matrix of other global rules — including in multiple US jurisdictions (e.g., California, Colorado, Connecticut, New York), Canada, Korea's Basic AI Act, the updated UK GDPR and emerging rules elsewhere.

Below is a pragmatic look at what use cases trigger the Act, and what global employers need to do from governance, procurement, data protection and employee relations perspectives.

Why this matters for employers

The Act regulates use of AI systems in the EU — including for recruiting, hiring and managing workforce. It is a risk-based model: the higher the potential impact on individuals' rights, safety or opportunities, the heavier the compliance burden.

Unsurprisingly, recruitment and employment are treated as inherently sensitive — a common approach globally. AI used to screen and rank candidates, assess performance, allocate work, monitor employees and influence promotion or termination decisions directly affect individual rights and opportunities.

To function efficiently across borders, business must incorporate these rules into their global compliance framework for legal, HR, talent acquisition, procurement, IT, data, compliance and operations. That means making it "work" alongside other rules, including the California CCPA "Automated Decisionmaking Tool" (ADMT) Rules, which take a different approach to coverage of HR tools but mercifully allow employers to leverage compliance efforts across frameworks.

When does workplace AI become 'high-risk'?

AI systems used for recruitment, selection, worker management, access to self-employment, task allocation, performance monitoring or decisions affecting the terms or continuation of work relationships may be high-risk. This includes:

(1) Sourcing and selection tools, those used for targeted job advertising, filtering applications, ranking or shortlisting or those used in interviews or assessments.

(2) Workforce management tools used to make or support promotion, termination, task allocation, performance monitoring or behavioural evaluation decisions.

The vendor's marketing label or description is not decisive. Whether standalone or embedded in an applicant tracking or HR system, productivity, workforce management platform or vendor service, AI systems require classification analysis.

Even where a human makes the final decision, if AI output materially influences the process — by ranking, scoring, filtering, recommending, flagging or steering a decision — the system may still be high-risk. In contrast to other frameworks, including the Act's California cousin, the GDPR and UK GDPR, "human involvement" is not relevant for the assessment.

The more a tool evaluates, ranks, scores, filters, recommends or otherwise steers decisions about individuals, the more likely it is to attract high-risk treatment. The more it performs a genuinely administrative or non-evaluative function, the stronger the argument it is outside the high-risk regime.

When triaging tools, consider whether the tool is merely organizing information or supporting human work, versus shaping a decision that will influence an individual's trajectory at work. The decision tree is similar but not identical across other frameworks, so care needs to be taken when reaching different conclusions for the same functionality in different jurisdictions.

The commercial issue is bigger than legal classification

For many employers, identifying all functions of a tool, understanding how they are used and building a governance process that scales to the volume of vendors and business functions adopting tools and mushrooming global laws is where the burden is heaviest.

Procurement will matter. Employers should understand and pressure test how vendors describe their tools, available documentation, and whether contractual terms allocate responsibility clearly. As developers, many vendors focus on preserving human decision-making, but that is not the end of the line for employers as tool deployers.

Use case specifics will matter. A generally low-risk tool may become high-risk when used to influence hiring, work allocation or performance decisions.

Data protection remains central. Workplace AI also raises GDPR issues, including transparency, lawful basis, special category data, automated decision-making and data protection impact assessments, and implicates other global privacy laws in jurisdictions without well-developed AI law. For global rollout, information disclosure and opt-out designs must consider multiple local laws.

Don't underestimate employee relations risk. Opaque AI use in recruitment or aggressive use in performance management or health & safety, can create trust, works council and employee relations issues for legally defensible tools.

These considerations make Act readiness a holistic governance project, much like GDPR readiness in 2018. Program design is more complex for organizations that need to ensure compatibility with frameworks like California ADMT. Businesses that already know where their AI is being used and how will be best placed to apply the high-risk rules.

What employers should do now

The delay gives employers a useful window to implement a pragmatic action plan:

Map use cases. Identify AI-enabled tools used in recruitment, onboarding, performance management, monitoring, workforce planning, task allocation, health & safety, pay, promotion, termination and contractor/platform worker management. Consider systematically checking in with every existing vendor as vendors are frequently releasing new embedded tools. Leverage GDPR data flow mapping.

The European Commission in late May published draft guidelines on the classification of high-risk AI systems for the Act. This is the clearest indication yet of how EU workplace AI tools will be treated, using many real examples.

Classify by function, not label. Focus on what the tool is intended to do and whether it influences decisions, rather than whether it is marketed pre or post sale as "automation," "workflow optimization," "productivity," "analytics" or "decision support."

Separate administrative tools from decision-influencing tools. Build a triage process distinguishing scheduling, formatting and factual verification from ranking, scoring, filtering, profiling or recommendation.

Pressure-test vendor positions. Review technical documentation, instructions for use, contractual commitments, audit rights, change management provisions and allocation of provider/deployer responsibilities. Some dialogue with vendors may be necessary. It is important to recognize that vendors may have built compliance on other frameworks.

Document the analysis. Keep a record of classification, assumptions, human oversight measures, data protection analysis and controls for deviations from intended use. Ensure that new use cases do not "creep in."

Build governance that can scale. Align legal, HR, procurement, IT, privacy, compliance and works council strategy so that AI adoption is reviewed before tools are bought, configured or expanded across the EU.

Don't wait! The early bird really does get the worm. There are some real advantages to rolling out now instead of more watchful waiting.

Bottom line: Employers with an EU footprint should assume that AI governance in HR and workforce management will become a standing compliance, procurement and employee relations issue, and act accordingly. The organizations that get to work now will be better positioned to adopt the growing surge of workplace AI at speed when the high-risk and other regimes come fully into view.

About the authors



Yana Komsitsky (L) is a global compliance lawyer in the international and data law practices at **Seyfarth Shaw LLP**, based in Los Angeles. She advises global companies on designing and implementing workplace AI and privacy compliance across their global workforce and works with AI technology vendors in bringing their products to various markets across the globe, including into the EU. She can be reached at ykomsitsky@seyfarth.com. **Paul Whinder** (C) is managing partner of the firm's London office and part of the international practice. He acts for a range of cross-sector businesses, from start-ups to household name U.K. and multi-national businesses, advising on a range of employment matters, both contentious and non-contentious, on both a domestic and an international basis. He can be reached at pwhinder@seyfarth.com. **Georgia Hill Smith**, (R) based in the firm's London office, is a lawyer in the international practice. She advises clients on employment law and industrial relations matters across multiple jurisdictions. She helps employers navigate the complexities of differing regulatory frameworks and cultural considerations in an increasingly globalized world. She can be reached at ghillsmith@seyfarth.com.

This article was first published on Reuters Legal News and Westlaw Today on July 17, 2026.